

Intel® 64 and IA-32 Architectures Software Developer's Manual

Volume 2B: Instruction Set Reference, N-Z

NOTE: The Intel 64 and IA-32 Architectures Software Developer's Manual consists of five volumes: *Basic Architecture*, Order Number 253665; *Instruction Set Reference A-M*, Order Number 253666; *Instruction Set Reference N-Z*, Order Number 253667; *System Programming Guide, Part 1*, Order Number 253668; *System Programming Guide, Part 2*, Order Number 253669. Refer to all five volumes when evaluating your design needs.

Order Number: 253667-028US
September 2008

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

Intel may make changes to specifications and product descriptions at any time, without notice.

Developers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Improper use of reserved or undefined features or instructions may cause unpredictable behavior or failure in developer's software code when running on an Intel processor. Intel reserves these features or instructions for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from their unauthorized use.

The Intel® 64 architecture processors may contain design defects or errors known as errata. Current characterized errata are available on request.

Hyper-Threading Technology requires a computer system with an Intel® processor supporting Hyper-Threading Technology and an HT Technology enabled chipset, BIOS and operating system. Performance will vary depending on the specific hardware and software you use. For more information, see <http://www.intel.com/technology/hyperthread/index.htm>; including details on which processors support HT Technology.

Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and for some uses, certain platform software enabled for it. Functionality, performance or other benefits will vary depending on hardware and software configurations. Intel® Virtualization Technology-enabled BIOS and VMM applications are currently in development.

64-bit computing on Intel architecture requires a computer system with a processor, chipset, BIOS, operating system, device drivers and applications enabled for Intel® 64 architecture. Processors will not operate (including 32-bit operation) without an Intel® 64 architecture-enabled BIOS. Performance will vary depending on your hardware and software configurations. Consult with your system vendor for more information.

Enabling Execute Disable Bit functionality requires a PC with a processor with Execute Disable Bit capability and a supporting operating system. Check with your PC manufacturer on whether your system delivers Execute Disable Bit functionality.

Intel, Pentium, Intel Xeon, Intel NetBurst, Intel Core Solo, Intel Core Duo, Intel Core 2 Duo, Intel Core 2 Extreme, Intel Pentium D, Itanium, Intel SpeedStep, MMX, Intel Atom, and VTune are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an ordering number and are referenced in this document, or other Intel literature, may be obtained from:

Intel Corporation
P.O. Box 5937
Denver, CO 80217-9808

or call 1-800-548-4725

or visit Intel's website at <http://www.intel.com>

Copyright © 1997-2008 Intel Corporation

CHAPTER 4

INSTRUCTION SET REFERENCE, N-Z

4.1 INSTRUCTIONS (N-Z)

Chapter 4 continues an alphabetical discussion of Intel® 64 and IA-32 instructions (N-Z). See also: Chapter 3, “Instruction Set Reference, A-M,” in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A*.

NEG—Two's Complement Negation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|---------------|-------------------|-------------|---------------------|--|
| F6 /3 | NEG <i>r/m8</i> | Valid | Valid | Two's complement negate <i>r/m8</i> . |
| REX + F6 /3 | NEG <i>r/m8</i> * | Valid | N.E. | Two's complement negate <i>r/m8</i> . |
| F7 /3 | NEG <i>r/m16</i> | Valid | Valid | Two's complement negate <i>r/m16</i> . |
| F7 /3 | NEG <i>r/m32</i> | Valid | Valid | Two's complement negate <i>r/m32</i> . |
| REX.W + F7 /3 | NEG <i>r/m64</i> | Valid | N.E. | Two's complement negate <i>r/m64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Replaces the value of operand (the destination operand) with its two's complement. (This operation is equivalent to subtracting the operand from 0.) The destination operand is located in a general-purpose register or a memory location.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

```
IF DEST = 0
    THEN CF ← 0;
    ELSE CF ← 1;
FI;
DEST ← [- (DEST)]
```

Flags Affected

The CF flag set to 0 if the source operand is 0; otherwise it is set to 1. The OF, SF, ZF, AF, and PF flags are set according to the result.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|--------|--|
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

NOP—No Operation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|-------------|-------------|---------------------|--------------------------------------|
| 90 | NOP | Valid | Valid | One byte no-operation instruction. |
| 0F 1F /0 | NOP r/m16 | Valid | Valid | Multi-byte no-operation instruction. |
| 0F 1F /0 | NOP r/m32 | Valid | Valid | Multi-byte no-operation instruction. |

Description

This instruction performs no operation. It is a one-byte or multi-byte NOP that takes up space in the instruction stream but does not impact machine context, except for the EIP register.

The multi-byte form of NOP is available on processors with model encoding:

- CPUID.01H.EAX[Bytes 11:8] = 0110B or 1111B

The multi-byte NOP instruction does not alter the content of a register and will not issue a memory operation. The instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

The one-byte NOP instruction is an alias mnemonic for the XCHG (E)AX, (E)AX instruction.

The multi-byte NOP instruction performs no operation on supported processors and generates undefined opcode exception on processors that do not support the multi-byte NOP instruction.

The memory operand form of the instruction allows software to create a byte sequence of "no operation" as one instruction. For situations where multiple-byte NOPs are needed, the recommended operations (32-bit mode and 64-bit mode) are:

Table 4-1. Recommended Multi-Byte Sequence of NOP Instruction

| Length | Assembly | Byte Sequence |
|---------|--------------------------------------|-----------------------|
| 2 bytes | 66 NOP | 66 90H |
| 3 bytes | NOP DWORD ptr [EAX] | 0F 1F 00H |
| 4 bytes | NOP DWORD ptr [EAX + 00H] | 0F 1F 40 00H |
| 5 bytes | NOP DWORD ptr [EAX + EAX*1 + 00H] | 0F 1F 44 00 00H |
| 6 bytes | 66 NOP DWORD ptr [EAX + EAX*1 + 00H] | 66 0F 1F 44 00 00H |
| 7 bytes | NOP DWORD ptr [EAX + 00000000H] | 0F 1F 80 00 00 00 00H |

Table 4-1. Recommended Multi-Byte Sequence of NOP Instruction (Contd.)

| Length | Assembly | Byte Sequence |
|---------|--|-----------------------------|
| 8 bytes | NOP DWORD ptr [EAX + EAX*1 + 00000000H] | 0F 1F 84 00 00 00 00 00H |
| 9 bytes | 66 NOP DWORD ptr [EAX + EAX*1 + 00000000H] | 66 0F 1F 84 00 00 00 00 00H |

Flags Affected

None.

Exceptions (All Operating Modes)

#UD If the LOCK prefix is used.

NOT—One's Complement Negation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|---------------|-------------------|-------------|------------------|------------------------------------|
| F6 /2 | NOT <i>r/m8</i> | Valid | Valid | Reverse each bit of <i>r/m8</i> . |
| REX + F6 /2 | NOT <i>r/m8</i> * | Valid | N.E. | Reverse each bit of <i>r/m8</i> . |
| F7 /2 | NOT <i>r/m16</i> | Valid | Valid | Reverse each bit of <i>r/m16</i> . |
| F7 /2 | NOT <i>r/m32</i> | Valid | Valid | Reverse each bit of <i>r/m32</i> . |
| REX.W + F7 /2 | NOT <i>r/m64</i> | Valid | N.E. | Reverse each bit of <i>r/m64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Performs a bitwise NOT operation (each 1 is set to 0, and each 0 is set to 1) on the destination operand and stores the result in the destination operand location. The destination operand can be a register or a memory location.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

DEST ← NOT DEST;

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination operand points to a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|--------|--|
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

OR—Logical Inclusive OR

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|--------------------------------|-------------|------------------|--|
| 0C <i>ib</i> | OR AL, <i>imm8</i> | Valid | Valid | AL OR <i>imm8</i> . |
| 0D <i>iw</i> | OR AX, <i>imm16</i> | Valid | Valid | AX OR <i>imm16</i> . |
| 0D <i>id</i> | OR EAX, <i>imm32</i> | Valid | Valid | EAX OR <i>imm32</i> . |
| REX.W + 0D <i>id</i> | OR RAX, <i>imm32</i> | Valid | N.E. | RAX OR <i>imm32</i> (<i>sign-extended</i>). |
| 80 /1 <i>ib</i> | OR <i>r/m8</i> , <i>imm8</i> | Valid | Valid | <i>r/m8</i> OR <i>imm8</i> . |
| REX + 80 /1 <i>ib</i> | OR <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | <i>r/m8</i> OR <i>imm8</i> . |
| 81 /1 <i>iw</i> | OR <i>r/m16</i> , <i>imm16</i> | Valid | Valid | <i>r/m16</i> OR <i>imm16</i> . |
| 81 /1 <i>id</i> | OR <i>r/m32</i> , <i>imm32</i> | Valid | Valid | <i>r/m32</i> OR <i>imm32</i> . |
| REX.W + 81 /1 <i>id</i> | OR <i>r/m64</i> , <i>imm32</i> | Valid | N.E. | <i>r/m64</i> OR <i>imm32</i> (<i>sign-extended</i>). |
| 83 /1 <i>ib</i> | OR <i>r/m16</i> , <i>imm8</i> | Valid | Valid | <i>r/m16</i> OR <i>imm8</i> (<i>sign-extended</i>). |
| 83 /1 <i>ib</i> | OR <i>r/m32</i> , <i>imm8</i> | Valid | Valid | <i>r/m32</i> OR <i>imm8</i> (<i>sign-extended</i>). |
| REX.W + 83 /1 <i>ib</i> | OR <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | <i>r/m64</i> OR <i>imm8</i> (<i>sign-extended</i>). |
| 08 / <i>r</i> | OR <i>r/m8</i> , <i>r8</i> | Valid | Valid | <i>r/m8</i> OR <i>r8</i> . |
| REX + 08 / <i>r</i> | OR <i>r/m8*</i> , <i>r8*</i> | Valid | N.E. | <i>r/m8</i> OR <i>r8</i> . |
| 09 / <i>r</i> | OR <i>r/m16</i> , <i>r16</i> | Valid | Valid | <i>r/m16</i> OR <i>r16</i> . |
| 09 / <i>r</i> | OR <i>r/m32</i> , <i>r32</i> | Valid | Valid | <i>r/m32</i> OR <i>r32</i> . |
| REX.W + 09 / <i>r</i> | OR <i>r/m64</i> , <i>r64</i> | Valid | N.E. | <i>r/m64</i> OR <i>r64</i> . |
| 0A / <i>r</i> | OR <i>r8</i> , <i>r/m8</i> | Valid | Valid | <i>r8</i> OR <i>r/m8</i> . |
| REX + 0A / <i>r</i> | OR <i>r8*</i> , <i>r/m8*</i> | Valid | N.E. | <i>r8</i> OR <i>r/m8</i> . |
| 0B / <i>r</i> | OR <i>r16</i> , <i>r/m16</i> | Valid | Valid | <i>r16</i> OR <i>r/m16</i> . |
| 0B / <i>r</i> | OR <i>r32</i> , <i>r/m32</i> | Valid | Valid | <i>r32</i> OR <i>r/m32</i> . |
| REX.W + 0B / <i>r</i> | OR <i>r64</i> , <i>r/m64</i> | Valid | N.E. | <i>r64</i> OR <i>r/m64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Performs a bitwise inclusive OR operation between the destination (first) and source (second) operands and stores the result in the destination operand location. The source operand can be an immediate, a register, or a memory location; the destination operand can be a register or a memory location. (However, two memory operands cannot be used in one instruction.) Each bit of the result of the OR instruction is set to 0 if both corresponding bits of the first and second operands are 0; otherwise, each bit is set to 1.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

DEST ← DEST OR SRC;

Flags Affected

The OF and CF flags are cleared; the SF, ZF, and PF flags are set according to the result. The state of the AF flag is undefined.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination operand points to a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |

#UD If the LOCK prefix is used but the destination is not a memory operand.

Virtual-8086 Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF (fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made.

#UD If the LOCK prefix is used but the destination is not a memory operand.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

#PF (fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

#UD If the LOCK prefix is used but the destination is not a memory operand.

ORPD—Bitwise Logical OR of Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|-------------------------------------|-------------|-----------------|--|
| 66 0F 56 /r | ORPD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Bitwise OR of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical OR of the two packed double-precision floating-point values from the source operand (second operand) and the destination operand (first operand), and stores the result in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[127:0] ← DEST[127:0] BitwiseOR SRC[127:0];

Intel® C/C++ Compiler Intrinsic Equivalent

ORPD __m128d _mm_or_pd(__m128d a, __m128d b)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

ORPS—Bitwise Logical OR of Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|-----------------------------|-------------|-----------------|--|
| OF 56 /r | ORPS <i>xmm1, xmm2/m128</i> | Valid | Valid | Bitwise OR of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical OR of the four packed single-precision floating-point values from the source operand (second operand) and the destination operand (first operand), and stores the result in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[127:0] ← DEST[127:0] BitwiseOR SRC[127:0];

Intel C/C++ Compiler Intrinsic Equivalent

ORPS __m128_mm_or_ps(__m128 a, __m128 b)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.
- #PF (fault-code) For a page fault.
- #NM If CR0.TS[bit 3] = 1.
- #UD If CR0.EM[bit 2] = 1.
If CR4.OSFXSR[bit 9] = 0.
If CPUID.01H:EDX.SSE[bit 25] = 0.
If the LOCK prefix is used.

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

OUT—Output to Port

| Opcode* | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------------|-----------------------|-------------|------------------|--|
| E6 <i>ib</i> | OUT <i>imm8</i> , AL | Valid | Valid | Output byte in AL to I/O port address <i>imm8</i> . |
| E7 <i>ib</i> | OUT <i>imm8</i> , AX | Valid | Valid | Output word in AX to I/O port address <i>imm8</i> . |
| E7 <i>ib</i> | OUT <i>imm8</i> , EAX | Valid | Valid | Output doubleword in EAX to I/O port address <i>imm8</i> . |
| EE | OUT DX, AL | Valid | Valid | Output byte in AL to I/O port address in DX. |
| EF | OUT DX, AX | Valid | Valid | Output word in AX to I/O port address in DX. |
| EF | OUT DX, EAX | Valid | Valid | Output doubleword in EAX to I/O port address in DX. |

NOTES:

* See IA-32 Architecture Compatibility section below.

Description

Copies the value from the second operand (source operand) to the I/O port specified with the destination operand (first operand). The source operand can be register AL, AX, or EAX, depending on the size of the port being accessed (8, 16, or 32 bits, respectively); the destination operand can be a byte-immediate or the DX register. Using a byte immediate allows I/O port addresses 0 to 255 to be accessed; using the DX register as a source operand allows I/O ports from 0 to 65,535 to be accessed.

The size of the I/O port being accessed is determined by the opcode for an 8-bit I/O port or by the operand-size attribute of the instruction for a 16- or 32-bit I/O port.

At the machine code level, I/O instructions are shorter when accessing 8-bit I/O ports. Here, the upper eight bits of the port address will be 0.

This instruction is only useful for accessing I/O ports located in the processor's I/O address space. See Chapter 13, "Input/Output," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for more information on accessing I/O ports in the I/O address space.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

IA-32 Architecture Compatibility

After executing an OUT instruction, the Pentium® processor insures that the EWBE# pin has been sampled active before it begins to execute the next instruction. (Note that the instruction can be prefetched if EWBE# is not active, but it will not be

executed until the EWBE# pin is sampled active.) Only the Pentium processor family has the EWBE# pin.

Operation

```
IF ((PE = 1) and ((CPL > IOPL) or (VM = 1)))
    THEN (* Protected mode with CPL > IOPL or virtual-8086 mode *)
        IF (Any I/O Permission Bit for I/O port being accessed = 1)
            THEN (* I/O operation is not allowed *)
                #GP(0);
            ELSE (* I/O operation is allowed *)
                DEST ← SRC; (* Writes to selected I/O port *)
        FI;
    ELSE (Real Mode or Protected Mode with CPL ≤ IOPL *)
        DEST ← SRC; (* Writes to selected I/O port *)
FI;
```

Flags Affected

None.

Protected Mode Exceptions

| | |
|--------|--|
| #GP(0) | If the CPL is greater than (has less privilege) the I/O privilege level (IOPL) and any of the corresponding I/O permission bits in TSS for the I/O port being accessed is 1. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|-----------------------------|
| #UD | If the LOCK prefix is used. |
|-----|-----------------------------|

Virtual-8086 Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If any of the I/O permission bits in the TSS for the I/O port being accessed is 1. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same as protected mode exceptions.

64-Bit Mode Exceptions

Same as protected mode exceptions.

OUTS/OUTSB/OUTSW/OUTSD—Output String to Port

| Opcode* | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|---------|---------------------|-------------|---------------------|--|
| 6E | OUTS DX, <i>m8</i> | Valid | Valid | Output byte from memory location specified in DS:(E)SI or RSI to I/O port specified in DX**. |
| 6F | OUTS DX, <i>m16</i> | Valid | Valid | Output word from memory location specified in DS:(E)SI or RSI to I/O port specified in DX**. |
| 6F | OUTS DX, <i>m32</i> | Valid | Valid | Output doubleword from memory location specified in DS:(E)SI or RSI to I/O port specified in DX**. |
| 6E | OUTSB | Valid | Valid | Output byte from memory location specified in DS:(E)SI or RSI to I/O port specified in DX**. |
| 6F | OUTSW | Valid | Valid | Output word from memory location specified in DS:(E)SI or RSI to I/O port specified in DX**. |
| 6F | OUTSD | Valid | Valid | Output doubleword from memory location specified in DS:(E)SI or RSI to I/O port specified in DX**. |

NOTES:

* See IA-32 Architecture Compatibility section below.

** In 64-bit mode, only 64-bit (RSI) and 32-bit (ESI) address sizes are supported. In non-64-bit mode, only 32-bit (ESI) and 16-bit (SI) address sizes are supported.

Description

Copies data from the source operand (second operand) to the I/O port specified with the destination operand (first operand). The source operand is a memory location, the address of which is read from either the DS:SI, DS:ESI or the RSI registers (depending on the address-size attribute of the instruction, 16, 32 or 64, respectively). (The DS segment may be overridden with a segment override prefix.) The destination operand is an I/O port address (from 0 to 65,535) that is read from the DX register. The size of the I/O port being accessed (that is, the size of the source and destination operands) is determined by the opcode for an 8-bit I/O port or by the operand-size attribute of the instruction for a 16- or 32-bit I/O port.

At the assembly-code level, two forms of this instruction are allowed: the “explicit-operands” form and the “no-operands” form. The explicit-operands form (specified with the OUTS mnemonic) allows the source and destination operands to be specified explicitly. Here, the source operand should be a symbol that indicates the size of the

I/O port and the source address, and the destination operand must be DX. This explicit-operands form is provided to allow documentation; however, note that the documentation provided by this form can be misleading. That is, the source operand symbol must specify the correct **type** (size) of the operand (byte, word, or doubleword), but it does not have to specify the correct **location**. The location is always specified by the DS: (E)SI or RSI registers, which must be loaded correctly before the OUTS instruction is executed.

The no-operands form provides “short forms” of the byte, word, and doubleword versions of the OUTS instructions. Here also DS: (E)SI is assumed to be the source operand and DX is assumed to be the destination operand. The size of the I/O port is specified with the choice of mnemonic: OUTSB (byte), OUTSW (word), or OUTSD (doubleword).

After the byte, word, or doubleword is transferred from the memory location to the I/O port, the SI/ESI/RSI register is incremented or decremented automatically according to the setting of the DF flag in the EFLAGS register. (If the DF flag is 0, the (E)SI register is incremented; if the DF flag is 1, the SI/ESI/RSI register is decremented.) The SI/ESI/RSI register is incremented or decremented by 1 for byte operations, by 2 for word operations, and by 4 for doubleword operations.

The OUTS, OUTSB, OUTSW, and OUTSD instructions can be preceded by the REP prefix for block input of ECX bytes, words, or doublewords. See “REP/REPE/REPZ/REPNE/REPZ—Repeat String Operation Prefix” in this chapter for a description of the REP prefix. This instruction is only useful for accessing I/O ports located in the processor’s I/O address space. See Chapter 13, “Input/Output,” in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 1*, for more information on accessing I/O ports in the I/O address space.

In 64-bit mode, the default operand size is 32 bits; operand size is not promoted by the use of REX.W. In 64-bit mode, the default address size is 64 bits, and 64-bit address is specified using RSI by default. 32-bit address using ESI is support using the prefix 67H, but 16-bit address is not supported in 64-bit mode.

IA-32 Architecture Compatibility

After executing an OUTS, OUTSB, OUTSW, or OUTSD instruction, the Pentium processor insures that the EWBE# pin has been sampled active before it begins to execute the next instruction. (Note that the instruction can be prefetched if EWBE# is not active, but it will not be executed until the EWBE# pin is sampled active.) Only the Pentium processor family has the EWBE# pin.

For the Pentium 4, Intel® Xeon®, and P6 processor family, upon execution of an OUTS, OUTSB, OUTSW, or OUTSD instruction, the processor will not execute the next instruction until the data phase of the transaction is complete.

Operation

```
IF ((PE = 1) and ((CPL > IOPL) or (VM = 1)))
  THEN (* Protected mode with CPL > IOPL or virtual-8086 mode *)
```

INSTRUCTION SET REFERENCE, N-Z

```
IF (Any I/O Permission Bit for I/O port being accessed = 1)
    THEN (* I/O operation is not allowed *)
        #GP(0);
    ELSE (* I/O operation is allowed *)
        DEST ← SRC; (* Writes to I/O port *)
FI;
ELSE (Real Mode or Protected Mode or 64-Bit Mode with CPL ≤ IOPL *)
    DEST ← SRC; (* Writes to I/O port *)
FI;
```

Byte transfer:

```
IF 64-bit mode
    Then
        IF 64-Bit Address Size
            THEN
                IF DF = 0
                    THEN RSI ← RSI + 1;
                    ELSE RSI ← RSI or - 1;
                FI;
            ELSE (* 32-Bit Address Size *)
                IF DF = 0
                    THEN ESI ← ESI + 1;
                    ELSE ESI ← ESI - 1;
                FI;
            FI;
        ELSE
            IF DF = 0
                THEN (ESI) ← (ESI) + 1;
                ELSE (ESI) ← (ESI) - 1;
            FI;
    FI;
```

Word transfer:

```
IF 64-bit mode
    Then
        IF 64-Bit Address Size
            THEN
                IF DF = 0
                    THEN RSI ← RSI + 2;
                    ELSE RSI ← RSI or - 2;
                FI;
            ELSE (* 32-Bit Address Size *)
                IF DF = 0
                    THEN ESI ← ESI + 2;
```

```

        ELSE    ESI ← ESI - 2;
    FI;
FI;
ELSE
    IF DF = 0
        THEN    (E)SI ← (E)SI + 2;
        ELSE    (E)SI ← (E)SI - 2;
    FI;
FI;
Doubleword transfer:
IF 64-bit mode
    Then
        IF 64-Bit Address Size
            THEN
                IF DF = 0
                    THEN RSI ← RSI + 4;
                    ELSE RSI ← RSI - 4;
                FI;
            ELSE (* 32-Bit Address Size *)
                IF DF = 0
                    THEN    ESI ← ESI + 4;
                    ELSE    ESI ← ESI - 4;
                FI;
            FI;
        ELSE
            IF DF = 0
                THEN    (E)SI ← (E)SI + 4;
                ELSE    (E)SI ← (E)SI - 4;
            FI;
FI;

```

Flags Affected

None.

Protected Mode Exceptions

- #GP(0) If the CPL is greater than (has less privilege) the I/O privilege level (IOPL) and any of the corresponding I/O permission bits in TSS for the I/O port being accessed is 1.
 If a memory operand effective address is outside the limit of the CS, DS, ES, FS, or GS segment.
 If the segment register contains a NULL segment selector.
- #PF(fault-code) If a page fault occurs.

INSTRUCTION SET REFERENCE, N-Z

| | |
|--------|--|
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If any of the I/O permission bits in the TSS for the I/O port being accessed is 1. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the CPL is greater than (has less privilege) the I/O privilege level (IOPL) and any of the corresponding I/O permission bits in TSS for the I/O port being accessed is 1. If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

PABSB/PABSW/PABSD – Packed Absolute Value

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|-----------------------|-------------|------------------|---|
| 0F 38 1C /r | PABSB mm1, mm2/m64 | Valid | Valid | Compute the absolute value of bytes in mm2/m64 and store UNSIGNED result in mm1. |
| 66 0F 38 1C /r | PABSB xmm1, xmm2/m128 | Valid | Valid | Compute the absolute value of bytes in xmm2/m128 and store UNSIGNED result in xmm1. |
| 0F 38 1D /r | PABSW mm1, mm2/m64 | Valid | Valid | Compute the absolute value of 16-bit integers in mm2/m64 and store UNSIGNED result in mm1. |
| 66 0F 38 1D /r | PABSW xmm1, xmm2/m128 | Valid | Valid | Compute the absolute value of 16-bit integers in xmm2/m128 and store UNSIGNED result in xmm1. |
| 0F 38 1E /r | PABSD mm1, mm2/m64 | Valid | Valid | Compute the absolute value of 32-bit integers in mm2/m64 and store UNSIGNED result in mm1. |
| 66 0F 38 1E /r | PABSD xmm1, xmm2/m128 | Valid | Valid | Compute the absolute value of 32-bit integers in xmm2/m128 and store UNSIGNED result in xmm1. |

Description

PABSB/W/D computes the absolute value of each data element of the source operand (the second operand) and stores the UNSIGNED results in the destination operand (the first operand). PABSB operates on signed bytes, PABSW operates on 16-bit words, and PABSD operates on signed 32-bit integers. The source operand can be an MMX register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX or an XMM register. Both operands can be MMX register or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PABSB with 64 bit operands

```
Unsigned DEST[7:0] ← ABS(SRC[7:0])
Repeat operation for 2nd through 7th bytes
Unsigned DEST[63:56] ← ABS(SRC[63:56])
```

INSTRUCTION SET REFERENCE, N-Z

PABSB with 128 bit operands:

Unsigned DEST[7:0] ← ABS(SRC[7:0])
Repeat operation for 2nd through 15th bytes
Unsigned DEST[127:120] ← ABS(SRC[127:120])

PABSW with 64 bit operands:

Unsigned DEST[15:0] ← ABS(SRC[15:0])
Repeat operation for 2nd through 3rd 16-bit words
Unsigned DEST[63:48] ← ABS(SRC[63:48])

PABSW with 128 bit operands:

Unsigned DEST[15:0] ← ABS(SRC[15:0])
Repeat operation for 2nd through 7th 16-bit words
Unsigned DEST[127:112] ← ABS(SRC[127:112])

PABSD with 64 bit operands:

Unsigned DEST[31:0] ← ABS(SRC[31:0])
Unsigned DEST[63:32] ← ABS(SRC[63:32])

PABSD with 128 bit operands:

Unsigned DEST[31:0] ← ABS(SRC[31:0])
Repeat operation for 2nd through 3rd 32-bit double words
Unsigned DEST[127:96] ← ABS(SRC[127:96])

Intel C/C++ Compiler Intrinsic Equivalents

PABSB __m64 __mm_abs_pi8 (__m64 a)
PABSB __m128i __mm_abs_epi8 (__m128i a)
PABSW __m64 __mm_abs_pi16 (__m64 a)
PABSW __m128i __mm_abs_epi16 (__m128i a)
PABSD __m64 __mm_abs_pi32 (__m64 a)
PABSD __m128i __mm_abs_epi32 (__m128i a)

Protected Mode Exceptions

#GP(0): If a memory operand effective address is outside the CS, DS, ES, FS or GS segments.
 (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

| | |
|-----------------|--|
| #PF(fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|---------|--|
| #GP(0): | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #UD: | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. |

| | |
|------------------|---|
| | (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PACKSSWB/PACKSSDW—Pack with Signed Saturation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F 63 /r | PACKSSWB <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Converts 4 packed signed word integers from <i>mm1</i> and from <i>mm2/m64</i> into 8 packed signed byte integers in <i>mm1</i> using signed saturation. |
| 66 0F 63 /r | PACKSSWB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Converts 8 packed signed word integers from <i>xmm1</i> and from <i>xmm2/m128</i> into 16 packed signed byte integers in <i>xmm1</i> using signed saturation. |
| 0F 6B /r | PACKSSDW <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Converts 2 packed signed doubleword integers from <i>mm1</i> and from <i>mm2/m64</i> into 4 packed signed word integers in <i>mm1</i> using signed saturation. |
| 66 0F 6B /r | PACKSSDW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Converts 4 packed signed doubleword integers from <i>xmm1</i> and from <i>xmm2/m128</i> into 8 packed signed word integers in <i>xmm1</i> using signed saturation. |

Description

Converts packed signed word integers into packed signed byte integers (PACKSSWB) or converts packed signed doubleword integers into packed signed word integers (PACKSSDW), using saturation to handle overflow conditions. See Figure 4-1 for an example of the packing operation.

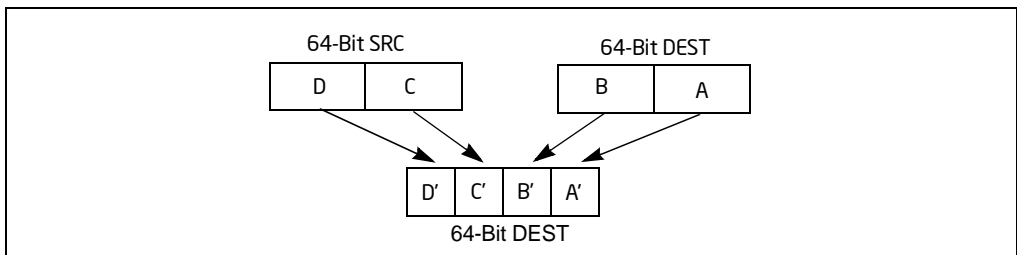


Figure 4-1. Operation of the PACKSSDW Instruction Using 64-bit Operands

The PACKSSWB instruction converts 4 or 8 signed word integers from the destination operand (first operand) and 4 or 8 signed word integers from the source operand

(second operand) into 8 or 16 signed byte integers and stores the result in the destination operand. If a signed word integer value is beyond the range of a signed byte integer (that is, greater than 7FH for a positive integer or greater than 80H for a negative integer), the saturated signed byte integer value of 7FH or 80H, respectively, is stored in the destination.

The PACKSSDW instruction packs 2 or 4 signed doublewords from the destination operand (first operand) and 2 or 4 signed doublewords from the source operand (second operand) into 4 or 8 signed words in the destination operand (see Figure 4-1). If a signed doubleword integer value is beyond the range of a signed word (that is, greater than 7FFFH for a positive integer or greater than 8000H for a negative integer), the saturated signed word integer value of 7FFFH or 8000H, respectively, is stored into the destination.

The PACKSSWB and PACKSSDW instructions operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PACKSSWB instruction with 64-bit operands:

```
DEST[7:0] ← SaturateSignedWordToSignedByte DEST[15:0];
DEST[15:8] ← SaturateSignedWordToSignedByte DEST[31:16];
DEST[23:16] ← SaturateSignedWordToSignedByte DEST[47:32];
DEST[31:24] ← SaturateSignedWordToSignedByte DEST[63:48];
DEST[39:32] ← SaturateSignedWordToSignedByte SRC[15:0];
DEST[47:40] ← SaturateSignedWordToSignedByte SRC[31:16];
DEST[55:48] ← SaturateSignedWordToSignedByte SRC[47:32];
DEST[63:56] ← SaturateSignedWordToSignedByte SRC[63:48];
```

PACKSSDW instruction with 64-bit operands:

```
DEST[15:0] ← SaturateSignedDoublewordToSignedWord DEST[31:0];
DEST[31:16] ← SaturateSignedDoublewordToSignedWord DEST[63:32];
DEST[47:32] ← SaturateSignedDoublewordToSignedWord SRC[31:0];
DEST[63:48] ← SaturateSignedDoublewordToSignedWord SRC[63:32];
```

PACKSSWB instruction with 128-bit operands:

```
DEST[7:0] ← SaturateSignedWordToSignedByte (DEST[15:0]);
DEST[15:8] ← SaturateSignedWordToSignedByte (DEST[31:16]);
DEST[23:16] ← SaturateSignedWordToSignedByte (DEST[47:32]);
DEST[31:24] ← SaturateSignedWordToSignedByte (DEST[63:48]);
DEST[39:32] ← SaturateSignedWordToSignedByte (DEST[79:64]);
```

DEST[47:40] ← SaturateSignedWordToSignedByte (DEST[95:80]);
 DEST[55:48] ← SaturateSignedWordToSignedByte (DEST[111:96]);
 DEST[63:56] ← SaturateSignedWordToSignedByte (DEST[127:112]);
 DEST[71:64] ← SaturateSignedWordToSignedByte (SRC[15:0]);
 DEST[79:72] ← SaturateSignedWordToSignedByte (SRC[31:16]);
 DEST[87:80] ← SaturateSignedWordToSignedByte (SRC[47:32]);
 DEST[95:88] ← SaturateSignedWordToSignedByte (SRC[63:48]);
 DEST[103:96] ← SaturateSignedWordToSignedByte (SRC[79:64]);
 DEST[111:104] ← SaturateSignedWordToSignedByte (SRC[95:80]);
 DEST[119:112] ← SaturateSignedWordToSignedByte (SRC[111:96]);
 DEST[127:120] ← SaturateSignedWordToSignedByte (SRC[127:112]);

PACKSSDW instruction with 128-bit operands:

DEST[15:0] ← SaturateSignedDwordToSignedWord (DEST[31:0]);
 DEST[31:16] ← SaturateSignedDwordToSignedWord (DEST[63:32]);
 DEST[47:32] ← SaturateSignedDwordToSignedWord (DEST[95:64]);
 DEST[63:48] ← SaturateSignedDwordToSignedWord (DEST[127:96]);
 DEST[79:64] ← SaturateSignedDwordToSignedWord (SRC[31:0]);
 DEST[95:80] ← SaturateSignedDwordToSignedWord (SRC[63:32]);
 DEST[111:96] ← SaturateSignedDwordToSignedWord (SRC[95:64]);
 DEST[127:112] ← SaturateSignedDwordToSignedWord (SRC[127:96]);

Intel C/C++ Compiler Intrinsic Equivalents

PACKSSWB __m64 _mm_packs_pi16(__m64 m1, __m64 m2)
 PACKSSWB __m128i _mm_packs_epi16(__m128i m1, __m128i m2)
 PACKSSDW __m64 _mm_packs_pi32 (__m64 m1, __m64 m2)
 PACKSSDW __m128i _mm_packs_epi32(__m128i m1, __m128i m2)

Flags Affected

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
 #SS(0) If a memory operand effective address is outside the SS segment limit.
 #UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one

that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

If the LOCK prefix is used.

| | |
|------------------|---|
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|------------------|--|
| #PF (fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. |

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.

(128-bit operations only) If CPUID.01H: EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

#NM

If CR0.TS[bit 3] = 1.

#MF

(64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code)

If a page fault occurs.

#AC(0)

(64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PACKUSDW — Pack with Unsigned Saturation

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|-------------------|--|-------------|------------------|---|
| 66 OF 38 2B /r | PACKUSDW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Convert 4 packed signed doubleword integers from <i>xmm1</i> and 4 packed signed doubleword integers from <i>xmm2/m128</i> into 8 packed unsigned word integers in <i>xmm1</i> using unsigned saturation. |

Description

Converts packed signed doubleword integers into packed unsigned word integers using unsigned saturation to handle overflow conditions. If the signed doubleword value is beyond the range of an unsigned word (that is, greater than FFFFH or less than 0000H), the saturated unsigned word integer value of FFFFH or 0000H, respectively, is stored in the destination.

Operation

```

TMP[15:0] ← (DEST[31:0] < 0) ? 0 : DEST[15:0];
DEST[15:0] ← (DEST[31:0] > FFFFH) ? FFFFH : TMP[15:0];
TMP[31:16] ← (DEST[63:32] < 0) ? 0 : DEST[47:32];
DEST[31:16] ← (DEST[63:32] > FFFFH) ? FFFFH : TMP[31:16];
TMP[47:32] ← (DEST[95:64] < 0) ? 0 : DEST[79:64];
DEST[47:32] ← (DEST[95:64] > FFFFH) ? FFFFH : TMP[47:32];
TMP[63:48] ← (DEST[127:96] < 0) ? 0 : DEST[111:96];
DEST[63:48] ← (DEST[127:96] > FFFFH) ? FFFFH : TMP[63:48];
TMP[63:48] ← (DEST[127:96] < 0) ? 0 : DEST[111:96];
DEST[63:48] ← (DEST[127:96] > FFFFH) ? FFFFH : TMP[63:48];
TMP[79:64] ← (SRC[31:0] < 0) ? 0 : SRC[15:0];
DEST[63:48] ← (SRC[31:0] > FFFFH) ? FFFFH : TMP[79:64];
TMP[95:80] ← (SRC[63:32] < 0) ? 0 : SRC[47:32];
DEST[95:80] ← (SRC[63:32] > FFFFH) ? FFFFH : TMP[95:80];
TMP[111:96] ← (SRC[95:64] < 0) ? 0 : SRC[79:64];
DEST[111:96] ← (SRC[95:64] > FFFFH) ? FFFFH : TMP[111:96];
TMP[127:112] ← (SRC[127:96] < 0) ? 0 : SRC[111:96];
DEST[128:112] ← (SRC[127:96] > FFFFH) ? FFFFH : TMP[127:112];

```

Intel C/C++ Compiler Intrinsic Equivalent

```
PACKUSDW    __m128i _mm_packus_epi32(__m128i m1, __m128i m2);
```

Flags Affected

None

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0): | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.SSE4_1(ECX bit 19) = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.SSE4_1(ECX bit 19) = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|--------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
|--------|---|

INSTRUCTION SET REFERENCE, N-Z

| | |
|------------------|--|
| | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. |
| | If OSFXSR in CR4 is 0. |
| | If CPUID feature flag ECX.SSE4_1 is 0. |
| | If LOCK prefix is used. |
| | Either the prefix REP (F3h) or REPN (F2H) is used. |

PACKUSWB—Pack with Unsigned Saturation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F 67 /r | PACKUSWB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Converts 4 signed word integers from <i>mm</i> and 4 signed word integers from <i>mm/m64</i> into 8 unsigned byte integers in <i>mm</i> using unsigned saturation. |
| 66 0F 67 /r | PACKUSWB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Converts 8 signed word integers from <i>xmm1</i> and 8 signed word integers from <i>xmm2/m128</i> into 16 unsigned byte integers in <i>xmm1</i> using unsigned saturation. |

Description

Converts 4 or 8 signed word integers from the destination operand (first operand) and 4 or 8 signed word integers from the source operand (second operand) into 8 or 16 unsigned byte integers and stores the result in the destination operand. (See Figure 4-1 for an example of the packing operation.) If a signed word integer value is beyond the range of an unsigned byte integer (that is, greater than FFH or less than 00H), the saturated unsigned byte integer value of FFH or 00H, respectively, is stored in the destination.

The PACKUSWB instruction operates on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PACKUSWB instruction with 64-bit operands:

```

DEST[7:0] ← SaturateSignedWordToUnsignedByte DEST[15:0];
DEST[15:8] ← SaturateSignedWordToUnsignedByte DEST[31:16];
DEST[23:16] ← SaturateSignedWordToUnsignedByte DEST[47:32];
DEST[31:24] ← SaturateSignedWordToUnsignedByte DEST[63:48];
DEST[39:32] ← SaturateSignedWordToUnsignedByte SRC[15:0];
DEST[47:40] ← SaturateSignedWordToUnsignedByte SRC[31:16];
DEST[55:48] ← SaturateSignedWordToUnsignedByte SRC[47:32];
DEST[63:56] ← SaturateSignedWordToUnsignedByte SRC[63:48];

```

PACKUSWB instruction with 128-bit operands:

DEST[7:0] ← SaturateSignedWordToUnsignedByte (DEST[15:0]);
 DEST[15:8] ← SaturateSignedWordToUnsignedByte (DEST[31:16]);
 DEST[23:16] ← SaturateSignedWordToUnsignedByte (DEST[47:32]);
 DEST[31:24] ← SaturateSignedWordToUnsignedByte (DEST[63:48]);
 DEST[39:32] ← SaturateSignedWordToUnsignedByte (DEST[79:64]);
 DEST[47:40] ← SaturateSignedWordToUnsignedByte (DEST[95:80]);
 DEST[55:48] ← SaturateSignedWordToUnsignedByte (DEST[111:96]);
 DEST[63:56] ← SaturateSignedWordToUnsignedByte (DEST[127:112]);
 DEST[71:64] ← SaturateSignedWordToUnsignedByte (SRC[15:0]);
 DEST[79:72] ← SaturateSignedWordToUnsignedByte (SRC[31:16]);
 DEST[87:80] ← SaturateSignedWordToUnsignedByte (SRC[47:32]);
 DEST[95:88] ← SaturateSignedWordToUnsignedByte (SRC[63:48]);
 DEST[103:96] ← SaturateSignedWordToUnsignedByte (SRC[79:64]);
 DEST[111:104] ← SaturateSignedWordToUnsignedByte (SRC[95:80]);
 DEST[119:112] ← SaturateSignedWordToUnsignedByte (SRC[111:96]);
 DEST[127:120] ← SaturateSignedWordToUnsignedByte (SRC[127:112]);

Intel C/C++ Compiler Intrinsic Equivalent

PACKUSWB __m64 _mm_packs_pu16(__m64 m1, __m64 m2)

PACKUSWB __m128i _mm_packs_epu16(__m128i m1, __m128i m2)

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | <p>If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.</p> |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | <p>If CR0.EM[bit 2] = 1.</p> <p>128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.</p> <p>If the LOCK prefix is used.</p> |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

If any part of the operand lies outside of the effective address space from 0 to FFFFH.

#UD If CR0.EM[bit 2] = 1.

128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

(128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.

(128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

INSTRUCTION SET REFERENCE, N-Z

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PADDB/PADDW/PADD—Add Packed Integers

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|---|-------------|-----------------|--|
| 0F FC /r | PADDB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed byte integers from <i>mm/m64</i> and <i>mm</i> . |
| 66 0F FC /r | PADDB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed byte integers from <i>xmm2/m128</i> and <i>xmm1</i> . |
| 0F FD /r | PADDW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed word integers from <i>mm/m64</i> and <i>mm</i> . |
| 66 0F FD /r | PADDW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed word integers from <i>xmm2/m128</i> and <i>xmm1</i> . |
| 0F FE /r | PADD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed doubleword integers from <i>mm/m64</i> and <i>mm</i> . |
| 66 0F FE /r | PADD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed doubleword integers from <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a SIMD add of the packed integers from the source operand (second operand) and the destination operand (first operand), and stores the packed integer results in the destination operand. See Figure 9-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD operation. Overflow is handled with wraparound, as described in the following paragraphs.

These instructions can operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

The PADDB instruction adds packed byte integers. When an individual result is too large to be represented in 8 bits (overflow), the result is wrapped around and the low 8 bits are written to the destination operand (that is, the carry is ignored).

The PADDW instruction adds packed word integers. When an individual result is too large to be represented in 16 bits (overflow), the result is wrapped around and the low 16 bits are written to the destination operand.

The PADD instruction adds packed doubleword integers. When an individual result is too large to be represented in 32 bits (overflow), the result is wrapped around and the low 32 bits are written to the destination operand.

Note that the PADDB, PADDW, and PADD instructions can operate on either unsigned or signed (two's complement notation) packed integers; however, it does not set bits in the EFLAGS register to indicate overflow and/or a carry. To prevent

undetected overflow conditions, software must control the ranges of values operated on.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PADDB instruction with 64-bit operands:

$DEST[7:0] \leftarrow DEST[7:0] + SRC[7:0];$
 (* Repeat add operation for 2nd through 7th byte *)
 $DEST[63:56] \leftarrow DEST[63:56] + SRC[63:56];$

PADDB instruction with 128-bit operands:

$DEST[7:0] \leftarrow DEST[7:0] + SRC[7:0];$
 (* Repeat add operation for 2nd through 14th byte *)
 $DEST[127:120] \leftarrow DEST[111:120] + SRC[127:120];$

PADDW instruction with 64-bit operands:

$DEST[15:0] \leftarrow DEST[15:0] + SRC[15:0];$
 (* Repeat add operation for 2nd and 3th word *)
 $DEST[63:48] \leftarrow DEST[63:48] + SRC[63:48];$

PADDW instruction with 128-bit operands:

$DEST[15:0] \leftarrow DEST[15:0] + SRC[15:0];$
 (* Repeat add operation for 2nd through 7th word *)
 $DEST[127:112] \leftarrow DEST[127:112] + SRC[127:112];$

PADD instruction with 64-bit operands:

$DEST[31:0] \leftarrow DEST[31:0] + SRC[31:0];$
 $DEST[63:32] \leftarrow DEST[63:32] + SRC[63:32];$

PADD instruction with 128-bit operands:

$DEST[31:0] \leftarrow DEST[31:0] + SRC[31:0];$
 (* Repeat add operation for 2nd and 3th doubleword *)
 $DEST[127:96] \leftarrow DEST[127:96] + SRC[127:96];$

Intel C/C++ Compiler Intrinsic Equivalents

PADDB `__m64 _mm_add_pi8(__m64 m1, __m64 m2)`
 PADDB `__m128i _mm_add_epi8 (__m128ia, __m128ib)`
 PADDW `__m64 _mm_add_pi16(__m64 m1, __m64 m2)`
 PADDW `__m128i _mm_add_epi16 (__m128i a, __m128i b)`
 PADD `__m64 _mm_add_pi32(__m64 m1, __m64 m2)`
 PADD `__m128i _mm_add_epi32 (__m128i a, __m128i b)`

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.
(128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.
(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
(128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.
If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PADDQ—Add Packed Quadword Integers

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|---|-------------|-----------------|--|
| 0F D4 /r | PADDQ <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Add quadword integer <i>mm2/m64</i> to <i>mm1</i> . |
| 66 0F D4 /r | PADDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed quadword integers <i>xmm2/m128</i> to <i>xmm1</i> . |

Description

Adds the first operand (destination operand) to the second operand (source operand) and stores the result in the destination operand. The source operand can be a quadword integer stored in an MMX technology register or a 64-bit memory location, or it can be two packed quadword integers stored in an XMM register or an 128-bit memory location. The destination operand can be a quadword integer stored in an MMX technology register or two packed quadword integers stored in an XMM register. When packed quadword operands are used, a SIMD add is performed. When a quadword result is too large to be represented in 64 bits (overflow), the result is wrapped around and the low 64 bits are written to the destination element (that is, the carry is ignored).

Note that the PADDQ instruction can operate on either unsigned or signed (two's complement notation) integers; however, it does not set bits in the EFLAGS register to indicate overflow and/or a carry. To prevent undetected overflow conditions, software must control the ranges of the values operated on.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PADDQ instruction with 64-Bit operands:

$$\text{DEST}[63:0] \leftarrow \text{DEST}[63:0] + \text{SRC}[63:0];$$

PADDQ instruction with 128-Bit operands:

$$\begin{aligned} \text{DEST}[63:0] &\leftarrow \text{DEST}[63:0] + \text{SRC}[63:0]; \\ \text{DEST}[127:64] &\leftarrow \text{DEST}[127:64] + \text{SRC}[127:64]; \end{aligned}$$

Intel C/C++ Compiler Intrinsic Equivalents

PADDQ `__m64 _mm_add_si64 (__m64 a, __m64 b)`

PADDQ `__m128i _mm_add_epi64 (__m128i a, __m128i b)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PADDSB/PADDSW—Add Packed Signed Integers with Signed Saturation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|---|
| 0F EC /r | PADDSB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed signed byte integers from <i>mm/m64</i> and <i>mm</i> and saturate the results. |
| 66 0F EC /r | PADDSB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed signed byte integers from <i>xmm2/m128</i> and <i>xmm1</i> saturate the results. |
| 0F ED /r | PADDSW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed signed word integers from <i>mm/m64</i> and <i>mm</i> and saturate the results. |
| 66 0F ED /r | PADDSW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed signed word integers from <i>xmm2/m128</i> and <i>xmm1</i> and saturate the results. |

Description

Performs a SIMD add of the packed signed integers from the source operand (second operand) and the destination operand (first operand), and stores the packed integer results in the destination operand. See Figure 9-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD operation. Overflow is handled with signed saturation, as described in the following paragraphs.

These instructions can operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

The PADDSB instruction adds packed signed byte integers. When an individual byte result is beyond the range of a signed byte integer (that is, greater than 7FH or less than 80H), the saturated value of 7FH or 80H, respectively, is written to the destination operand.

The PADDSW instruction adds packed signed word integers. When an individual word result is beyond the range of a signed word integer (that is, greater than 7FFFH or less than 8000H), the saturated value of 7FFFH or 8000H, respectively, is written to the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PADDSB instruction with 64-bit operands:

```
DEST[7:0] ← SaturateToSignedByte(DEST[7:0] + SRC[7:0]);
(* Repeat add operation for 2nd through 7th bytes *)
DEST[63:56] ← SaturateToSignedByte(DEST[63:56] + SRC[63:56]);
```

PADDSB instruction with 128-bit operands:

```
DEST[7:0] ← SaturateToSignedByte (DEST[7:0] + SRC[7:0]);
(* Repeat add operation for 2nd through 14th bytes *)
DEST[127:120] ← SaturateToSignedByte (DEST[111:120] + SRC[127:120]);
```

PADDSW instruction with 64-bit operands

```
DEST[15:0] ← SaturateToSignedWord(DEST[15:0] + SRC[15:0] );
(* Repeat add operation for 2nd and 7th words *)
DEST[63:48] ← SaturateToSignedWord(DEST[63:48] + SRC[63:48] );
```

PADDSW instruction with 128-bit operands

```
DEST[15:0] ← SaturateToSignedWord (DEST[15:0] + SRC[15:0]);
(* Repeat add operation for 2nd through 7th words *)
DEST[127:112] ← SaturateToSignedWord (DEST[127:112] + SRC[127:112]);
```

Intel C/C++ Compiler Intrinsic Equivalents

```
PADDSB   __m64 _mm_adds_pi8(__m64 m1, __m64 m2)
PADDSB   __m128i _mm_adds_epi8 ( __m128i a, __m128i b)
PADDSW   __m64 _mm_adds_pi16(__m64 m1, __m64 m2)
PADDSW   __m128i _mm_adds_epi16 ( __m128i a, __m128i b)
```

Flags Affected

None.

Protected Mode Exceptions

| | |
|--------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. |

| | |
|-----------------|---|
| | If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |

| | |
|------------------|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PADDUSB/PADDUSW—Add Packed Unsigned Integers with Unsigned Saturation

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|---|-------------|-----------------|--|
| 0F DC /r | PADDUSB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed unsigned byte integers from <i>mm/m64</i> and <i>mm</i> and saturate the results. |
| 66 0F DC /r | PADDUSB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed unsigned byte integers from <i>xmm2/m128</i> and <i>xmm1</i> saturate the results. |
| 0F DD /r | PADDUSW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Add packed unsigned word integers from <i>mm/m64</i> and <i>mm</i> and saturate the results. |
| 66 0F DD /r | PADDUSW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Add packed unsigned word integers from <i>xmm2/m128</i> to <i>xmm1</i> and saturate the results. |

Description

Performs a SIMD add of the packed unsigned integers from the source operand (second operand) and the destination operand (first operand), and stores the packed integer results in the destination operand. See Figure 9-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD operation. Overflow is handled with unsigned saturation, as described in the following paragraphs.

These instructions can operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

The PADDUSB instruction adds packed unsigned byte integers. When an individual byte result is beyond the range of an unsigned byte integer (that is, greater than FFH), the saturated value of FFH is written to the destination operand.

The PADDUSW instruction adds packed unsigned word integers. When an individual word result is beyond the range of an unsigned word integer (that is, greater than FFFFH), the saturated value of FFFFH is written to the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PADDUSB instruction with 64-bit operands:

DEST[7:0] ← SaturateToUnsignedByte(DEST[7:0] + SRC[7:0]);
 (* Repeat add operation for 2nd through 7th bytes *)
 DEST[63:56] ← SaturateToUnsignedByte(DEST[63:56] + SRC[63:56])

PADDUSB instruction with 128-bit operands:

DEST[7:0] ← SaturateToUnsignedByte (DEST[7:0] + SRC[7:0]);
 (* Repeat add operation for 2nd through 14th bytes *)
 DEST[127:120] ← SaturateToUnSignedByte (DEST[127:120] + SRC[127:120]);

PADDUSW instruction with 64-bit operands:

DEST[15:0] ← SaturateToUnsignedWord(DEST[15:0] + SRC[15:0]);
 (* Repeat add operation for 2nd and 3rd words *)
 DEST[63:48] ← SaturateToUnsignedWord(DEST[63:48] + SRC[63:48]);

PADDUSW instruction with 128-bit operands:

DEST[15:0] ← SaturateToUnsignedWord (DEST[15:0] + SRC[15:0]);
 (* Repeat add operation for 2nd through 7th words *)
 DEST[127:112] ← SaturateToUnSignedWord (DEST[127:112] + SRC[127:112]);

Intel C/C++ Compiler Intrinsic Equivalents

PADDUSB __m64 _mm_adds_pu8(__m64 m1, __m64 m2)
 PADDUSW __m64 _mm_adds_pu16(__m64 m1, __m64 m2)
 PADDUSB __m128i _mm_adds_epu8 (__m128i a, __m128i b)
 PADDUSW __m128i _mm_adds_epu16 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

| | |
|------------------|---|
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|------------------|--|
| #PF (fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PALIGNR — Packed Align Right

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|-------------------------------|-------------|------------------|---|
| 0F 3A 0F | PALIGNR mm1, mm2/m64, imm8 | Valid | Valid | Concatenate destination and source operands, extract byte-aligned result shifted to the right by constant value in imm8 into mm1. |
| 66 0F 3A 0F | PALIGNR xmm1, xmm2/m128, imm8 | Valid | Valid | Concatenate destination and source operands, extract byte-aligned result shifted to the right by constant value in imm8 into xmm1 |

Description

PALIGNR concatenates the destination operand (the first operand) and the source operand (the second operand) into an intermediate composite, shifts the composite at byte granularity to the right by a constant immediate, and extracts the right-aligned result into the destination. The first and the second operands can be an MMX or an XMM register. The immediate value is considered unsigned. Immediate shift counts larger than the 2L (i.e. 32 for 128-bit operands, or 16 for 64-bit operands) produce a zero result. Both operands can be MMX register or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PALIGNR with 64-bit operands:

```
temp1[127:0] = CONCATENATE(DEST,SRC)>>(imm8*8)
DEST[63:0] = temp1[63:0]
```

PALIGNR with 128-bit operands:

```
temp1[255:0] = CONCATENATE(DEST,SRC)>>(imm8*8)
DEST[127:0] = temp1[127:0]
```

Intel C/C++ Compiler Intrinsic Equivalents

PALIGNR `__m64 __mm_alignr_pi8 (__m64 a, __m64 b, int n)`

PALIGNR `__m128i __mm_alignr_epi8 (__m128i a, __m128i b, int n)`

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS or GS segments. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PAND—Logical AND

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|-----------------------------|-------------|------------------|---|
| 0F DB /r | PAND <i>mm, mm/m64</i> | Valid | Valid | Bitwise AND <i>mm/m64</i> and <i>mm</i> . |
| 66 0F DB /r | PAND <i>xmm1, xmm2/m128</i> | Valid | Valid | Bitwise AND of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical AND operation on the source operand (second operand) and the destination operand (first operand) and stores the result in the destination operand. The source operand can be an MMX technology register or a 64-bit memory location or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. Each bit of the result is set to 1 if the corresponding bits of the first and second operands are 1; otherwise, it is set to 0.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST ← (DEST AND SRC);

Intel C/C++ Compiler Intrinsic Equivalent

PAND `__m64 _mm_and_si64 (__m64 m1, __m64 m2)`

PAND `__m128i _mm_and_si128 (__m128i a, __m128i b)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PANDN—Logical AND NOT

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--------------------------------------|-------------|-----------------|---|
| 0F DF /r | PANDN <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Bitwise AND NOT of <i>mm/m64</i> and <i>mm</i> . |
| 66 0F DF /r | PANDN <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Bitwise AND NOT of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical NOT of the destination operand (first operand), then performs a bitwise logical AND of the source operand (second operand) and the inverted destination operand. The result is stored in the destination operand. The source operand can be an MMX technology register or a 64-bit memory location or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. Each bit of the result is set to 1 if the corresponding bit in the first operand is 0 and the corresponding bit in the second operand is 1; otherwise, it is set to 0.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST ← ((NOT DEST) AND SRC);

Intel C/C++ Compiler Intrinsic Equivalent

PANDN `__m64 _mm_andnot_si64 (__m64 m1, __m64 m2)`

PANDN `__m128i _mm_andnot_si128 (__m128i a, __m128i b)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0)

If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.

(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PAUSE—Spin Loop Hint

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|---|
| F3 90 | PAUSE | Valid | Valid | Gives hint to processor that improves performance of spin-wait loops. |

Description

Improves the performance of spin-wait loops. When executing a “spin-wait loop,” a Pentium 4 or Intel Xeon processor suffers a severe performance penalty when exiting the loop because it detects a possible memory order violation. The PAUSE instruction provides a hint to the processor that the code sequence is a spin-wait loop. The processor uses this hint to avoid the memory order violation in most situations, which greatly improves processor performance. For this reason, it is recommended that a PAUSE instruction be placed in all spin-wait loops.

An additional function of the PAUSE instruction is to reduce the power consumed by a Pentium 4 processor while executing a spin loop. The Pentium 4 processor can execute a spin-wait loop extremely quickly, causing the processor to consume a lot of power while it waits for the resource it is spinning on to become available. Inserting a pause instruction in a spin-wait loop greatly reduces the processor's power consumption.

This instruction was introduced in the Pentium 4 processors, but is backward compatible with all IA-32 processors. In earlier IA-32 processors, the PAUSE instruction operates like a NOP instruction. The Pentium 4 and Intel Xeon processors implement the PAUSE instruction as a pre-defined delay. The delay is finite and can be zero for some processors. This instruction does not change the architectural state of the processor (that is, it performs essentially a delaying no-op operation).

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

Execute_Next_Instruction(Delay);

Numeric Exceptions

None.

Exceptions (All Operating Modes)

#UD If the LOCK prefix is used.

PAVGB/PAVGW—Average Packed Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------------|---|-------------|------------------|--|
| 0F E0 /r | PAVGB <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Average packed unsigned byte integers from <i>mm2/m64</i> and <i>mm1</i> with rounding. |
| 66 0F E0, /r | PAVGB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Average packed unsigned byte integers from <i>xmm2/m128</i> and <i>xmm1</i> with rounding. |
| 0F E3 /r | PAVGW <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Average packed unsigned word integers from <i>mm2/m64</i> and <i>mm1</i> with rounding. |
| 66 0F E3 /r | PAVGW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Average packed unsigned word integers from <i>xmm2/m128</i> and <i>xmm1</i> with rounding. |

Description

Performs a SIMD average of the packed unsigned integers from the source operand (second operand) and the destination operand (first operand), and stores the results in the destination operand. For each corresponding pair of data elements in the first and second operands, the elements are added together, a 1 is added to the temporary sum, and that result is shifted right one bit position. The source operand can be an MMX technology register or a 64-bit memory location or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

The PAVGB instruction operates on packed unsigned bytes and the PAVGW instruction operates on packed unsigned words.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PAVGB instruction with 64-bit operands:

$$\text{DEST}[7:0] \leftarrow (\text{SRC}[7:0] + \text{DEST}[7:0] + 1) \gg 1; \text{ (* Temp sum before shifting is 9 bits *)}$$

(* Repeat operation performed for bytes 2 through 6 *)

$$\text{DEST}[63:56] \leftarrow (\text{SRC}[63:56] + \text{DEST}[63:56] + 1) \gg 1;$$

PAVGW instruction with 64-bit operands:

$$\text{DEST}[15:0] \leftarrow (\text{SRC}[15:0] + \text{DEST}[15:0] + 1) \gg 1; \text{ (* Temp sum before shifting is 17 bits *)}$$

(* Repeat operation performed for words 2 and 3 *)

$$\text{DEST}[63:48] \leftarrow (\text{SRC}[63:48] + \text{DEST}[63:48] + 1) \gg 1;$$

PAVGB instruction with 128-bit operands:

$$\text{DEST}[7:0] \leftarrow (\text{SRC}[7:0] + \text{DEST}[7:0] + 1) \gg 1; \text{ (* Temp sum before shifting is 9 bits *)}$$

(* Repeat operation performed for bytes 2 through 14 *)

$$\text{DEST}[127:120] \leftarrow (\text{SRC}[127:120] + \text{DEST}[127:120] + 1) \gg 1;$$

PAVGW instruction with 128-bit operands:

$$\text{DEST}[15:0] \leftarrow (\text{SRC}[15:0] + \text{DEST}[15:0] + 1) \gg 1; \text{ (* Temp sum before shifting is 17 bits *)}$$

(* Repeat operation performed for words 2 through 6 *)

$$\text{DEST}[127:112] \leftarrow (\text{SRC}[127:112] + \text{DEST}[127:112] + 1) \gg 1;$$

Intel C/C++ Compiler Intrinsic Equivalent

PAVGB `__m64_mm_avg_pu8 (__m64 a, __m64 b)`
 PAVGW `__m64_mm_avg_pu16 (__m64 a, __m64 b)`
 PAVGB `__m128i_mm_avg_epu8 (__m128i a, __m128i b)`
 PAVGW `__m128i_mm_avg_epu16 (__m128i a, __m128i b)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
If any part of the operand lies outside of the effective address space from 0 to FFFFH.

#UD If CR0.EM[bit 2] = 1.
(128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.
(128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.
(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
(128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.
If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PBLENDVB – Variable Blend Packed Bytes

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------|--|-------------|------------------|---|
| 66 OF 38 10 /r | PBLENDVB <i>xmm1</i> , <i>xmm2/m128</i> , <XMM0> | Valid | Valid | Select byte values from <i>xmm1</i> and <i>xmm2/m128</i> from mask specified in the high bit of each byte in XMM0 and store the values into <i>xmm1</i> . |

Description

Conditionally copies byte elements from the source operand (second operand) to the destination operand (first operand) depending on mask bits defined in the implicit third register argument, XMM0. The mask bits are the most significant bit in each byte element of the XMM0 register.

If a mask bit is "1", then the corresponding byte element in the source operand is copied to the destination, else the byte element in the destination operand is left unchanged.

The register assignment of the implicit third operand is defined to be the architectural register XMM0.

Operation

```

MASK ← XMM0;
IF (MASK[7] == 1)
    THEN DEST[7:0] ← SRC[7:0];
    ELSE DEST[7:0] ← DEST[7:0]; FI;
IF (MASK[15] == 1)
    THEN DEST[15:8] ← SRC[15:8];
    ELSE DEST[15:8] ← DEST[15:8]; FI;
IF (MASK[23] == 1)
    THEN DEST[23:16] ← SRC[23:16];
    ELSE DEST[23:16] ← DEST[23:16]; FI;
IF (MASK[31] == 1)
    THEN DEST[31:24] ← SRC[31:24];
    ELSE DEST[31:24] ← DEST[31:24]; FI;
IF (MASK[39] == 1)
    THEN DEST[39:32] ← SRC[39:32];
    ELSE DEST[39:32] ← DEST[39:32]; FI;
IF (MASK[47] == 1)
    THEN DEST[47:40] ← SRC[47:40];
    ELSE DEST[47:40] ← DEST[47:40]; FI;

```

```

IF (MASK[55] == 1)
    THEN DEST[55:48] ← SRC[55:48]
    ELSE DEST[55:48] ← DEST[55:48]; FI;
IF (MASK[63] == 1)
    THEN DEST[63:56] ← SRC[63:56]
    ELSE DEST[63:56] ← DEST[63:56]; FI;
IF (MASK[71] == 1)
    THEN DEST[71:64] ← SRC[71:64]
    ELSE DEST[71:64] ← DEST[71:64]; FI;
IF (MASK[79] == 1)
    THEN DEST[79:72] ← SRC[79:72]
    ELSE DEST[79:72] ← DEST[79:72]; FI;
IF (MASK[87] == 1)
    THEN DEST[87:80] ← SRC[87:80]
    ELSE DEST[87:80] ← DEST[87:80]; FI;
IF (MASK[95] == 1)
    THEN DEST[95:88] ← SRC[95:88]
    ELSE DEST[95:88] ← DEST[95:88]; FI;
IF (MASK[103] == 1)
    THEN DEST[103:96] ← SRC[103:96]
    ELSE DEST[103:96] ← DEST[103:96]; FI;
IF (MASK[111] == 1)
    THEN DEST[111:104] ← SRC[111:104]
    ELSE DEST[111:104] ← DEST[111:104]; FI;
IF (MASK[119] == 1)
    THEN DEST[119:112] ← SRC[119:112]
    ELSE DEST[119:112] ← DEST[119:112]; FI;
IF (MASK[127] == 1)
    THEN DEST[127:120] ← SRC[127:120]
    ELSE DEST[127:120] ← DEST[127:120]; FI;

```

Intel C/C++ Compiler Intrinsic Equivalent

PBLENDVB `__m128i _mm_blendv_epi8 (__m128i v1, __m128i v2, __m128i mask);`

Flags Affected

None

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.

| | |
|-----------------|--|
| | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If not aligned on 16-byte boundary, regardless of segment |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. |

If CPUID feature flag ECX.SSE4_1 is 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

PBLENDW — Blend Packed Words

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------------|---|-------------|------------------|---|
| 66 OF 3A OE /r ib | PBLENDW <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Select words from <i>xmm1</i> and <i>xmm2/m128</i> from mask specified in <i>imm8</i> and store the values into <i>xmm1</i> . |

Description

Conditionally copies word elements from the source operand (second operand) to the destination operand (first operand) depending on the immediate byte (third operand). Each bit of Imm8 correspond to a word element.

If a bit is "1", then the corresponding word element in the source operand is copied to the destination, else the word element in the destination operand is left unchanged.

Operation

```

IF (imm8[0] == 1)
    THEN DEST[15:0] ← SRC[15:0];
    ELSE DEST[15:0] ← DEST[15:0]; FI;
IF (imm8[1] == 1)
    THEN DEST[31:16] ← SRC[31:16];
    ELSE DEST[31:16] ← DEST[31:16]; FI;
IF (imm8[2] == 1)
    THEN DEST[47:32] ← SRC[47:32];
    ELSE DEST[47:32] ← DEST[47:32]; FI;
IF (imm8[3] == 1)
    THEN DEST[63:48] ← SRC[63:48];
    ELSE DEST[63:48] ← DEST[63:48]; FI;
IF (imm8[4] == 1)
    THEN DEST[79:64] ← SRC[79:64];
    ELSE DEST[79:64] ← DEST[79:64]; FI;
IF (imm8[5] == 1)
    THEN DEST[95:80] ← SRC[95:80];
    ELSE DEST[95:80] ← DEST[95:80]; FI;
IF (imm8[6] == 1)
    THEN DEST[111:96] ← SRC[111:96];
    ELSE DEST[111:96] ← DEST[111:96]; FI;
IF (imm8[7] == 1)

```

```
THEN DEST[127:112] ← SRC[127:112];
ELSE DEST[127:112] ← DEST[127:112]; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PBLENDW      __m128i_mm_blend_epi16 (__m128i v1, __m128i v2, const int mask);
```

Flags Affected

None

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) For an illegal address in the SS segment.

#PF(fault-code) For a page fault.

#NM If CR0.TS[bit 3] = 1.

#UD If CR0.EM[bit 2] = 1.
If CR4.OSFXSR[bit 9] = 0.
If CPUID.01H:ECX.SSE4_1[bit 19] = 0.
If LOCK prefix is used.
Either the prefix REP (F3h) or REPN (F2H) is used.

Real Mode Exceptions

#GP(0) if any part of the operand lies outside of the effective address space from 0 to 0FFFFH.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#NM If CR0.TS[bit 3] = 1.

#UD If CR0.EM[bit 2] = 1.
If CR4.OSFXSR[bit 9] = 0.
If CPUID.01H:ECX.SSE4_1[bit 19] = 0.
If LOCK prefix is used.
Either the prefix REP (F3h) or REPN (F2H) is used.

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PCMPEQB/PCMPEQW/PCMPEQD— Compare Packed Data for Equal

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|--|
| 0F 74 /r | PCMPEQB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Compare packed bytes in <i>mm/m64</i> and <i>mm</i> for equality. |
| 66 0F 74 /r | PCMPEQB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed bytes in <i>xmm2/m128</i> and <i>xmm1</i> for equality. |
| 0F 75 /r | PCMPEQW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Compare packed words in <i>mm/m64</i> and <i>mm</i> for equality. |
| 66 0F 75 /r | PCMPEQW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed words in <i>xmm2/m128</i> and <i>xmm1</i> for equality. |
| 0F 76 /r | PCMPEQD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Compare packed doublewords in <i>mm/m64</i> and <i>mm</i> for equality. |
| 66 0F 76 /r | PCMPEQD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed doublewords in <i>xmm2/m128</i> and <i>xmm1</i> for equality. |

Description

Performs a SIMD compare for equality of the packed bytes, words, or doublewords in the destination operand (first operand) and the source operand (second operand). If a pair of data elements is equal, the corresponding data element in the destination operand is set to all 1s; otherwise, it is set to all 0s. The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

The PCMPEQB instruction compares the corresponding bytes in the destination and source operands; the PCMPEQW instruction compares the corresponding words in the destination and source operands; and the PCMPEQD instruction compares the corresponding doublewords in the destination and source operands.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PCMPEQB instruction with 64-bit operands:

```
IF DEST[7:0] = SRC[7:0]
    THEN DEST[7:0] ← FFH;
    ELSE DEST[7:0] ← 0; FI;
```

(* Continue comparison of 2nd through 7th bytes in DEST and SRC *)

```

IF DEST[63:56] = SRC[63:56]
  THEN DEST[63:56] ← FFH;
  ELSE DEST[63:56] ← 0; FI;

```

PCMPEQB instruction with 128-bit operands:

```

IF DEST[7:0] = SRC[7:0]
  THEN DEST[7:0] ← FFH;
  ELSE DEST[7:0] ← 0; FI;
(* Continue comparison of 2nd through 15th bytes in DEST and SRC *)
IF DEST[127:120] = SRC[127:120]
  THEN DEST[127:120] ← FFH;
  ELSE DEST[127:120] ← 0; FI;

```

PCMPEQW instruction with 64-bit operands:

```

IF DEST[15:0] = SRC[15:0]
  THEN DEST[15:0] ← FFFFH;
  ELSE DEST[15:0] ← 0; FI;
(* Continue comparison of 2nd and 3rd words in DEST and SRC *)
IF DEST[63:48] = SRC[63:48]
  THEN DEST[63:48] ← FFFFH;
  ELSE DEST[63:48] ← 0; FI;

```

PCMPEQW instruction with 128-bit operands:

```

IF DEST[15:0] = SRC[15:0]
  THEN DEST[15:0] ← FFFFH;
  ELSE DEST[15:0] ← 0; FI;
(* Continue comparison of 2nd through 7th words in DEST and SRC *)
IF DEST[127:112] = SRC[127:112]
  THEN DEST[127:112] ← FFFFH;
  ELSE DEST[127:112] ← 0; FI;

```

PCMPEQD instruction with 64-bit operands:

```

IF DEST[31:0] = SRC[31:0]
  THEN DEST[31:0] ← FFFFFFFFH;
  ELSE DEST[31:0] ← 0; FI;
IF DEST[63:32] = SRC[63:32]
  THEN DEST[63:32] ← FFFFFFFFH;
  ELSE DEST[63:32] ← 0; FI;

```

PCMPEQD instruction with 128-bit operands:

```

IF DEST[31:0] = SRC[31:0]
  THEN DEST[31:0] ← FFFFFFFFH;
  ELSE DEST[31:0] ← 0; FI;
(* Continue comparison of 2nd and 3rd doublewords in DEST and SRC *)
IF DEST[127:96] = SRC[127:96]

```

THEN DEST[127:96] ← FFFFFFFFH;
 ELSE DEST[127:96] ← 0; FI;

Intel C/C++ Compiler Intrinsic Equivalents

PCMPEQB __m64 __mm_cmpeq_pi8 (__m64 m1, __m64 m2)
 PCMPEQW __m64 __mm_cmpeq_pi16 (__m64 m1, __m64 m2)
 PCMPEQD __m64 __mm_cmpeq_pi32 (__m64 m1, __m64 m2)
 PCMPEQB __m128i __mm_cmpeq_epi8 (__m128i a, __m128i b)
 PCMPEQW __m128i __mm_cmpeq_epi16 (__m128i a, __m128i b)
 PCMPEQD __m128i __mm_cmpeq_epi32 (__m128i a, __m128i b)

Flags Affected

None.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
|-----|---|

| | |
|-----|---|
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PCMPEQQ — Compare Packed Qword Data for Equal

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|-------------------|---|-------------|------------------|---|
| 66 OF 38 29 /r | PCMPEQQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed qwords in <i>xmm2/m128</i> and <i>xmm1</i> for equality. |

Description

Performs an SIMD compare for equality of the packed quadwords in the destination operand (first operand) and the source operand (second operand). If a pair of data elements is equal, the corresponding data element in the destination is set to all 1s; otherwise, it is set to 0s.

Operation

```
IF (DEST[63:0] = SRC[63:0])
    THEN DEST[63:0] ← FFFFFFFFFFFFFFFFH;
    ELSE DEST[63:0] ← 0; FI;
IF (DEST[127:64] = SRC[127:64])
    THEN DEST[127:64] ← FFFFFFFFFFFFFFFFH;
    ELSE DEST[127:64] ← 0; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

PCMPEQQ `__m128i __mm_cmpeq_epi64(__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

| | |
|------------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. |

If CPUID.01H: ECX.SSE4_1[bit 19] = 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

Real Mode Exceptions

#GP(0) if any part of the operand lies outside of the effective address space from 0 to 0FFFFH.

If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#NM If CR0.TS[bit 3] = 1.

#UD If CR0.EM[bit 2] = 1.

If CR4.OSFXSR[bit 9] = 0.

If CPUID.01H: ECX.SSE4_1[bit 19] = 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

#GP(0) If the memory address is in a non-canonical form.

If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#PF(fault-code) For a page fault.

#NM If TS in CR0 is set.

#UD If EM in CR0 is set.

If OSFXSR in CR4 is 0.

If CPUID feature flag ECX.SSE4_1 is 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

PCMPESTRI – Packed Compare Explicit Length Strings, Return Index

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------------|---|-------------|------------------|---|
| 66 0F 3A 61 <i>/r imm8</i> | PCMPESTRI <i>xmm1,</i> <i>xmm2/m128,</i> <i>imm8</i> | Valid | Valid | Perform a packed comparison of string data with explicit lengths, generating an index, and storing the result in ECX. |

Description

The instruction compares and processes data from two string fragments based on the encoded value in the Imm8 Control Byte (see Section 3.1.2, “Imm8 Control Byte Operation for PCMPESTRI / PCMPESTRM / PCMPISTRI / PCMPISTRM”), and generates an index stored to ECX.

Each string fragment is represented by two values. The first value is an xmm (or possibly m128 for the second operand) which contains the data elements of the string (byte or word data). The second value is stored in EAX (for xmm1) or EDX (for xmm2/m128) and represents the number of bytes/words which are valid for the respective xmm/m128 data.

The length of each input is interpreted as being the absolute-value of the value in EAX (EDX). The absolute-value computation saturates to 16 (for bytes) and 8 (for words), based on the value of imm8[bit3] when the value in EAX (EDX) is greater than 16 (8) or less than -16 (-8).

The comparison and aggregation operations are performed according to the encoded value of Imm8 bit fields (see Section 3.1.2). The index of the first (or last, according to imm8[6]) set bit of IntRes2 (see Section 3.1.2.4) is returned in ECX. If no bits are set in IntRes2, ECX is set to 16 (8).

Note that the Arithmetic Flags are written in a non-standard manner in order to supply the most relevant information:

- CFlag - Reset if IntRes2 is equal to zero, set otherwise
- ZFlag - Set if absolute-value of EDX is < 16 (8), reset otherwise
- SFlag - Set if absolute-value of EAX is < 16 (8), reset otherwise
- OFlag - IntRes2[0]
- AFlag - Reset
- PFlag - Reset

Effective Operand Size

| Operating mode/size | Operand 1 | Operand 2 | Length 1 | Length 2 | Result |
|---------------------|-----------|-----------|----------|----------|--------|
| 16 bit | xmm | xmm/m128 | EAX | EDX | ECX |
| 32 bit | xmm | xmm/m128 | EAX | EDX | ECX |
| 64 bit | xmm | xmm/m128 | EAX | EDX | ECX |
| 64 bit + REX.W | xmm | xmm/m128 | RAX | RDX | RCX |

Intel C/C++ Compiler Intrinsic Equivalent For Returning Index

```
int __mm_cmpestri (__m128i a, int la, __m128i b, int lb, const int mode);
```

Intel C/C++ Compiler Intrinsics For Reading EFlag Results

```
int __mm_cmpestra (__m128i a, int la, __m128i b, int lb, const int mode);
```

```
int __mm_cmpestrc (__m128i a, int la, __m128i b, int lb, const int mode);
```

```
int __mm_cmpestro (__m128i a, int la, __m128i b, int lb, const int mode);
```

```
int __mm_cmpestrs (__m128i a, int la, __m128i b, int lb, const int mode);
```

```
int __mm_cmpestrz (__m128i a, int la, __m128i b, int lb, const int mode);
```

SIMD Floating-Point Exceptions

N/A.

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments.
- #PF(fault-code) For a page fault.
- #NM If TS in CR0 is set.
- #SS(0) For an illegal address in the SS segment
- #UD If EM in CR0 is set.
- If OSFXSR in CR4 is 0.
- If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0.
- If LOCK prefix is used.
- Either the prefix REP (F3h) or REPN (F2H) is used.

Real-Address Mode Exceptions

- #GP Interrupt 13 If any part of the operand lies outside the effective address space from 0 to FFFFH.

| | |
|-----|--|
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in Real Address Mode

| | |
|-----------------|------------------|
| #PF(fault-code) | For a page fault |
|-----------------|------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PCMPESTRM – Packed Compare Explicit Length Strings, Return Mask

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------------------------|---|-------------|-----------------|--|
| 66 0F 3A 60 <i>/r imm8</i> | PCMPESTRM <i>xmm1,</i> <i>xmm2/m128,</i> <i>imm8</i> | Valid | Valid | Perform a packed comparison of string data with explicit lengths, generating a mask, and storing the result in <i>XMM0</i> |

Description

The instruction compares data from two string fragments based on the encoded value in the *imm8* control byte (see Section 3.1.2, “*Imm8* Control Byte Operation for *PCMPESTRM* / *PCMPESTRM* / *PCMPISTRM* / *PCMPISTRM*”), and generates a mask stored to *XMM0*.

Each string fragment is represented by two values. The first value is an *xmm* (or possibly *m128* for the second operand) which contains the data elements of the string (byte or word data). The second value is stored in *EAX* (for *xmm1*) or *EDX* (for *xmm2/m128*) and represents the number of bytes/words which are valid for the respective *xmm/m128* data.

The length of each input is interpreted as being the absolute-value of the value in *EAX* (*EDX*). The absolute-value computation saturates to 16 (for bytes) and 8 (for words), based on the value of *imm8*[bit3] when the value in *EAX* (*EDX*) is greater than 16 (8) or less than -16 (-8).

The comparison and aggregation operations are performed according to the encoded value of *Imm8* bit fields (see Section 3.1.2). As defined by *imm8*[6], *IntRes2* is then either stored to the least significant bits of *XMM0* (zero extended to 128 bits) or expanded into a byte/word-mask and then stored to *XMM0*.

Note that the Arithmetic Flags are written in a non-standard manner in order to supply the most relevant information:

- CFlag - Reset if *IntRes2* is equal to zero, set otherwise
- ZFlag - Set if absolute-value of *EDX* is < 16 (8), reset otherwise
- SFlag - Set if absolute-value of *EAX* is < 16 (8), reset otherwise
- OFlag - *IntRes2*[0]
- AFlag - Reset
- PFlag - Reset

Effective Operand Size

| Operating mode/size | Operand1 | Operand2 | Length1 | Length2 | Result |
|---------------------|----------|----------|---------|---------|--------|
| 16 bit | xmm | xmm/m128 | EAX | EDX | XMM0 |
| 32 bit | xmm | xmm/m128 | EAX | EDX | XMM0 |
| 64 bit | xmm | xmm/m128 | EAX | EDX | XMM0 |
| 64 bit + REX.W | xmm | xmm/m128 | RAX | RDX | XMM0 |

Intel C/C++ Compiler Intrinsic Equivalent For Returning Mask

`__m128i _mm_cmpestrm (__m128i a, int la, __m128i b, int lb, const int mode);`

Intel C/C++ Compiler Intrinsics For Reading EFlag Results

`int _mm_cmpestra (__m128i a, int la, __m128i b, int lb, const int mode);`

`int _mm_cmpestrc (__m128i a, int la, __m128i b, int lb, const int mode);`

`int _mm_cmpestro (__m128i a, int la, __m128i b, int lb, const int mode);`

`int _mm_cmpestrs (__m128i a, int la, __m128i b, int lb, const int mode);`

`int _mm_cmpestrz (__m128i a, int la, __m128i b, int lb, const int mode);`

SIMD Floating-Point Exceptions

N/A.

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments.

#PF(fault-code) For a page fault.

#NM If TS in CR0 is set.

#SS(0) For an illegal address in the SS segment

#UD If EM in CR0 is set.

If OSFXSR in CR4 is 0.

If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2h) is used.

Real-Address Mode Exceptions

#GP Interrupt 13 If any part of the operand lies outside the effective address space from 0 to FFFFH.

#NM If TS in CR0 is set.

#UD If EM in CR0 is set.
 If OSFXSR in CR4 is 0.
 If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0.
 If LOCK prefix is used.
 Either the prefix REP (F3h) or REPN (F2H) is used.

Virtual-8086 Mode Exceptions

Same exceptions as in Real Address Mode

#PF(fault-code) For a page fault

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

#GP(0) If the memory address is in a non-canonical form.
#SS(0) If a memory address referencing the SS segment is in a non-canonical form.
#PF (fault-code) For a page fault.
#NM If TS in CR0 is set.
#UD If EM in CR0 is set.
 If OSFXSR in CR4 is 0.
 If CPUID.01H: ECX.SSE4_2 [Bit 20] = 0.
 If LOCK prefix is used.
 Either the prefix REP (F3h) or REPN (F2H) is used.

PCMPISTRI – Packed Compare Implicit Length Strings, Return Index

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------------------|--|-------------|------------------|---|
| 66 0F 3A 63 /r imm8 | PCMPISTRI <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Perform a packed comparison of string data with implicit lengths, generating an index, and storing the result in ECX. |

Description

The instruction compares data from two strings based on the encoded value in the Imm8 Control Byte (see Section 3.1.2, “Imm8 Control Byte Operation for PCMPSTRM / PCMPSTRM / PCMPISTRI / PCMPISTRM”), and generates an index stored to ECX.

Each string is represented by a single value. The value is an xmm (or possibly m128 for the second operand) which contains the data elements of the string (byte or word data). Each input byte/word is augmented with a valid/invalid tag. A byte/word is considered valid only if it has a lower index than the least significant null byte/word. (The least significant null byte/word is also considered invalid.)

The comparison and aggregation operations are performed according to the encoded value of Imm8 bit fields (see Section 3.1.2). The index of the first (or last, according to imm8[6]) set bit of IntRes2 is returned in ECX. If no bits are set in IntRes2, ECX is set to 16 (8).

Note that the Arithmetic Flags are written in a non-standard manner in order to supply the most relevant information:

CFlag - Reset if IntRes2 is equal to zero, set otherwise

ZFlag - Set if any byte/word of xmm2/mem128 is null, reset otherwise

SFlag - Set if any byte/word of xmm1 is null, reset otherwise

OFlag -IntRes2[0]

AFlag - Reset

PFlag - Reset

Effective Operand Size

| Operating mode/size | Operand1 | Operand2 | Result |
|---------------------|----------|----------|--------|
| 16 bit | xmm | xmm/m128 | ECX |
| 32 bit | xmm | xmm/m128 | ECX |
| 64 bit | xmm | xmm/m128 | ECX |
| 64 bit + REX.W | xmm | xmm/m128 | RCX |

Intel C/C++ Compiler Intrinsic Equivalent For Returning Index

```
int  __mm_cmpistri (__m128i a, __m128i b, const int mode);
```

Intel C/C++ Compiler Intrinsics For Reading EFlag Results

```
int  __mm_cmpistra (__m128i a, __m128i b, const int mode);
```

```
int  __mm_cmpistrc (__m128i a, __m128i b, const int mode);
```

```
int  __mm_cmpistro (__m128i a, __m128i b, const int mode);
```

```
int  __mm_cmpistrs (__m128i a, __m128i b, const int mode);
```

```
int  __mm_cmpistrz (__m128i a, __m128i b, const int mode);
```

SIMD Floating-Point Exceptions

N/A.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #SS(0) | For an illegal address in the SS segment. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | Interrupt 13 If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in Real Address Mode

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PCMPISTRM – Packed Compare Implicit Length Strings, Return Mask

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------------------|---|-------------|------------------|--|
| 66 OF 3A 62 /r imm8 | PCMPISTRM <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Perform a packed comparison of string data with implicit lengths, generating a mask, and storing the result in <i>XMM0</i> . |

Description

The instruction compares data from two strings based on the encoded value in the *imm8* byte (see Section 3.1.2, “Imm8 Control Byte Operation for PCMPSTRM / PCMPISTRM / PCMPISTRM”) generating a mask stored to *XMM0*.

Each string is represented by a single value. The value is an *xmm* (or possibly *m128* for the second operand) which contains the data elements of the string (byte or word data). Each input byte/word is augmented with a valid/invalid tag. A byte/word is considered valid only if it has a lower index than the least significant null byte/word. (The least significant null byte/word is also considered invalid.)

The comparison and aggregation operation are performed according to the encoded value of *Imm8* bit fields (see Section 3.1.2). As defined by *imm8*[6], *IntRes2* is then either stored to the least significant bits of *XMM0* (zero extended to 128 bits) or expanded into a byte/word-mask and then stored to *XMM0*.

Note that the Arithmetic Flags are written in a non-standard manner in order to supply the most relevant information:

CFlag - Reset if *IntRes2* is equal to zero, set otherwise

ZFlag - Set if any byte/word of *xmm2/mem128* is null, reset otherwise

SFlag - Set if any byte/word of *xmm1* is null, reset otherwise

OFlag - *IntRes2*[0]

AFlag - Reset

PFlag - Reset

Effective Operand Size

| Operating mode/size | Operand1 | Operand2 | Result |
|---------------------|------------|-----------------|-------------|
| 16 bit | <i>xmm</i> | <i>xmm/m128</i> | <i>XMM0</i> |
| 32 bit | <i>xmm</i> | <i>xmm/m128</i> | <i>XMM0</i> |
| 64 bit | <i>xmm</i> | <i>xmm/m128</i> | <i>XMM0</i> |
| 64 bit + REX.W | <i>xmm</i> | <i>xmm/m128</i> | <i>XMM0</i> |

Intel C/C++ Compiler Intrinsic Equivalent For Returning Mask

```
__m128i _mm_cmpistrm (__m128i a, __m128i b, const int mode);
```

Intel C/C++ Compiler Intrinsics For Reading EFlag Results

```
int  _mm_cmpistra (__m128i a, __m128i b, const int mode);
int  _mm_cmpistrc (__m128i a, __m128i b, const int mode);
int  _mm_cmpistro (__m128i a, __m128i b, const int mode);
int  _mm_cmpistrs (__m128i a, __m128i b, const int mode);
int  _mm_cmpistrz (__m128i a, __m128i b, const int mode);
```

SIMD Floating-Point Exceptions

N/A.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #SS(0) | For an illegal address in the SS segment |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | Interrupt 13 If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in Real Address Mode

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PCMPGTB/PCMPGTW/PCMPGTD—Compare Packed Signed Integers for Greater Than

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|---|
| 0F 64 /r | PCMPGTB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Compare packed signed byte integers in <i>mm</i> and <i>mm/m64</i> for greater than. |
| 66 0F 64 /r | PCMPGTB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed byte integers in <i>xmm1</i> and <i>xmm2/m128</i> for greater than. |
| 0F 65 /r | PCMPGTW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Compare packed signed word integers in <i>mm</i> and <i>mm/m64</i> for greater than. |
| 66 0F 65 /r | PCMPGTW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed word integers in <i>xmm1</i> and <i>xmm2/m128</i> for greater than. |
| 0F 66 /r | PCMPGTD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Compare packed signed doubleword integers in <i>mm</i> and <i>mm/m64</i> for greater than. |
| 66 0F 66 /r | PCMPGTD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed doubleword integers in <i>xmm1</i> and <i>xmm2/m128</i> for greater than. |

Description

Performs a SIMD signed compare for the greater value of the packed byte, word, or doubleword integers in the destination operand (first operand) and the source operand (second operand). If a data element in the destination operand is greater than the corresponding data element in the source operand, the corresponding data element in the destination operand is set to all 1s; otherwise, it is set to all 0s. The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

The PCMPGTB instruction compares the corresponding signed byte integers in the destination and source operands; the PCMPGTW instruction compares the corresponding signed word integers in the destination and source operands; and the PCMPGTD instruction compares the corresponding signed doubleword integers in the destination and source operands.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PCMPGTB instruction with 64-bit operands:

```
IF DEST[7:0] > SRC[7:0]
    THEN DEST[7:0] ← FFH;
    ELSE DEST[7:0] ← 0; FI;
(* Continue comparison of 2nd through 7th bytes in DEST and SRC *)
IF DEST[63:56] > SRC[63:56]
    THEN DEST[63:56] ← FFH;
    ELSE DEST[63:56] ← 0; FI;
```

PCMPGTB instruction with 128-bit operands:

```
IF DEST[7:0] > SRC[7:0]
    THEN DEST[7:0] ← FFH;
    ELSE DEST[7:0] ← 0; FI;
(* Continue comparison of 2nd through 15th bytes in DEST and SRC *)
IF DEST[127:120] > SRC[127:120]
    THEN DEST[127:120] ← FFH;
    ELSE DEST[127:120] ← 0; FI;
```

PCMPGTW instruction with 64-bit operands:

```
IF DEST[15:0] > SRC[15:0]
    THEN DEST[15:0] ← FFFFH;
    ELSE DEST[15:0] ← 0; FI;
(* Continue comparison of 2nd and 3rd words in DEST and SRC *)
IF DEST[63:48] > SRC[63:48]
    THEN DEST[63:48] ← FFFFH;
    ELSE DEST[63:48] ← 0; FI;
```

PCMPGTW instruction with 128-bit operands:

```
IF DEST[15:0] > SRC[15:0]
    THEN DEST[15:0] ← FFFFH;
    ELSE DEST[15:0] ← 0; FI;
(* Continue comparison of 2nd through 7th words in DEST and SRC *)
IF DEST[63:48] > SRC[127:112]
    THEN DEST[127:112] ← FFFFH;
    ELSE DEST[127:112] ← 0; FI;
```

PCMPGTD instruction with 64-bit operands:

```
IF DEST[31:0] > SRC[31:0]
    THEN DEST[31:0] ← FFFFFFFFH;
    ELSE DEST[31:0] ← 0; FI;
IF DEST[63:32] > SRC[63:32]
    THEN DEST[63:32] ← FFFFFFFFH;
    ELSE DEST[63:32] ← 0; FI;
```


PCMPGTD instruction with 128-bit operands:

IF DEST[31:0] > SRC[31:0]

THEN DEST[31:0] ← FFFFFFFFH;

ELSE DEST[31:0] ← 0; FI;

(* Continue comparison of 2nd and 3rd doublewords in DEST and SRC *)

IF DEST[127:96] > SRC[127:96]

THEN DEST[127:96] ← FFFFFFFFH;

ELSE DEST[127:96] ← 0; FI;

Intel C/C++ Compiler Intrinsic Equivalents

PCMPGTB __m64 _mm_cmpgt_pi8 (__m64 m1, __m64 m2)

PCMPGTW __m64 _mm_pcmplt_pi16 (__m64 m1, __m64 m2)

DCMPGTD __m64 _mm_pcmplt_pi32 (__m64 m1, __m64 m2)

PCMPGTB __m128i _mm_cmpgt_epi8 (__m128i a, __m128i b)

PCMPGTW __m128i _mm_cmpgt_epi16 (__m128i a, __m128i b)

DCMPGTD __m128i _mm_cmpgt_epi32 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
If any part of the operand lies outside of the effective address space from 0 to FFFFH.

#UD If CR0.EM[bit 2] = 1.
128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF (fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.
(128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.
(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
(128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.
If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF (fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PCMPGTQ — Compare Packed Data for Greater Than

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------------|--------------------------------------|-------------|-----------------|---|
| 66 OF 38 37 /r | PCMPGTQ <i>xmm1,xmm2/m1</i> 28 | Valid | Valid | Compare packed qwords in <i>xmm2/m128</i> and <i>xmm1</i> for greater than. |

Description

Performs an SIMD compare for the packed quadwords in the destination operand (first operand) and the source operand (second operand). If the data element in the first (destination) operand is greater than the corresponding element in the second (source) operand, the corresponding data element in the destination is set to all 1s; otherwise, it is set to 0s.

Operation

```
IF (DEST[63-0] > SRC[63-0])
    THEN DEST[63-0] ← FFFFFFFFFFFFFFFFH;
    ELSE DEST[63-0] ← 0; FI
IF (DEST[127-64] > SRC[127-64])
    THEN DEST[127-64] ← FFFFFFFFFFFFFFFFH;
    ELSE DEST[127-64] ← 0; FI
```

Flags Affected

None

Intel C/C++ Compiler Intrinsic Equivalent

PCMPGTQ __m128i _mm_cmpgt_epi64(__m128i a, __m128i b)

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS or GS segments.
If not aligned on 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF (fault-code) For a page fault.

#UD If CR0.EM = 1.
If CR4.OSFXSR(bit 9) = 0.
If CPUID.01H:ECX.SSE4_2 [Bit 20] = 0.

| | |
|-----|--|
| | If LOCK prefix is used. |
| | Either the prefix REP (F3h) or REPN (F2H) is used. |
| #NM | If TS bit in CR0 is set. |

Real Mode Exceptions

| | |
|-----|--|
| #GP | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If not aligned on 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM = 1. If CR4.OSFXSR(bit 9) = 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |
| #NM | If TS bit in CR0 is set. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|------------------|-------------------|
| #PF (fault-code) | For a page fault. |
|------------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|--|
| #GP(0) | If the memory address is in a non-canonical form. If not aligned on 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #UD | If CR0.EM = 1. If CR4.OSFXSR(bit 9) = 0. If CPUID.01H: ECX.SSE4_2 [Bit 20] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |
| #NM | If TS bit in CR0 is set. |

PEXTRB/PEXTRD/PEXTRQ – Extract Byte/Dword/Qword

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|-------------------------------|---|-------------|------------------|---|
| 66 OF 3A 14 /r ib | PEXTRB <i>reg/m8</i> , <i>xmm2</i> , <i>imm8</i> | Valid | Valid | Extract a byte integer value from <i>xmm2</i> at the source byte offset specified by <i>imm8</i> into <i>rreg</i> or <i>m8</i> . The upper bits of <i>r32</i> or <i>r64</i> are zeroed. |
| 66 OF 3A 16 /r ib | PEXTRD <i>r/m32</i> , <i>xmm2</i> , <i>imm8</i> | Valid | Valid | Extract a dword integer value from <i>xmm2</i> at the source dword offset specified by <i>imm8</i> into <i>r/m32</i> . |
| 66 REX.W OF 3A 16 /r ib | PEXTRQ <i>r/m64</i> , <i>xmm2</i> , <i>imm8</i> | Valid | N. E. | Extract a qword integer value from <i>xmm2</i> at the source dword offset specified by <i>imm8</i> into <i>r/m64</i> . |

Description

Copies a data element (byte, dword, quadword) in the source operand (second operand) specified by the count operand (third operand) to the destination operand (first operand). The source operand is an XMM register. The destination operand can be a general-purpose register or a memory address. The count operand is an 8-bit immediate. When specifying a quadword [dword, byte] element, the [2, 4] least-significant bit(s) of the count operand specify the location.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15, R8-15). PEXTRQ requires REX.W. If the destination operand is a general-purpose register, the default operand size of PEXTRB is 64 bits.

Operation

CASE of

```

PEXTRB: SEL ← COUNT[3:0];
        TEMP ← (Src >> SEL*8) AND FFH;
        IF (DEST = Mem8)
            THEN
                Mem8 ← TEMP[7:0];
        ELSE IF (64-Bit Mode and 64-bit register selected)
            THEN
                R64[7:0] ← TEMP[7:0];
                r64[63:8] ← ZERO_FILL;
        ELSE

```

```

        R32[7:0] ← TEMP[7:0];
        r32[31:8] ← ZERO_FILL; };
    FI;
PEXTRD:SEL ← COUNT[1:0];
        TEMP ← (Src >> SEL*32) AND FFFF_FFFFH;
        DEST ← TEMP;
PEXTRQ:SEL ← COUNT[0];
        TEMP ← (Src >> SEL*64);
        DEST ← TEMP;
EASC:

```

Intel C/C++ Compiler Intrinsic Equivalent

```

PEXTRB    int __mm_extract_epi8 (__m128i src, const int ndx);
PEXTRD    int __mm_extract_epi32 (__m128i src, const int ndx);
PEXTRQ    __int64 __mm_extract_epi64 (__m128i src, const int ndx);

```

Flags Affected

None

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |
| #AC(0) | (Dword and qword references) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|---|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to OFFFh. |
| #UD | If CR0.EM[bit 2] = 1. |

| | |
|-----|--|
| | If CR4.OSFXSR[bit 9] = 0. |
| | If CPUID.01H: ECX.SSE4_1[bit 19] = 0. |
| | If LOCK prefix is used. |
| | Either the prefix REP (F3h) or REPN (F2H) is used. |
| #NM | If CR0.TS[bit 3] = 1. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (Dword and qword references) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. |
| | If OSFXSR in CR4 is 0. |
| | If CPUID.01H: ECX.SSE4_1[bit 19] = 0. |
| | If LOCK prefix is used. |
| | Either the prefix REP (F3h) or REPN (F2H) is used. |
| #AC(0) | (Dword and qword references) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PEXTRW—Extract Word

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------|----------------------------------|-------------|------------------|---|
| 0F C5 /r ib | PEXTRW <i>reg, mm, imm8</i> | Valid | Valid | Extract the word specified by <i>imm8</i> from <i>mm</i> and move it to <i>reg</i> , bits 15-0. The upper bits of r32 or r64 is zeroed. |
| 66 0F C5 /r ib | PEXTRW <i>reg, xmm, imm8</i> | Valid | Valid | Extract the word specified by <i>imm8</i> from <i>xmm</i> and move it to <i>reg</i> , bits 15-0. The upper bits of r32 or r64 is zeroed. |
| 66 0F 3A 15 /r ib | PEXTRW <i>reg/m16, xmm, imm8</i> | Valid | Valid | Extract the word specified by <i>imm8</i> from <i>xmm</i> and copy it to lowest 16 bits of <i>reg or m16</i> . Zero-extend the result in the destination, r32 or r64. |

Description

Copies the word in the source operand (second operand) specified by the count operand (third operand) to the destination operand (first operand). The source operand can be an MMX technology register or an XMM register. The destination operand can be the low word of a general-purpose register or a 16-bit memory address. The count operand is an 8-bit immediate. When specifying a word location in an MMX technology register, the 2 least-significant bits of the count operand specify the location; for an XMM register, the 3 least-significant bits specify the location. The content of the destination register above bit 16 is cleared (set to all 0s).

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15, R8-15). If the destination operand is a general-purpose register, the default operand size is 64-bits in 64-bit mode.

Operation

```

IF (DEST = Mem16)
THEN
    SEL ← COUNT[2:0];
    TEMP ← (Src >> SEL*16) AND FFFFH;
    Mem16 ← TEMP[15:0];
ELSE IF (64-Bit Mode and destination is a general-purpose register)
THEN
    FOR (PEXTRW instruction with 64-bit source operand)
    { SEL ← COUNT[1:0];
      TEMP ← (SRC >> (SEL * 16)) AND FFFFH;
  
```

```

    r64[15:0] ← TEMP[15:0];
    r64[63:16] ← ZERO_FILL; };
FOR (PEXTRW instruction with 128-bit source operand)
{ SEL ← COUNT[2:0];
  TEMP ← (SRC >> (SEL * 16)) AND FFFFH;
  r64[15:0] ← TEMP[15:0];
  r64[63:16] ← ZERO_FILL; }
ELSE
FOR (PEXTRW instruction with 64-bit source operand)
{ SEL ← COUNT[1:0];
  TEMP ← (SRC >> (SEL * 16)) AND FFFFH;
  r32[15:0] ← TEMP[15:0];
  r32[31:16] ← ZERO_FILL; };
FOR (PEXTRW instruction with 128-bit source operand)
{ SEL ← COUNT[2:0];
  TEMP ← (SRC >> (SEL * 16)) AND FFFFH;
  r32[15:0] ← TEMP[15:0];
  r32[31:16] ← ZERO_FILL; };
FI;
FI;

```

Intel C/C++ Compiler Intrinsic Equivalent

PEXTRW int_mm_extract_pi16 (__m64 a, int n)

PEXTRW int_mm_extract_epi16 (__m128i a, int imm)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

- #GP(0) (3 byte opcode only) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
- #SS(0) (3 byte opcode only) If a memory operand effective address is outside the SS segment limit.
- #UD If CR0.EM[bit 2] = 1.
 - (128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
 - (3 byte opcode only) If CPUID.01H:ECX.SSE4_1[bit 19] = 0.
 - (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.
 - If the LOCK prefix is used.

| | |
|-----------------|---|
| | (3 byte opcode only) Either the prefix REP (F3h) or REPN (F2H) is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | (3 byte opcode only) If a page fault occurs. |
| #AC(0) | (3 byte opcode only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (3 byte opcode only) If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (3 byte opcode only) If CPUID.01H:ECX.SSE4_1[bit 19] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. (3 byte opcode only) Either the prefix REP (F3h) or REPN (F2H) is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | (3 byte opcode only) For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | (3 byte opcode only) If the memory address is in a non-canonical form. |
| #SS(0) | (3 byte opcode only) If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | (3 byte opcode only) For a page fault. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. |

(3 byte opcode only) If CPUID.01H: ECX.SSE4_1[bit 19] = 0.
(128-bit operations only) If CPUID.01H: EDX.SSE2[bit 26] = 0.
If the LOCK prefix is used.

(3 byte opcode only) Either the prefix REP (F3h) or REPN (F2H) is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#AC(0) (3 byte opcode only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PHADDW/PHADD – Packed Horizontal Add

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|------------------------|-------------|------------------|--|
| 0F 38 01 /r | PHADDW mm1, mm2/m64 | Valid | Valid | Add 16-bit signed integers horizontally, pack to MM1. |
| 66 0F 38 01 /r | PHADDW xmm1, xmm2/m128 | Valid | Valid | Add 16-bit signed integers horizontally, pack to XMM1. |
| 0F 38 02 /r | PHADD mm1, mm2/m64 | Valid | Valid | Add 32-bit signed integers horizontally, pack to MM1. |
| 66 0F 38 02 /r | PHADD xmm1, xmm2/m128 | Valid | Valid | Add 32-bit signed integers horizontally, pack to XMM1. |

Description

PHADDW adds two adjacent 16-bit signed integers horizontally from the source and destination operands and packs the 16-bit signed results to the destination operand (first operand). PHADD adds two adjacent 32-bit signed integers horizontally from the source and destination operands and packs the 32-bit signed results to the destination operand (first operand). Both operands can be MMX or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PHADDW with 64-bit operands:

$$\begin{aligned} \text{mm1}[15-0] &= \text{mm1}[31-16] + \text{mm1}[15-0]; \\ \text{mm1}[31-16] &= \text{mm1}[63-48] + \text{mm1}[47-32]; \\ \text{mm1}[47-32] &= \text{mm2/m64}[31-16] + \text{mm2/m64}[15-0]; \\ \text{mm1}[63-48] &= \text{mm2/m64}[63-48] + \text{mm2/m64}[47-32]; \end{aligned}$$

PHADDW with 128-bit operands :

$$\begin{aligned} \text{xmm1}[15-0] &= \text{xmm1}[31-16] + \text{xmm1}[15-0]; \\ \text{xmm1}[31-16] &= \text{xmm1}[63-48] + \text{xmm1}[47-32]; \\ \text{xmm1}[47-32] &= \text{xmm1}[95-80] + \text{xmm1}[79-64]; \\ \text{xmm1}[63-48] &= \text{xmm1}[127-112] + \text{xmm1}[111-96]; \\ \text{xmm1}[79-64] &= \text{xmm2/m128}[31-16] + \text{xmm2/m128}[15-0]; \\ \text{xmm1}[95-80] &= \text{xmm2/m128}[63-48] + \text{xmm2/m128}[47-32]; \\ \text{xmm1}[111-96] &= \text{xmm2/m128}[95-80] + \text{xmm2/m128}[79-64]; \\ \text{xmm1}[127-112] &= \text{xmm2/m128}[127-112] + \text{xmm2/m128}[111-96]; \end{aligned}$$

PHADDD with 64-bit operands :

$$\begin{aligned} \text{mm1}[31-0] &= \text{mm1}[63-32] + \text{mm1}[31-0]; \\ \text{mm1}[63-32] &= \text{mm2}/\text{m64}[63-32] + \text{mm2}/\text{m64}[31-0]; \end{aligned}$$

PHADDD with 128-bit operands:

$$\begin{aligned} \text{xmm1}[31-0] &= \text{xmm1}[63-32] + \text{xmm1}[31-0]; \\ \text{xmm1}[63-32] &= \text{xmm1}[127-96] + \text{xmm1}[95-64]; \\ \text{xmm1}[95-64] &= \text{xmm2}/\text{m128}[63-32] + \text{xmm2}/\text{m128}[31-0]; \\ \text{xmm1}[127-96] &= \text{xmm2}/\text{m128}[127-96] + \text{xmm2}/\text{m128}[95-64]; \end{aligned}$$

Intel C/C++ Compiler Intrinsic Equivalents

PHADDW `__m64 __mm_hadd_pi16 (__m64 a, __m64 b)`
 PHADDW `__m128i __mm_hadd_epi16 (__m128i a, __m128i b)`
 PHADDD `__m64 __mm_hadd_pi32 (__m64 a, __m64 b)`
 PHADDD `__m128i __mm_hadd_epi32 (__m128i a, __m128i b)`

Protected Mode Exceptions

#GP(0): If a memory operand effective address is outside the CS, DS, ES, FS or GS segments.
 (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF(fault-code) If a page fault occurs.

#UD If CR0.EM(bit 2) = 1.
 (128-bit operations only) If CR4.OSFXSR(bit 9) = 0.
 If CPUID.SSSE3(ECX bit 9) = 0.
 If the LOCK prefix is used.

#NM If TS bit in CR0 is set.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#AC(0) (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3.

Real Mode Exceptions

#GP(0) If any part of the operand lies outside of the effective address space from 0 to 0FFFFH.
 (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment.

| | |
|-----|--|
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only). If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PHADDSW – Packed Horizontal Add and Saturate

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|-------------------------|-------------|------------------|---|
| 0F 38 03 /r | PHADDSW mm1, mm2/m64 | Valid | Valid | Add 16-bit signed integers horizontally, pack saturated integers to MM1. |
| 66 0F 38 03 /r | PHADDSW xmm1, xmm2/m128 | Valid | Valid | Add 16-bit signed integers horizontally, pack saturated integers to XMM1. |

Description

PHADDSW adds two adjacent signed 16-bit integers horizontally from the source and destination operands and saturates the signed results; packs the signed, saturated 16-bit results to the destination operand (first operand) Both operands can be MMX or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PHADDSW with 64-bit operands:

```
mm1[15-0] = SaturateToSignedWord((mm1[31-16] + mm1[15-0]));
mm1[31-16] = SaturateToSignedWord(mm1[63-48] + mm1[47-32]);
mm1[47-32] = SaturateToSignedWord(mm2/m64[31-16] + mm2/m64[15-0]);
mm1[63-48] = SaturateToSignedWord(mm2/m64[63-48] + mm2/m64[47-32]);
```

PHADDSW with 128-bit operands :

```
xmm1[15-0]= SaturateToSignedWord(xmm1[31-16] + xmm1[15-0]);
xmm1[31-16] = SaturateToSignedWord(xmm1[63-48] + xmm1[47-32]);
xmm1[47-32] = SaturateToSignedWord(xmm1[95-80] + xmm1[79-64]);
xmm1[63-48] = SaturateToSignedWord(xmm1[127-112] + xmm1[111-96]);
xmm1[79-64] = SaturateToSignedWord(xmm2/m128[31-16] + xmm2/m128[15-0]);
xmm1[95-80] = SaturateToSignedWord(xmm2/m128[63-48] + xmm2/m128[47-32]);
xmm1[111-96] = SaturateToSignedWord(xmm2/m128[95-80] + xmm2/m128[79-64]);
xmm1[127-112] = SaturateToSignedWord(xmm2/m128[127-112] + xmm2/m128[111-96]);
```

Intel C/C++ Compiler Intrinsic Equivalent

PHADDSW __m64 __mm_hadds_pi16 (__m64 a, __m64 b)

PHADDSW __m128i __mm_hadds_epi16 (__m128i a, __m128i b)

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS or GS segments. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #AC(0): | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PHMINPOSUW — Packed Horizontal Word Minimum

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|-------------------|--|-------------|------------------|--|
| 66 OF 38 41 /r | PHMINPOSUW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Find the minimum unsigned word in <i>xmm2/m128</i> and place its value in the low word of <i>xmm1</i> and its index in the second-lowest word of <i>xmm1</i> . |

Description

Determine the minimum unsigned word value in the source operand (second operand) and place the unsigned word in the low word (bits 0-15) of the destination operand (first operand). The word index of the minimum value is stored in bits 16-18 of the destination operand. The remaining upper bits of the destination are set to zero.

Operation

```
INDEX ← 0;
MIN ← SRC[15:0]
IF (SRC[31:16] < MIN)
    THEN INDEX ← 1; MIN ← SRC[31:16]; FI;
IF (SRC[47:32] < MIN)
    THEN INDEX ← 2; MIN ← SRC[47:32]; FI;
* Repeat operation for words 3 through 6
IF (SRC[127:112] < MIN)
    THEN INDEX ← 7; MIN ← SRC[127:112]; FI;
DEST[15:0] ← MIN;
DEST[18:16] ← INDEX;
DEST[127:19] ← 00000000000000000000000000000000H;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PHMINPOSUW    __m128i_mm_minpos_epu16(__m128i packed_words);
```

Flags Affected

None

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.

| | |
|-----------------|--|
| | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. |

If CPUID feature flag ECX.SSE4_1 is 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

PHSUBW/PHSUBD – Packed Horizontal Subtract

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|------------------------|-------------|------------------|---|
| 0F 38 05 /r | PHSUBW mm1, mm2/m64 | Valid | Valid | Subtract 16-bit signed integers horizontally, pack to MM1. |
| 66 0F 38 05 /r | PHSUBW xmm1, xmm2/m128 | Valid | Valid | Subtract 16-bit signed integers horizontally, pack to XMM1. |
| 0F 38 06 /r | PHSUBD mm1, mm2/m64 | Valid | Valid | Subtract 32-bit signed integers horizontally, pack to MM1. |
| 66 0F 38 06 /r | PHSUBD xmm1, xmm2/m128 | Valid | Valid | Subtract 32-bit signed integers horizontally, pack to XMM1. |

Description

PHSUBW performs horizontal subtraction on each adjacent pair of 16-bit signed integers by subtracting the most significant word from the least significant word of each pair in the source and destination operands, and packs the signed 16-bit results to the destination operand (first operand). PHSUBD performs horizontal subtraction on each adjacent pair of 32-bit signed integers by subtracting the most significant doubleword from the least significant doubleword of each pair, and packs the signed 32-bit result to the destination operand. Both operands can be MMX or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PHSUBW with 64-bit operands:

```
mm1[15-0] = mm1[15-0] - mm1[31-16];
mm1[31-16] = mm1[47-32] - mm1[63-48];
mm1[47-32] = mm2/m64[15-0] - mm2/m64[31-16];
mm1[63-48] = mm2/m64[47-32] - mm2/m64[63-48];
```

PHSUBW with 128-bit operands:

```
xmm1[15-0] = xmm1[15-0] - xmm1[31-16];
xmm1[31-16] = xmm1[47-32] - xmm1[63-48];
xmm1[47-32] = xmm1[79-64] - xmm1[95-80];
```

```

xmm1[63-48] = xmm1[111-96] - xmm1[127-112];
xmm1[79-64] = xmm2/m128[15-0] - xmm2/m128[31-16];
xmm1[95-80] = xmm2/m128[47-32] - xmm2/m128[63-48];
xmm1[111-96] = xmm2/m128[79-64] - xmm2/m128[95-80];
xmm1[127-112] = xmm2/m128[111-96] - xmm2/m128[127-112];

```

PHSUBD with 64-bit operands:

```

mm1[31-0] = mm1[31-0] - mm1[63-32];
mm1[63-32] = mm2/m64[31-0] - mm2/m64[63-32];

```

PHSUBD with 128-bit operands:

```

xmm1[31-0] = xmm1[31-0] - xmm1[63-32];
xmm1[63-32] = xmm1[95-64] - xmm1[127-96];
xmm1[95-64] = xmm2/m128[31-0] - xmm2/m128[63-32];
xmm1[127-96] = xmm2/m128[95-64] - xmm2/m128[127-96];

```

Intel C/C++ Compiler Intrinsic Equivalents

```

PHSUBW  __m64 _mm_hsub_pi16 (__m64 a, __m64 b)
PHSUBW  __m128i _mm_hsub_epi16 (__m128i a, __m128i b)
PHSUBD  __m64 _mm_hsub_pi32 (__m64 a, __m64 b)
PHSUBD  __m128i _mm_hsub_epi32 (__m128i a, __m128i b)

```

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS or GS segments. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | If there is a pending x87 FPU exception (64-bit operations only). |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|---------|--|
| #GP(0): | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #UD: | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PHSUBSW — Packed Horizontal Subtract and Saturate

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|-------------------------|-------------|------------------|--|
| 0F 38 07 /r | PHSUBSW mm1, mm2/m64 | Valid | Valid | Subtract 16-bit signed integer horizontally, pack saturated integers to MM1. |
| 66 0F 38 07 /r | PHSUBSW xmm1, xmm2/m128 | Valid | Valid | Subtract 16-bit signed integer horizontally, pack saturated integers to XMM1 |

Description

PHSUBSW performs horizontal subtraction on each adjacent pair of 16-bit signed integers by subtracting the most significant word from the least significant word of each pair in the source and destination operands. The signed, saturated 16-bit results are packed to the destination operand (first operand). Both operands can be MMX or XMM register. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PHSUBSW with 64-bit operands:

```
mm1[15-0] = SaturateToSignedWord(mm1[15-0] - mm1[31-16]);
mm1[31-16] = SaturateToSignedWord(mm1[47-32] - mm1[63-48]);
mm1[47-32] = SaturateToSignedWord(mm2/m64[15-0] - mm2/m64[31-16]);
mm1[63-48] = SaturateToSignedWord(mm2/m64[47-32] - mm2/m64[63-48]);
```

PHSUBSW with 128-bit operands:

```
xmm1[15-0] = SaturateToSignedWord(xmm1[15-0] - xmm1[31-16]);
xmm1[31-16] = SaturateToSignedWord(xmm1[47-32] - xmm1[63-48]);
xmm1[47-32] = SaturateToSignedWord(xmm1[79-64] - xmm1[95-80]);
xmm1[63-48] = SaturateToSignedWord(xmm1[111-96] - xmm1[127-112]);
xmm1[79-64] = SaturateToSignedWord(xmm2/m128[15-0] - xmm2/m128[31-16]);
xmm1[95-80] = SaturateToSignedWord(xmm2/m128[47-32] - xmm2/m128[63-48]);
xmm1[111-96] = SaturateToSignedWord(xmm2/m128[79-64] - xmm2/m128[95-80]);
xmm1[127-112] = SaturateToSignedWord(xmm2/m128[111-96] - xmm2/m128[127-112]);
```

Intel C/C++ Compiler Intrinsic Equivalent

PHSUBSW __m64 __mm_hsubs_pi16 (__m64 a, __m64 b)

PHSUBSW __m128i __mm_hsubs_epi16 (__m128i a, __m128i b)

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | if a memory operand effective address is outside the CS, DS, ES, FS or GS segments. If not aligned on 16-byte boundary, regardless of segment (128-bit operations only). |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. If CR4.OSFXSR(bit 9) = 0 (128-bit operations only). If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | If there is a pending x87 FPU exception (64-bit operations only). |
| #AC(0) | If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3 (64-bit operations only). |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If not aligned on 16-byte boundary, regardless of segment (128-bit operations only). |
| #UD | If CR0.EM = 1. If CR4.OSFXSR(bit 9) = 0 (128-bit operations only). If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | If there is a pending x87 FPU exception (64-bit operations only). |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and unaligned memory reference is made (64-bit operations only). |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PINSRB/PINSRD/PINSRQ – Insert Byte/Dword/Qword

| Opcode | Instruction | Compat/ Leg Mode | 64-bit Mode | Description |
|-------------------------------|---|---------------------|----------------|--|
| 66 OF 3A 20 /r ib | PINSRB <i>xmm1</i> , <i>r32/m8, imm8</i> | Valid | Valid | Insert a byte integer value from <i>r32/m8</i> into <i>xmm1</i> at the destination element in <i>xmm1</i> specified by <i>imm8</i> . |
| 66 OF 3A 22 /r ib | PINSRD <i>xmm1</i> , <i>r/m32, imm8</i> | Valid | Valid | Insert a dword integer value from <i>r/m32</i> into the <i>xmm1</i> at the destination elements specified by <i>imm8</i> . |
| 66 REX.W OF 3A 22 /r ib | PINSRQ <i>xmm1</i> , <i>r/m64, imm8</i> | N. E. | Valid | Insert a qword integer value from <i>r/m32</i> into the <i>xmm1</i> at the destination elements specified by <i>imm8</i> . |

Description

Copies a byte/dword/qword from the source operand (second operand) and inserts it in the destination operand (first operand) at the location specified with the count operand (third operand). (The other elements in the destination register are left untouched.) The source operand can be a general-purpose register or a memory location. (When the source operand is a general-purpose register, PINSRB copies the low byte of the register.) The destination operand is an XMM register. The count operand is an 8-bit immediate. When specifying a qword[dword, byte] location in an XMM register, the [2, 4] least-significant bit(s) of the count operand specify the location.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15, R8-15). Use of REX.W permits the use of 64 bit general purpose registers.

Operation

CASE OF

```

PINSRB: SEL ← COUNT[3:0];
        MASK ← (OFFH << (SEL * 8));
        TEMP ← (((SRC[7:0] << (SEL * 8)) AND MASK);
PINSRD: SEL ← COUNT[1:0];
        MASK ← (OFFFFFFFFFH << (SEL * 32));
        TEMP ← (((SRC << (SEL * 32)) AND MASK) ;
PINSRQ: SEL ← COUNT[0]
        MASK ← (OFFFFFFFFFHH << (SEL * 64));
        TEMP ← (((SRC << (SEL * 32)) AND MASK) ;

```

ESAC;

```
DEST ← ((DEST AND NOT MASK) OR TEMP);
```

Intel C/C++ Compiler Intrinsic Equivalent

PINSRB `__m128i _mm_insert_epi8 (__m128i s1, int s2, const int ndx);`

PINSRD `__m128i _mm_insert_epi32 (__m128i s2, int s, const int ndx);`

PINSRQ `__m128i _mm_insert_epi64(__m128i s2, __int64 s, const int ndx);`

Flags Affected

None

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |
| #AC(0) | (Dword and qword references) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|---|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

#PF(fault-code) For a page fault.

#AC(0) (Dword and qword references) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

#GP(0) If the memory address is in a non-canonical form.

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#PF(fault-code) For a page fault.

#NM If TS in CR0 is set.

#UD If EM in CR0 is set.

If OSFXSR in CR4 is 0.

If CPUID feature flag ECX.SSE4_1 is 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

#AC(0) (Dword and qword references) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PINSRW—Insert Word

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------------|---|-------------|-----------------|---|
| 0F C4 /r ib | PINSRW <i>mm</i> , <i>r32/m16</i> , <i>imm8</i> | Valid | Valid | Insert the low word from <i>r32</i> or from <i>m16</i> into <i>mm</i> at the word position specified by <i>imm8</i> |
| 66 0F C4 /r ib | PINSRW <i>xmm</i> , <i>r32/m16</i> , <i>imm8</i> | Valid | Valid | Move the low word of <i>r32</i> or from <i>m16</i> into <i>xmm</i> at the word position specified by <i>imm8</i> . |

Description

Copies a word from the source operand (second operand) and inserts it in the destination operand (first operand) at the location specified with the count operand (third operand). (The other words in the destination register are left untouched.) The source operand can be a general-purpose register or a 16-bit memory location. (When the source operand is a general-purpose register, the low word of the register is copied.) The destination operand can be an MMX technology register or an XMM register. The count operand is an 8-bit immediate. When specifying a word location in an MMX technology register, the 2 least-significant bits of the count operand specify the location; for an XMM register, the 3 least-significant bits specify the location.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15, R8-15).

Operation

PINSRW instruction with 64-bit source operand:

```
SEL ← COUNT AND 3H;
CASE (Determine word position) OF
  SEL ← 0:  MASK ← 000000000000FFFFH;
  SEL ← 1:  MASK ← 00000000FFFF0000H;
  SEL ← 2:  MASK ← 0000FFFF00000000H;
  SEL ← 3:  MASK ← FFFF000000000000H;
DEST ← (DEST AND NOT MASK) OR (((SRC << (SEL * 16)) AND MASK);
```

PINSRW instruction with 128-bit source operand:

```
SEL ← COUNT AND 7H;
CASE (Determine word position) OF
  SEL ← 0:  MASK ← 00000000000000000000000000000000FFFFH;
  SEL ← 1:  MASK ← 00000000000000000000000000000000FFFF0000H;
  SEL ← 2:  MASK ← 00000000000000000000000000000000FFFF00000000H;
  SEL ← 3:  MASK ← 00000000000000000000000000000000FFFF000000000000H;
```

SEL ← 4: MASK ← 000000000000FFFF0000000000000000H;
 SEL ← 5: MASK ← 00000000FFFF00000000000000000000H;
 SEL ← 6: MASK ← 0000FFFF000000000000000000000000H;
 SEL ← 7: MASK ← FFFF0000000000000000000000000000H;
 DEST ← (DEST AND NOT MASK) OR (((SRC << (SEL * 16)) AND MASK);

Intel C/C++ Compiler Intrinsic Equivalent

PINSRW __m64 _mm_insert_pi16 (__m64 a, int d, int n)

PINSRW __m128i _mm_insert_epi16 (__m128i a, int b, int imm)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. |
| | If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one |

that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

If the LOCK prefix is used.

| | |
|-----|---|
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMADDUBSW — Multiply and Add Packed Signed and Unsigned Bytes

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|---------------------------------|-------------|---------------------|---|
| 0F 38 04 /r | PMADDUBSW mm1, mm2/m64 | Valid | Valid | Multiply signed and unsigned bytes, add horizontal pair of signed words, pack saturated signed-words to MM1. |
| 66 0F 38 04 /r | PMADDUBSW xmm1, xmm2/m128 | Valid | Valid | Multiply signed and unsigned bytes, add horizontal pair of signed words, pack saturated signed-words to XMM1. |

Description

PMADDUBSW multiplies vertically each unsigned byte of the destination operand (first operand) with the corresponding signed byte of the source operand (second operand), producing intermediate signed 16-bit integers. Each adjacent pair of signed words is added and the saturated result is packed to the destination operand. For example, the lowest-order bytes (bits 7-0) in the source and destination operands are multiplied and the intermediate signed word result is added with the corresponding intermediate result from the 2nd lowest-order bytes (bits 15-8) of the operands; the sign-saturated result is stored in the lowest word of the destination register (15-0). The same operation is performed on the other pairs of adjacent bytes. Both operands can be MMX register or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PMADDUBSW with 64 bit operands:

```
DEST[15-0] = SaturateToSignedWord(SRC[15-8]*DEST[15-8]+SRC[7-0]*DEST[7-0]);
DEST[31-16] = SaturateToSignedWord(SRC[31-24]*DEST[31-24]+SRC[23-16]*DEST[23-16]);
DEST[47-32] = SaturateToSignedWord(SRC[47-40]*DEST[47-40]+SRC[39-32]*DEST[39-32]);
DEST[63-48] = SaturateToSignedWord(SRC[63-56]*DEST[63-56]+SRC[55-48]*DEST[55-48]);
```

PMADDUBSW with 128 bit operands:

```
DEST[15-0] = SaturateToSignedWord(SRC[15-8]* DEST[15-8]+SRC[7-0]*DEST[7-0]);
// Repeat operation for 2nd through 7th word
```

$SRC1/DEST[127-112] = \text{SaturateToSignedWord}(SRC[127-120]*DEST[127-120] + SRC[119-112]* DEST[119-112]);$

Intel C/C++ Compiler Intrinsic Equivalents

PMADDUBSW `__m64 __mm_maddubs_pi16 (__m64 a, __m64 b)`

PMADDUBSW `__m128i __mm_maddubs_epi16 (__m128i a, __m128i b)`

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS or GS segments. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. If CR4.OSFXSR(bit 9) = 0 (128-bit operations only) If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMADDWD—Multiply and Add Packed Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|--|
| 0F F5 /r | PMADDWD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Multiply the packed words in <i>mm</i> by the packed words in <i>mm/m64</i> , add adjacent doubleword results, and store in <i>mm</i> . |
| 66 0F F5 /r | PMADDWD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply the packed word integers in <i>xmm1</i> by the packed word integers in <i>xmm2/m128</i> , add adjacent doubleword results, and store in <i>xmm1</i> . |

Description

Multiplies the individual signed words of the destination operand (first operand) by the corresponding signed words of the source operand (second operand), producing temporary signed, doubleword results. The adjacent doubleword results are then summed and stored in the destination operand. For example, the corresponding low-order words (15-0) and (31-16) in the source and destination operands are multiplied by one another and the doubleword results are added together and stored in the low doubleword of the destination register (31-0). The same operation is performed on the other pairs of adjacent words. (Figure 4-2 shows this operation when using 64-bit operands.) The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

The PMADDWD instruction wraps around only in one situation: when the 2 pairs of words being operated on in a group are all 8000H. In this case, the result wraps around to 80000000H.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

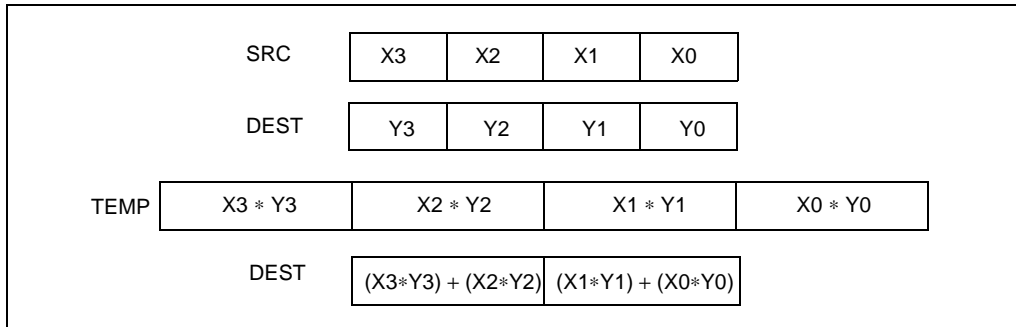


Figure 4-2. PMADDWD Execution Model Using 64-bit Operands

Operation

PMADDWD instruction with 64-bit operands:

$$\begin{aligned} \text{DEST}[31:0] &\leftarrow (\text{DEST}[15:0] * \text{SRC}[15:0]) + (\text{DEST}[31:16] * \text{SRC}[31:16]); \\ \text{DEST}[63:32] &\leftarrow (\text{DEST}[47:32] * \text{SRC}[47:32]) + (\text{DEST}[63:48] * \text{SRC}[63:48]); \end{aligned}$$

PMADDWD instruction with 128-bit operands:

$$\begin{aligned} \text{DEST}[31:0] &\leftarrow (\text{DEST}[15:0] * \text{SRC}[15:0]) + (\text{DEST}[31:16] * \text{SRC}[31:16]); \\ \text{DEST}[63:32] &\leftarrow (\text{DEST}[47:32] * \text{SRC}[47:32]) + (\text{DEST}[63:48] * \text{SRC}[63:48]); \\ \text{DEST}[95:64] &\leftarrow (\text{DEST}[79:64] * \text{SRC}[79:64]) + (\text{DEST}[95:80] * \text{SRC}[95:80]); \\ \text{DEST}[127:96] &\leftarrow (\text{DEST}[111:96] * \text{SRC}[111:96]) + (\text{DEST}[127:112] * \text{SRC}[127:112]); \end{aligned}$$

Intel C/C++ Compiler Intrinsic Equivalent

PMADDWD `__m64 __mm_madd_pi16(__m64 m1, __m64 m2)`

PMADDWD `__m128i __mm_madd_epi16 (__m128i a, __m128i b)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

- #GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMAXSB — Maximum of Packed Signed Byte Integers

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|-------------------|--|-------------|------------------|--|
| 66 OF 38 3C /r | PMAXSB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed byte integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed maximum values in <i>xmm1</i> . |

Description

Compares packed signed byte integers in the destination operand (first operand) and the source operand (second operand), and returns the maximum for each packed value in the destination operand.

Operation

```

IF (DEST[7:0] > SRC[7:0])
    THEN DEST[7:0] ← DEST[7:0];
    ELSE DEST[7:0] ← SRC[7:0]; FI;
IF (DEST[15:8] > SRC[15:8])
    THEN DEST[15:8] ← DEST[15:8];
    ELSE DEST[15:8] ← SRC[15:8]; FI;
IF (DEST[23:16] > SRC[23:16])
    THEN DEST[23:16] ← DEST[23:16];
    ELSE DEST[23:16] ← SRC[23:16]; FI;
IF (DEST[31:24] > SRC[31:24])
    THEN DEST[31:24] ← DEST[31:24];
    ELSE DEST[31:24] ← SRC[31:24]; FI;
IF (DEST[39:32] > SRC[39:32])
    THEN DEST[39:32] ← DEST[39:32];
    ELSE DEST[39:32] ← SRC[39:32]; FI;
IF (DEST[47:40] > SRC[47:40])
    THEN DEST[47:40] ← DEST[47:40];
    ELSE DEST[47:40] ← SRC[47:40]; FI;
IF (DEST[55:48] > SRC[55:48])
    THEN DEST[55:48] ← DEST[55:48];
    ELSE DEST[55:48] ← SRC[55:48]; FI;
IF (DEST[63:56] > SRC[63:56])
    THEN DEST[63:56] ← DEST[63:56];
    ELSE DEST[63:56] ← SRC[63:56]; FI;
IF (DEST[71:64] > SRC[71:64])
    THEN DEST[71:64] ← DEST[71:64];

```

```

ELSE DEST[71:64] ← SRC[71:64]; FI;
IF (DEST[79:72] > SRC[79:72])
  THEN DEST[79:72] ← DEST[79:72];
  ELSE DEST[79:72] ← SRC[79:72]; FI;
IF (DEST[87:80] > SRC[87:80])
  THEN DEST[87:80] ← DEST[87:80];
  ELSE DEST[87:80] ← SRC[87:80]; FI;
IF (DEST[95:88] > SRC[95:88])
  THEN DEST[95:88] ← DEST[95:88];
  ELSE DEST[95:88] ← SRC[95:88]; FI;
IF (DEST[103:96] > SRC[103:96])
  THEN DEST[103:96] ← DEST[103:96];
  ELSE DEST[103:96] ← SRC[103:96]; FI;
IF (DEST[111:104] > SRC[111:104])
  THEN DEST[111:104] ← DEST[111:104];
  ELSE DEST[111:104] ← SRC[111:104]; FI;
IF (DEST[119:112] > SRC[119:112])
  THEN DEST[119:112] ← DEST[119:112];
  ELSE DEST[119:112] ← SRC[119:112]; FI;
IF (DEST[127:120] > SRC[127:120])
  THEN DEST[127:120] ← DEST[127:120];
  ELSE DEST[127:120] ← SRC[127:120]; FI;

```

Intel C/C++ Compiler Intrinsic Equivalent

PMAXSB `__m128i_mm_max_epi8 (__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

| | |
|------------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. |

Either the prefix REP (F3h) or REPN (F2H) is used.

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PMAXSD — Maximum of Packed Signed Dword Integers

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|-------------------|--|-------------|-----------------|---|
| 66 OF 38 3D /r | PMAXSD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed dword integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed maximum values in <i>xmm1</i> . |

Description

Compares packed signed dword integers in the destination operand (first operand) and the source operand (second operand), and returns the maximum for each packed value in the destination operand.

Operation

```
IF (DEST[31:0] > SRC[31:0])
    THEN DEST[31:0] ← DEST[31:0];
    ELSE DEST[31:0] ← SRC[31:0]; FI;
IF (DEST[63:32] > SRC[63:32])
    THEN DEST[63:32] ← DEST[63:32];
    ELSE DEST[63:32] ← SRC[63:32]; FI;
IF (DEST[95:64] > SRC[95:64])
    THEN DEST[95:64] ← DEST[95:64];
    ELSE DEST[95:64] ← SRC[95:64]; FI;
IF (DEST[127:96] > SRC[127:96])
    THEN DEST[127:96] ← DEST[127:96];
    ELSE DEST[127:96] ← SRC[127:96]; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

PMAXSD `__m128i _mm_max_epi32 (__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. |

Either the prefix REP (F3h) or REPN (F2H) is used.

PMAXSW—Maximum of Packed Signed Word Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|---|
| 0F EE /r | PMAXSW <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Compare signed word integers in <i>mm2/m64</i> and <i>mm1</i> and return maximum values. |
| 66 0F EE /r | PMAXSW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare signed word integers in <i>xmm2/m128</i> and <i>xmm1</i> and return maximum values. |

Description

Performs a SIMD compare of the packed signed word integers in the destination operand (first operand) and the source operand (second operand), and returns the maximum value for each pair of word integers to the destination operand. The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PMAXSW instruction for 64-bit operands:

```
IF DEST[15:0] > SRC[15:0]) THEN
    DEST[15:0] ← DEST[15:0];
ELSE
    DEST[15:0] ← SRC[15:0]; FI;
(* Repeat operation for 2nd and 3rd words in source and destination operands *)
IF DEST[63:48] > SRC[63:48]) THEN
    DEST[63:48] ← DEST[63:48];
ELSE
    DEST[63:48] ← SRC[63:48]; FI;
```

PMAXSW instruction for 128-bit operands:

```
IF DEST[15:0] > SRC[15:0]) THEN
    DEST[15:0] ← DEST[15:0];
ELSE
    DEST[15:0] ← SRC[15:0]; FI;
(* Repeat operation for 2nd through 7th words in source and destination operands *)
IF DEST[127:112] > SRC[127:112]) THEN
    DEST[127:112] ← DEST[127:112];
ELSE
```

DEST[127:112] ← SRC[127:112]; FI;

Intel C/C++ Compiler Intrinsic Equivalent

PMAXSW __m64 _mm_max_pi16(__m64 a, __m64 b)

PMAXSW __m128i _mm_max_epi16 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
|-----|---|

| | |
|-----|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMAXUB—Maximum of Packed Unsigned Byte Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F DE /r | PMAXUB <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Compare unsigned byte integers in <i>mm2/m64</i> and <i>mm1</i> and returns maximum values. |
| 66 0F DE /r | PMAXUB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare unsigned byte integers in <i>xmm2/m128</i> and <i>xmm1</i> and returns maximum values. |

Description

Performs a SIMD compare of the packed unsigned byte integers in the destination operand (first operand) and the source operand (second operand), and returns the maximum value for each pair of byte integers to the destination operand. The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PMAXUB instruction for 64-bit operands:

```

IF DEST[7:0] > SRC[7:0] THEN
    DEST[7:0] ← DEST[7:0];
ELSE
    DEST[7:0] ← SRC[7:0]; FI;
(* Repeat operation for 2nd through 7th bytes in source and destination operands *)
IF DEST[63:56] > SRC[63:56] THEN
    DEST[63:56] ← DEST[63:56];
ELSE
    DEST[63:56] ← SRC[63:56]; FI;

```

PMAXUB instruction for 128-bit operands:

```

IF DEST[7:0] > SRC[7:0] THEN
    DEST[7:0] ← DEST[7:0];
ELSE
    DEST[7:0] ← SRC[7:0]; FI;
(* Repeat operation for 2nd through 15th bytes in source and destination operands *)
IF DEST[127:120] > SRC[127:120] THEN
    DEST[127:120] ← DEST[127:120];

```

ELSE

DEST[127:120] ← SRC[127:120]; FI;

Intel C/C++ Compiler Intrinsic Equivalent

PMAXUB __m64 _mm_max_pu8(__m64 a, __m64 b)

PMAXUB __m128i _mm_max_epu8 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
|-----|---|

| | |
|-----|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMAXUD – Maximum of Packed Unsigned Dword Integers

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|-------------------|--|-------------|---------------------|---|
| 66 OF 38 3F /r | PMAXUD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed unsigned dword integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed maximum values in <i>xmm1</i> . |

Description

Compares packed unsigned dword integers in the destination operand (first operand) and the source operand (second operand), and returns the maximum for each packed value in the destination operand.

Operation

```
IF (DEST[31:0] > SRC[31:0])
    THEN DEST[31:0] ← DEST[31:0];
    ELSE DEST[31:0] ← SRC[31:0]; FI;
IF (DEST[63:32] > SRC[63:32])
    THEN DEST[63:32] ← DEST[63:32];
    ELSE DEST[63:32] ← SRC[63:32]; FI;
IF (DEST[95:64] > SRC[95:64])
    THEN DEST[95:64] ← DEST[95:64];
    ELSE DEST[95:64] ← SRC[95:64]; FI;
IF (DEST[127:96] > SRC[127:96])
    THEN DEST[127:96] ← DEST[127:96];
    ELSE DEST[127:96] ← SRC[127:96]; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

PMAXUD `__m128i _mm_max_epu32 (__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
 If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|--|
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. |

If CPUID feature flag ECX.SSE4_1 is 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

PMAXUW – Maximum of Packed Word Integers

| Opcode | Instruction | Compat/ Leg Mode | 64-bit Mode | Description |
|-------------------|--|---------------------|----------------|--|
| 66 OF 38 3E /r | PMAXUW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed unsigned word integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed maximum values in <i>xmm1</i> . |

Description

Compares packed unsigned word integers in the destination operand (first operand) and the source operand (second operand), and returns the maximum for each packed value in the destination operand.

Operation

```

IF (DEST[15:0] > SRC[15:0])
    THEN DEST[15:0] ← DEST[15:0];
    ELSE DEST[15:0] ← SRC[15:0]; FI;
IF (DEST[31:16] > SRC[31:16])
    THEN DEST[31:16] ← DEST[31:16];
    ELSE DEST[31:16] ← SRC[31:16]; FI;
IF (DEST[47:32] > SRC[47:32])
    THEN DEST[47:32] ← DEST[47:32];
    ELSE DEST[47:32] ← SRC[47:32]; FI;
IF (DEST[63:48] > SRC[63:48])
    THEN DEST[63:48] ← DEST[63:48];
    ELSE DEST[63:48] ← SRC[63:48]; FI;
IF (DEST[79:64] > SRC[79:64])
    THEN DEST[79:64] ← DEST[79:64];
    ELSE DEST[79:64] ← SRC[79:64]; FI;
IF (DEST[95:80] > SRC[95:80])
    THEN DEST[95:80] ← DEST[95:80];
    ELSE DEST[95:80] ← SRC[95:80]; FI;
IF (DEST[111:96] > SRC[111:96])
    THEN DEST[111:96] ← DEST[111:96];
    ELSE DEST[111:96] ← SRC[111:96]; FI;
IF (DEST[127:112] > SRC[127:112])
    THEN DEST[127:112] ← DEST[127:112];
    ELSE DEST[127:112] ← SRC[127:112]; FI;

```


Intel C/C++ Compiler Intrinsic Equivalent

PMAXUW__m128i__mm_max_epu16 (__m128i a, __m128i b);

Flags Affected

None

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PMINSB — Minimum of Packed Signed Byte Integers

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------|--|-------------|------------------|--|
| 66 OF 38 38 /r | PMINSB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed byte integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed minimum values in <i>xmm1</i> . |

Description

Compares packed signed byte integers in the destination operand (first operand) and the source operand (second operand), and returns the minimum for each packed value in the destination operand.

Operation

```

IF (DEST[7:0] < SRC[7:0])
    THEN DEST[7:0] ← DEST[7:0];
    ELSE DEST[7:0] ← SRC[7:0]; FI;
IF (DEST[15:8] < SRC[15:8])
    THEN DEST[15:8] ← DEST[15:8];
    ELSE DEST[15:8] ← SRC[15:8]; FI;
IF (DEST[23:16] < SRC[23:16])
    THEN DEST[23:16] ← DEST[23:16];
    ELSE DEST[23:16] ← SRC[23:16]; FI;
IF (DEST[31:24] < SRC[31:24])
    THEN DEST[31:24] ← DEST[31:24];
    ELSE DEST[31:24] ← SRC[31:24]; FI;
IF (DEST[39:32] < SRC[39:32])
    THEN DEST[39:32] ← DEST[39:32];
    ELSE DEST[39:32] ← SRC[39:32]; FI;
IF (DEST[47:40] < SRC[47:40])
    THEN DEST[47:40] ← DEST[47:40];
    ELSE DEST[47:40] ← SRC[47:40]; FI;
IF (DEST[55:48] < SRC[55:48])
    THEN DEST[55:48] ← DEST[55:48];
    ELSE DEST[55:48] ← SRC[55:48]; FI;
IF (DEST[63:56] < SRC[63:56])
    THEN DEST[63:56] ← DEST[63:56];
    ELSE DEST[63:56] ← SRC[63:56]; FI;
IF (DEST[71:64] < SRC[71:64])
    THEN DEST[71:64] ← DEST[71:64];

```

```

ELSE DEST[71:64] ← SRC[71:64]; FI;
IF (DEST[79:72] < SRC[79:72])
  THEN DEST[79:72] ← DEST[79:72];
  ELSE DEST[79:72] ← SRC[79:72]; FI;
IF (DEST[87:80] < SRC[87:80])
  THEN DEST[87:80] ← DEST[87:80];
  ELSE DEST[87:80] ← SRC[87:80]; FI;
IF (DEST[95:88] < SRC[95:88])
  THEN DEST[95:88] ← DEST[95:88];
  ELSE DEST[95:88] ← SRC[95:88]; FI;
IF (DEST[103:96] < SRC[103:96])
  THEN DEST[103:96] ← DEST[103:96];
  ELSE DEST[103:96] ← SRC[103:96]; FI;
IF (DEST[111:104] < SRC[111:104])
  THEN DEST[111:104] ← DEST[111:104];
  ELSE DEST[111:104] ← SRC[111:104]; FI;
IF (DEST[119:112] < SRC[119:112])
  THEN DEST[119:112] ← DEST[119:112];
  ELSE DEST[119:112] ← SRC[119:112]; FI;
IF (DEST[127:120] < SRC[127:120])
  THEN DEST[127:120] ← DEST[127:120];
  ELSE DEST[127:120] ← SRC[127:120]; FI;

```

Intel C/C++ Compiler Intrinsic Equivalent

PMINSB `__m128i_mm_min_epi8 (__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

| | |
|------------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. |

Either the prefix REP (F3h) or REPN (F2H) is used.

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to OFFFh. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PMINSD – Minimum of Packed Dword Integers

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|----------------|--|-------------|-----------------|---|
| 66 0F 38 39 /r | PMINSD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed signed dword integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed minimum values in <i>xmm1</i> . |

Description

Compares packed signed dword integers in the destination operand (first operand) and the source operand (second operand), and returns the minimum for each packed value in the destination operand.

Operation

```
IF (DEST[31:0] < SRC[31:0])
    THEN DEST[31:0] ← DEST[31:0];
    ELSE DEST[31:0] ← SRC[31:0]; FI;
IF (DEST[63:32] < SRC[63:32])
    THEN DEST[63:32] ← DEST[63:32];
    ELSE DEST[63:32] ← SRC[63:32]; FI;
IF (DEST[95:64] < SRC[95:64])
    THEN DEST[95:64] ← DEST[95:64];
    ELSE DEST[95:64] ← SRC[95:64]; FI;
IF (DEST[127:96] < SRC[127:96])
    THEN DEST[127:96] ← DEST[127:96];
    ELSE DEST[127:96] ← SRC[127:96]; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

PMINSD `__m128i _mm_min_epi32 (__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. |

Either the prefix REP (F3h) or REPN (F2H) is used.

PMINSW—Minimum of Packed Signed Word Integers

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--|-------------|-----------------|---|
| 0F EA /r | PMINSW <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Compare signed word integers in <i>mm2/m64</i> and <i>mm1</i> and return minimum values. |
| 66 0F EA /r | PMINSW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare signed word integers in <i>xmm2/m128</i> and <i>xmm1</i> and return minimum values. |

Description

Performs a SIMD compare of the packed signed word integers in the destination operand (first operand) and the source operand (second operand), and returns the minimum value for each pair of word integers to the destination operand. The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PMINSW instruction for 64-bit operands:

```
IF DEST[15:0] < SRC[15:0] THEN
    DEST[15:0] ← DEST[15:0];
ELSE
    DEST[15:0] ← SRC[15:0]; FI;
(* Repeat operation for 2nd and 3rd words in source and destination operands *)
IF DEST[63:48] < SRC[63:48] THEN
    DEST[63:48] ← DEST[63:48];
ELSE
    DEST[63:48] ← SRC[63:48]; FI;
```

PMINSW instruction for 128-bit operands:

```
IF DEST[15:0] < SRC[15:0] THEN
    DEST[15:0] ← DEST[15:0];
ELSE
    DEST[15:0] ← SRC[15:0]; FI;
(* Repeat operation for 2nd through 7th words in source and destination operands *)
IF DEST[127:112] < SRC/m64[127:112] THEN
    DEST[127:112] ← DEST[127:112];
```

ELSE

DEST[127:112] ← SRC[127:112]; FI;

Intel C/C++ Compiler Intrinsic Equivalent

PMINSW __m64_mm_min_pi16 (__m64 a, __m64 b)

PMINSW __m128i_mm_min_epi16 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. |

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

If the LOCK prefix is used.

#NM

If CR0.TS[bit 3] = 1.

#MF

(64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

(128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.

(128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PMINUB—Minimum of Packed Unsigned Byte Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F DA /r | PMINUB <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Compare unsigned byte integers in <i>mm2/m64</i> and <i>mm1</i> and returns minimum values. |
| 66 0F DA /r | PMINUB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare unsigned byte integers in <i>xmm2/m128</i> and <i>xmm1</i> and returns minimum values. |

Description

Performs a SIMD compare of the packed unsigned byte integers in the destination operand (first operand) and the source operand (second operand), and returns the minimum value for each pair of byte integers to the destination operand. The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PMINUB instruction for 64-bit operands:

```
IF DEST[7:0] < SRC[17:0] THEN
    DEST[7:0] ← DEST[7:0];
ELSE
    DEST[7:0] ← SRC[7:0]; FI;
(* Repeat operation for 2nd through 7th bytes in source and destination operands *)
IF DEST[63:56] < SRC[63:56] THEN
    DEST[63:56] ← DEST[63:56];
ELSE
    DEST[63:56] ← SRC[63:56]; FI;
```

PMINUB instruction for 128-bit operands:

```
IF DEST[7:0] < SRC[17:0] THEN
    DEST[7:0] ← DEST[7:0];
ELSE
    DEST[7:0] ← SRC[7:0]; FI;
(* Repeat operation for 2nd through 15th bytes in source and destination operands *)
IF DEST[127:120] < SRC[127:120] THEN
    DEST[127:120] ← DEST[127:120];
```

ELSE

DEST[127:120] ← SRC[127:120]; FI;

Intel C/C++ Compiler Intrinsic Equivalent

PMINUB __m64 _m_min_pu8 (__m64 a, __m64 b)

PMINUB __m128i _mm_min_epu8 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
|-----|---|

| | |
|-----|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMINUD – Minimum of Packed Dword Integers

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|-------------------|--|-------------|-----------------|---|
| 66 OF 38 3B /r | PMINUD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed unsigned dword integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed minimum values in <i>xmm1</i> . |

Description

Compares packed unsigned dword integers in the destination operand (first operand) and the source operand (second operand), and returns the minimum for each packed value in the destination operand.

Operation

```
IF (DEST[31:0] < SRC[31:0])
    THEN DEST[31:0] ← DEST[31:0];
    ELSE DEST[31:0] ← SRC[31:0]; FI;
IF (DEST[63:32] < SRC[63:32])
    THEN DEST[63:32] ← DEST[63:32];
    ELSE DEST[63:32] ← SRC[63:32]; FI;
IF (DEST[95:64] < SRC[95:64])
    THEN DEST[95:64] ← DEST[95:64];
    ELSE DEST[95:64] ← SRC[95:64]; FI;
IF (DEST[127:96] < SRC[127:96])
    THEN DEST[127:96] ← DEST[127:96];
    ELSE DEST[127:96] ← SRC[127:96]; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

PMINUD __m128i __mm_min_epu32 (__m128i a, __m128i b);

Flags Affected

None

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|--|
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. |

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

PMINUW — Minimum of Packed Word Integers

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------|--|-------------|------------------|--|
| 66 OF 38 3A /r | PMINUW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Compare packed unsigned word integers in <i>xmm1</i> and <i>xmm2/m128</i> and store packed minimum values in <i>xmm1</i> . |

Description

Compares packed unsigned word integers in the destination operand (first operand) and the source operand (second operand), and returns the minimum for each packed value in the destination operand.

Operation

```

IF (DEST[15:0] < SRC[15:0])
    THEN DEST[15:0] ← DEST[15:0];
    ELSE DEST[15:0] ← SRC[15:0]; FI;
IF (DEST[31:16] < SRC[31:16])
    THEN DEST[31:16] ← DEST[31:16];
    ELSE DEST[31:16] ← SRC[31:16]; FI;
IF (DEST[47:32] < SRC[47:32])
    THEN DEST[47:32] ← DEST[47:32];
    ELSE DEST[47:32] ← SRC[47:32]; FI;
IF (DEST[63:48] < SRC[63:48])
    THEN DEST[63:48] ← DEST[63:48];
    ELSE DEST[63:48] ← SRC[63:48]; FI;
IF (DEST[79:64] < SRC[79:64])
    THEN DEST[79:64] ← DEST[79:64];
    ELSE DEST[79:64] ← SRC[79:64]; FI;
IF (DEST[95:80] < SRC[95:80])
    THEN DEST[95:80] ← DEST[95:80];
    ELSE DEST[95:80] ← SRC[95:80]; FI;
IF (DEST[111:96] < SRC[111:96])
    THEN DEST[111:96] ← DEST[111:96];
    ELSE DEST[111:96] ← SRC[111:96]; FI;
IF (DEST[127:112] < SRC[127:112])
    THEN DEST[127:112] ← DEST[127:112];
    ELSE DEST[127:112] ← SRC[127:112]; FI;

```

Intel C/C++ Compiler Intrinsic Equivalent

PMINUW `__m128i __mm_min_epu16 (__m128i a, __m128i b);`

Flags Affected

None

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PMOVMSKB—Move Byte Mask

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------------|----------------------------|-------------|------------------|--|
| 0F D7 /r | PMOVMSKB <i>r32, mm</i> | Valid | Valid | Move a byte mask of <i>mm</i> to <i>r32</i> . |
| REX.W + 0F D7 /r | PMOVMSKB <i>r64, mm</i> | Valid | N.E. | Move a byte mask of <i>mm</i> to the lower 32-bits of <i>r64</i> and zero-fill the upper 32-bits. |
| 66 0F D7 /r | PMOVMSKB <i>reg, xmm</i> | Valid | Valid | Move a byte mask of <i>xmm</i> to <i>reg</i> . The upper bits of <i>r32</i> or <i>r64</i> are zeroed |

Description

Creates a mask made up of the most significant bit of each byte of the source operand (second operand) and stores the result in the low byte or word of the destination operand (first operand). The source operand is an MMX technology register or an XMM register; the destination operand is a general-purpose register. When operating on 64-bit operands, the byte mask is 8 bits; when operating on 128-bit operands, the byte mask is 16-bits.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15, R8-15). The default operand size is 64-bit in 64-bit mode.

Operation

PMOVMSKB instruction with 64-bit source operand and *r32*:

```
r32[0] ← SRC[7];
r32[1] ← SRC[15];
(* Repeat operation for bytes 2 through 6 *)
r32[7] ← SRC[63];
r32[31:8] ← ZERO_FILL;
```

PMOVMSKB instruction with 128-bit source operand and *r32*:

```
r32[0] ← SRC[7];
r32[1] ← SRC[15];
(* Repeat operation for bytes 2 through 14 *)
r32[15] ← SRC[127];
r32[31:16] ← ZERO_FILL;
```

PMOVMSKB instruction with 64-bit source operand and *r64*:

```
r64[0] ← SRC[7];
r64[1] ← SRC[15];
```

(* Repeat operation for bytes 2 through 6 *)

r64[7] ← SRC[63];

r64[63:8] ← ZERO_FILL;

PMOVMSKB instruction with 128-bit source operand and r64:

r64[0] ← SRC[7];

r64[1] ← SRC[15];

(* Repeat operation for bytes 2 through 14 *)

r64[15] ← SRC[127];

r64[63:16] ← ZERO_FILL;

Intel C/C++ Compiler Intrinsic Equivalent

PMOVMSKB int __mm_movemask_pi8(__m64 a)

PMOVMSKB int __mm_movemask_epi8 (__m128i a)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

- #UD If CR0.EM[bit 2] = 1.
(128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
If the LOCK prefix is used.
- #NM If CR0.TS[bit 3] = 1.
- #MF (64-bit operations only) If there is a pending x87 FPU exception.

Real-Address Mode Exceptions

Same exceptions as in protected mode.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

PMOVSX — Packed Move with Sign Extend

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|-------------------|---|-------------|-----------------|---|
| 66 Of 38 20 /r | PMOVSXBW <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Sign extend 8 packed signed 8-bit integers in the low 8 bytes of <i>xmm2/m64</i> to 8 packed signed 16-bit integers in <i>xmm1</i> . |
| 66 Of 38 21 /r | PMOVSXBD <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Sign extend 4 packed signed 8-bit integers in the low 4 bytes of <i>xmm2/m32</i> to 4 packed signed 32-bit integers in <i>xmm1</i> . |
| 66 Of 38 22 /r | PMOVSXBQ <i>xmm1</i> , <i>xmm2/m16</i> | Valid | Valid | Sign extend 2 packed signed 8-bit integers in the low 2 bytes of <i>xmm2/m16</i> to 2 packed signed 64-bit integers in <i>xmm1</i> . |
| 66 Of 38 23 /r | PMOVSXWD <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Sign extend 4 packed signed 16-bit integers in the low 8 bytes of <i>xmm2/m64</i> to 4 packed signed 32-bit integers in <i>xmm1</i> . |
| 66 Of 38 24 /r | PMOVSXWQ <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Sign extend 2 packed signed 16-bit integers in the low 4 bytes of <i>xmm2/m32</i> to 2 packed signed 64-bit integers in <i>xmm1</i> . |
| 66 Of 38 25 /r | PMOVSXDQ <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Sign extend 2 packed signed 32-bit integers in the low 8 bytes of <i>xmm2/m64</i> to 2 packed signed 64-bit integers in <i>xmm1</i> . |

Description

Sign-extend the low byte/word/dword values in each word/dword/qword element of the source operand (second operand) to word/dword/qword integers and stored as packed data in the destination operand (first operand).

Operation

PMOVSXBW

```

DEST[15:0] ← SignExtend(SRC[7:0]);
DEST[31:16] ← SignExtend(SRC[15:8]);
DEST[47:32] ← SignExtend(SRC[23:16]);
DEST[63:48] ← SignExtend(SRC[31:24]);
DEST[79:64] ← SignExtend(SRC[39:32]);

```


DEST[95:80] ← SignExtend(SRC[47:40]);
 DEST[111:96] ← SignExtend(SRC[55:48]);
 DEST[127:112] ← SignExtend(SRC[63:56]);

PMOVSB

DEST[31:0] ← SignExtend(SRC[7:0]);
 DEST[63:32] ← SignExtend(SRC[15:8]);
 DEST[95:64] ← SignExtend(SRC[23:16]);
 DEST[127:96] ← SignExtend(SRC[31:24]);

PMOVSBQ

DEST[63:0] ← SignExtend(SRC[7:0]);
 DEST[127:64] ← SignExtend(SRC[15:8]);

PMOVSWD

DEST[31:0] ← SignExtend(SRC[15:0]);
 DEST[63:32] ← SignExtend(SRC[31:16]);
 DEST[95:64] ← SignExtend(SRC[47:32]);
 DEST[127:96] ← SignExtend(SRC[63:48]);

PMOVSWQ

DEST[63:0] ← SignExtend(SRC[15:0]);
 DEST[127:64] ← SignExtend(SRC[31:16]);

PMOVSDQ

DEST[63:0] ← SignExtend(SRC[31:0]);
 DEST[127:64] ← SignExtend(SRC[63:32]);

Flags Affected

None

Intel C/C++ Compiler Intrinsic Equivalent

PMOVSBW __m128i __mm_cvtepi8_epi16 (__m128i a);
 PMOVSB __m128i __mm_cvtepi8_epi32 (__m128i a);
 PMOVSBQ __m128i __mm_cvtepi8_epi64 (__m128i a);
 PMOVSWD __m128i __mm_cvtepi16_epi32 (__m128i a);
 PMOVSWQ __m128i __mm_cvtepi16_epi64 (__m128i a);
 PMOVSDQ __m128i __mm_cvtepi32_epi64 (__m128i a);

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
 #SS(0) For an illegal address in the SS segment.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|-----|--|
| #GP | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. |

#AC(0)

Either the prefix REP (F3h) or REPN (F2H) is used.

If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PMOVZX — Packed Move with Zero Extend

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|-------------------|---|-------------|-----------------|---|
| 66 Of 38 30 /r | PMOVZXBW <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Zero extend 8 packed 8-bit integers in the low 8 bytes of <i>xmm2/m64</i> to 8 packed 16-bit integers in <i>xmm1</i> . |
| 66 Of 38 31 /r | PMOVZXBW <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Zero extend 4 packed 8-bit integers in the low 4 bytes of <i>xmm2/m32</i> to 4 packed 32-bit integers in <i>xmm1</i> . |
| 66 Of 38 32 /r | PMOVZXBQ <i>xmm1</i> , <i>xmm2/m16</i> | Valid | Valid | Zero extend 2 packed 8-bit integers in the low 2 bytes of <i>xmm2/m16</i> to 2 packed 64-bit integers in <i>xmm1</i> . |
| 66 Of 38 33 /r | PMOVZXWD <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Zero extend 4 packed 16-bit integers in the low 8 bytes of <i>xmm2/m64</i> to 4 packed 32-bit integers in <i>xmm1</i> . |
| 66 Of 38 34 /r | PMOVZXWQ <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Zero extend 2 packed 16-bit integers in the low 4 bytes of <i>xmm2/m32</i> to 2 packed 64-bit integers in <i>xmm1</i> . |
| 66 Of 38 35 /r | PMOVZXDQ <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Zero extend 2 packed 32-bit integers in the low 8 bytes of <i>xmm2/m64</i> to 2 packed 64-bit integers in <i>xmm1</i> . |

Description

Zero-extend the low byte/word/dword values in each word/dword/qword element of the source operand (second operand) to word/dword/qword integers and stored as packed data in the destination operand (first operand).

Operation

PMOVZXBW

```
DEST[15:0] ← ZeroExtend(SRC[7:0]);
DEST[31:16] ← ZeroExtend(SRC[15:8]);
DEST[47:32] ← ZeroExtend(SRC[23:16]);
DEST[63:48] ← ZeroExtend(SRC[31:24]);
DEST[79:64] ← ZeroExtend(SRC[39:32]);
DEST[95:80] ← ZeroExtend(SRC[47:40]);
DEST[111:96] ← ZeroExtend(SRC[55:48]);
DEST[127:112] ← ZeroExtend(SRC[63:56]);
```

PMOVZXBW

```
DEST[31:0] ← ZeroExtend(SRC[7:0]);
```

DEST[63:32] ← ZeroExtend(SRC[15:8]);
 DEST[95:64] ← ZeroExtend(SRC[23:16]);
 DEST[127:96] ← ZeroExtend(SRC[31:24]);

PMOVZXQB

DEST[63:0] ← ZeroExtend(SRC[7:0]);
 DEST[127:64] ← ZeroExtend(SRC[15:8]);

PMOVZXWD

DEST[31:0] ← ZeroExtend(SRC[15:0]);
 DEST[63:32] ← ZeroExtend(SRC[31:16]);
 DEST[95:64] ← ZeroExtend(SRC[47:32]);
 DEST[127:96] ← ZeroExtend(SRC[63:48]);

PMOVZXWQ

DEST[63:0] ← ZeroExtend(SRC[15:0]);
 DEST[127:64] ← ZeroExtend(SRC[31:16]);

PMOVZXDQ

DEST[63:0] ← ZeroExtend(SRC[31:0]);
 DEST[127:64] ← ZeroExtend(SRC[63:32]);

Flags Affected

None

Intel C/C++ Compiler Intrinsic Equivalent

PMOVZXBW __m128i_mm_cvtepu8_epi16 (__m128i a);
 PMOVZXBQ __m128i_mm_cvtepu8_epi32 (__m128i a);
 PMOVZXBQ __m128i_mm_cvtepu8_epi64 (__m128i a);
 PMOVZXWD __m128i_mm_cvtepu16_epi32 (__m128i a);
 PMOVZXWQ __m128i_mm_cvtepu16_epi64 (__m128i a);
 PMOVZXDQ __m128i_mm_cvtepu32_epi64 (__m128i a);

Flags Affected

None

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
 #SS(0) For an illegal address in the SS segment.
 #PF(fault-code) For a page fault.
 #NM If CR0.TS[bit 3] = 1.

| | |
|--------|---|
| #UD | <p>If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

Real Mode Exceptions

| | |
|-----|---|
| #GP | <p>if any part of the operand lies outside of the effective address space from 0 to 0FFFFH.</p> |
| #NM | <p>If CR0.TS[bit 3] = 1.</p> |
| #UD | <p>If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used.</p> |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|---|
| #PF(fault-code) | <p>For a page fault.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | <p>If the memory address is in a non-canonical form.</p> |
| #SS(0) | <p>If a memory address referencing the SS segment is in a non-canonical form.</p> |
| #PF(fault-code) | <p>For a page fault.</p> |
| #NM | <p>If TS in CR0 is set.</p> |
| #UD | <p>If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used.</p> |

#AC(0)

If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PMULDQ — Multiply Packed Signed Dword Integers

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|-------------------|--|-------------|-----------------|---|
| 66 OF 38 28 /r | PMULDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply the packed signed dword integers in <i>xmm1</i> and <i>xmm2/m128</i> and store the quadword product in <i>xmm1</i> . |

Description

Performs two signed multiplications from two pairs of signed dword integers and stores two 64-bit products in the destination operand (first operand). The 64-bit product from the first/third dword element in the destination operand and the first/third dword element of the source operand (second operand) is stored to the low/high qword element of the destination.

If the source is a memory operand then all 128 bits will be fetched from memory but the second and fourth dwords will not be used in the computation.

Operation

```
DEST[63:0] = DEST[31:0] * SRC[31:0];
DEST[127:64] = DEST[95:64] * SRC[95:64];
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PMULDQ    __m128i __mm_mul_epi32( __m128i a, __m128i b);
```

Flags Affected

None

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. |

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PMULHRWSW — Packed Multiply High with Round and Scale

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|---------------------------------|-------------|------------------|--|
| 0F 38 0B /r | PMULHRWSW mm1, mm2/m64 | Valid | Valid | Multiply 16-bit signed words, scale and round signed doublewords, pack high 16 bits to MM1. |
| 66 0F 38 0B /r | PMULHRWSW xmm1, xmm2/m128 | Valid | Valid | Multiply 16-bit signed words, scale and round signed doublewords, pack high 16 bits to XMM1. |

Description

PMULHRWSW multiplies vertically each signed 16-bit integer from the destination operand (first operand) with the corresponding signed 16-bit integer of the source operand (second operand), producing intermediate, signed 32-bit integers. Each intermediate 32-bit integer is truncated to the 18 most significant bits. Rounding is always performed by adding 1 to the least significant bit of the 18-bit intermediate result. The final result is obtained by selecting the 16 bits immediately to the right of the most significant bit of each 18-bit intermediate result and packed to the destination operand. Both operands can be MMX register or XMM registers.

When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PMULHRWSW with 64-bit operands:

```
temp0[31:0] = INT32 ((DEST[15:0] * SRC[15:0]) >>14) + 1;
temp1[31:0] = INT32 ((DEST[31:16] * SRC[31:16]) >>14) + 1;
temp2[31:0] = INT32 ((DEST[47:32] * SRC[47:32]) >> 14) + 1;
temp3[31:0] = INT32 ((DEST[63:48] * SRC[63:48]) >> 14) + 1;
DEST[15:0] = temp0[16:1];
DEST[31:16] = temp1[16:1];
DEST[47:32] = temp2[16:1];
DEST[63:48] = temp3[16:1];
```

PMULHRWSW with 128-bit operand:

```
temp0[31:0] = INT32 ((DEST[15:0] * SRC[15:0]) >>14) + 1;
temp1[31:0] = INT32 ((DEST[31:16] * SRC[31:16]) >>14) + 1;
temp2[31:0] = INT32 ((DEST[47:32] * SRC[47:32]) >>14) + 1;
```

```

temp3[31:0] = INT32 ((DEST[63:48] * SRC[63:48]) >>14) + 1;
temp4[31:0] = INT32 ((DEST[79:64] * SRC[79:64]) >>14) + 1;
temp5[31:0] = INT32 ((DEST[95:80] * SRC[95:80]) >>14) + 1;
temp6[31:0] = INT32 ((DEST[111:96] * SRC[111:96]) >>14) + 1;
temp7[31:0] = INT32 ((DEST[127:112] * SRC[127:112]) >>14) + 1;
DEST[15:0] = temp0[16:1];
DEST[31:16] = temp1[16:1];
DEST[47:32] = temp2[16:1];
DEST[63:48] = temp3[16:1];
DEST[79:64] = temp4[16:1];
DEST[95:80] = temp5[16:1];
DEST[111:96] = temp6[16:1];
DEST[127:112] = temp7[16:1];

```

Intel C/C++ Compiler Intrinsic Equivalents

```

PMULHRWSW    __m64 __mm_mulhrs_pi16 (__m64 a, __m64 b)
PMULHRWSW    __m128i __mm_mulhrs_epi16 (__m128i a, __m128i b)

```

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS or GS segments. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
|--------|--|

| | |
|-----|--|
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMULHUW—Multiply Packed Unsigned Integers and Store High Result

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|--|
| 0F E4 /r | PMULHUW <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Multiply the packed unsigned word integers in <i>mm1</i> register and <i>mm2/m64</i> , and store the high 16 bits of the results in <i>mm1</i> . |
| 66 0F E4 /r | PMULHUW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply the packed unsigned word integers in <i>xmm1</i> and <i>xmm2/m128</i> , and store the high 16 bits of the results in <i>xmm1</i> . |

Description

Performs a SIMD unsigned multiply of the packed unsigned word integers in the destination operand (first operand) and the source operand (second operand), and stores the high 16 bits of each 32-bit intermediate results in the destination operand. (Figure 4-3 shows this operation when using 64-bit operands.) The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

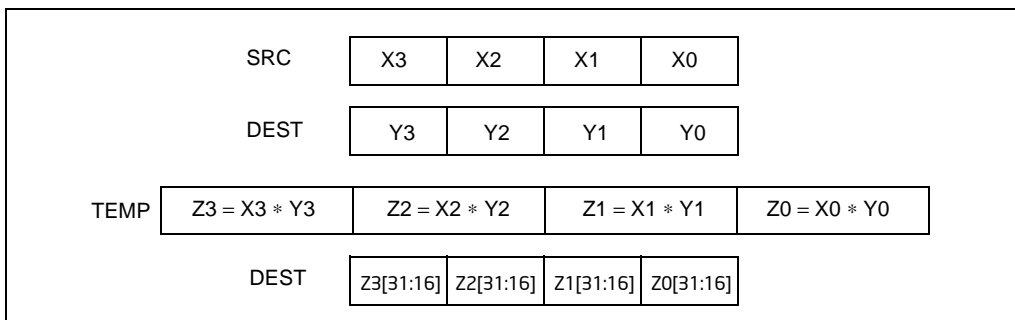


Figure 4-3. PMULHUW and PMULHW Instruction Operation Using 64-bit Operands

Operation

PMULHUW instruction with 64-bit operands:

```

TEMP0[31:0] ← DEST[15:0] * SRC[15:0]; (* Unsigned multiplication *)
TEMP1[31:0] ← DEST[31:16] * SRC[31:16];
TEMP2[31:0] ← DEST[47:32] * SRC[47:32];

```

TEMP3[31:0] ← DEST[63:48] * SRC[63:48];
 DEST[15:0] ← TEMP0[31:16];
 DEST[31:16] ← TEMP1[31:16];
 DEST[47:32] ← TEMP2[31:16];
 DEST[63:48] ← TEMP3[31:16];

PMULHUW instruction with 128-bit operands:

TEMP0[31:0] ← DEST[15:0] * SRC[15:0]; (* Unsigned multiplication *)
 TEMP1[31:0] ← DEST[31:16] * SRC[31:16];
 TEMP2[31:0] ← DEST[47:32] * SRC[47:32];
 TEMP3[31:0] ← DEST[63:48] * SRC[63:48];
 TEMP4[31:0] ← DEST[79:64] * SRC[79:64];
 TEMP5[31:0] ← DEST[95:80] * SRC[95:80];
 TEMP6[31:0] ← DEST[111:96] * SRC[111:96];
 TEMP7[31:0] ← DEST[127:112] * SRC[127:112];
 DEST[15:0] ← TEMP0[31:16];
 DEST[31:16] ← TEMP1[31:16];
 DEST[47:32] ← TEMP2[31:16];
 DEST[63:48] ← TEMP3[31:16];
 DEST[79:64] ← TEMP4[31:16];
 DEST[95:80] ← TEMP5[31:16];
 DEST[111:96] ← TEMP6[31:16];
 DEST[127:112] ← TEMP7[31:16];

Intel C/C++ Compiler Intrinsic Equivalent

PMULHUW __m64 _mm_mulhi_pu16(__m64 a, __m64 b)
 PMULHUW __m128i _mm_mulhi_epu16 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
 #SS(0) If a memory operand effective address is outside the SS segment limit.

| | |
|-----------------|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |

| | |
|-----------------|---|
| | (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMULHW—Multiply Packed Signed Integers and Store High Result

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F E5 /r | PMULHW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Multiply the packed signed word integers in <i>mm1</i> register and <i>mm2/m64</i> , and store the high 16 bits of the results in <i>mm1</i> . |
| 66 0F E5 /r | PMULHW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply the packed signed word integers in <i>xmm1</i> and <i>xmm2/m128</i> , and store the high 16 bits of the results in <i>xmm1</i> . |

Description

Performs a SIMD signed multiply of the packed signed word integers in the destination operand (first operand) and the source operand (second operand), and stores the high 16 bits of each intermediate 32-bit result in the destination operand. (Figure 4-3 shows this operation when using 64-bit operands.) The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PMULHW instruction with 64-bit operands:

```

TEMP0[31:0] ← DEST[15:0] * SRC[15:0]; (* Signed multiplication *)
TEMP1[31:0] ← DEST[31:16] * SRC[31:16];
TEMP2[31:0] ← DEST[47:32] * SRC[47:32];
TEMP3[31:0] ← DEST[63:48] * SRC[63:48];
DEST[15:0] ← TEMP0[31:16];
DEST[31:16] ← TEMP1[31:16];
DEST[47:32] ← TEMP2[31:16];
DEST[63:48] ← TEMP3[31:16];

```

PMULHW instruction with 128-bit operands:

```

TEMP0[31:0] ← DEST[15:0] * SRC[15:0]; (* Signed multiplication *)
TEMP1[31:0] ← DEST[31:16] * SRC[31:16];
TEMP2[31:0] ← DEST[47:32] * SRC[47:32];
TEMP3[31:0] ← DEST[63:48] * SRC[63:48];
TEMP4[31:0] ← DEST[79:64] * SRC[79:64];
TEMP5[31:0] ← DEST[95:80] * SRC[95:80];

```

TEMP6[31:0] ← DEST[111:96] * SRC[111:96];
 TEMP7[31:0] ← DEST[127:112] * SRC[127:112];
 DEST[15:0] ← TEMP0[31:16];
 DEST[31:16] ← TEMP1[31:16];
 DEST[47:32] ← TEMP2[31:16];
 DEST[63:48] ← TEMP3[31:16];
 DEST[79:64] ← TEMP4[31:16];
 DEST[95:80] ← TEMP5[31:16];
 DEST[111:96] ← TEMP6[31:16];
 DEST[127:112] ← TEMP7[31:16];

Intel C/C++ Compiler Intrinsic Equivalent

PMULHW __m64 __mm_mulhi_pi16 (__m64 m1, __m64 m2)

PMULHW __m128i __mm_mulhi_epi16 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | <p>If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.</p> |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | <p>If CR0.EM[bit 2] = 1.</p> <p>128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.</p> <p>If the LOCK prefix is used.</p> |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMULLD — Multiply Packed Signed Dword Integers and Store Low Result

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------|--|-------------|------------------|--|
| 66 0F 38 40 /r | PMULLD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply the packed dword signed integers in <i>xmm1</i> and <i>xmm2/m128</i> and store the low 32 bits of each product in <i>xmm1</i> . |

Description

Performs four signed multiplications from four pairs of signed dword integers and stores the lower 32 bits of the four 64-bit products in the destination operand (first operand). Each dword element in the destination operand is multiplied with the corresponding dword element of the source operand (second operand) to obtain a 64-bit intermediate product.

Operation

```
Temp0[63:0] ← DEST[31:0] * SRC[31:0];
Temp1[63:0] ← DEST[63:32] * SRC[63:32];
Temp2[63:0] ← DEST[95:64] * SRC[95:64];
Temp3[63:0] ← DEST[127:96] * SRC[127:96];
DEST[31:0] ← Temp0[31:0];
DEST[63:32] ← Temp1[31:0];
DEST[95:64] ← Temp2[31:0];
DEST[127:96] ← Temp3[31:0];
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PMULLUD __m128i _mm_mullo_epi32(__m128i a, __m128i b);
```

Flags Affected

None

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.
- #PF(fault-code) For a page fault.

| | |
|-----|--|
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

PMULLW—Multiply Packed Signed Integers and Store Low Result

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|---|
| 0F D5 /r | PMULLW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Multiply the packed signed word integers in <i>mm1</i> register and <i>mm2/m64</i> , and store the low 16 bits of the results in <i>mm1</i> . |
| 66 0F D5 /r | PMULLW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply the packed signed word integers in <i>xmm1</i> and <i>xmm2/m128</i> , and store the low 16 bits of the results in <i>xmm1</i> . |

Description

Performs a SIMD signed multiply of the packed signed word integers in the destination operand (first operand) and the source operand (second operand), and stores the low 16 bits of each intermediate 32-bit result in the destination operand. (Figure 4-3 shows this operation when using 64-bit operands.) The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

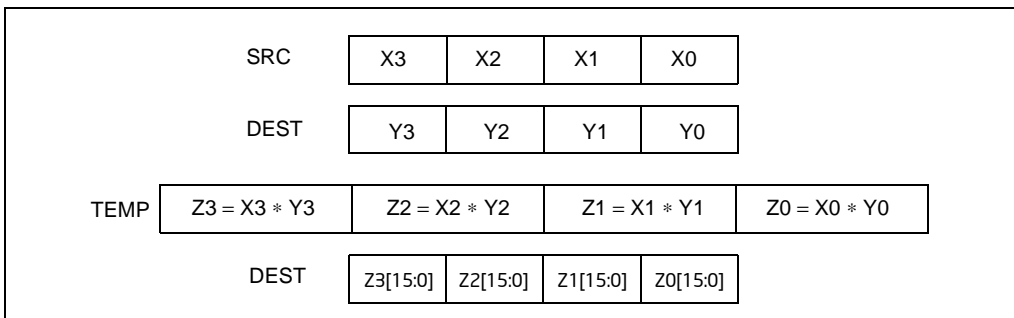


Figure 4-4. PMULLU Instruction Operation Using 64-bit Operands

Operation

PMULLW instruction with 64-bit operands:

TEMP0[31:0] ← DEST[15:0] * SRC[15:0]; (* Signed multiplication *)
 TEMP1[31:0] ← DEST[31:16] * SRC[31:16];
 TEMP2[31:0] ← DEST[47:32] * SRC[47:32];
 TEMP3[31:0] ← DEST[63:48] * SRC[63:48];

DEST[15:0] ← TEMP0[15:0];
 DEST[31:16] ← TEMP1[15:0];
 DEST[47:32] ← TEMP2[15:0];
 DEST[63:48] ← TEMP3[15:0];

PMULLW instruction with 128-bit operands:

TEMP0[31:0] ← DEST[15:0] * SRC[15:0]; (* Signed multiplication *)
 TEMP1[31:0] ← DEST[31:16] * SRC[31:16];
 TEMP2[31:0] ← DEST[47:32] * SRC[47:32];
 TEMP3[31:0] ← DEST[63:48] * SRC[63:48];
 TEMP4[31:0] ← DEST[79:64] * SRC[79:64];
 TEMP5[31:0] ← DEST[95:80] * SRC[95:80];
 TEMP6[31:0] ← DEST[111:96] * SRC[111:96];
 TEMP7[31:0] ← DEST[127:112] * SRC[127:112];
 DEST[15:0] ← TEMP0[15:0];
 DEST[31:16] ← TEMP1[15:0];
 DEST[47:32] ← TEMP2[15:0];
 DEST[63:48] ← TEMP3[15:0];
 DEST[79:64] ← TEMP4[15:0];
 DEST[95:80] ← TEMP5[15:0];
 DEST[111:96] ← TEMP6[15:0];
 DEST[127:112] ← TEMP7[15:0];

Intel C/C++ Compiler Intrinsic Equivalent

PMULLW __m64 _mm_mullo_pi16(__m64 m1, __m64 m2)

PMULLW __m128i _mm_mullo_epi16 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

- #GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) If a memory operand effective address is outside the SS segment limit.

| | |
|------------------|---|
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|------------------|--|
| #PF (fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PMULUDQ—Multiply Packed Unsigned Doubleword Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|--|
| 0F F4 /r | PMULUDQ <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Multiply unsigned doubleword integer in <i>mm1</i> by unsigned doubleword integer in <i>mm2/m64</i> , and store the quadword result in <i>mm1</i> . |
| 66 0F F4 /r | PMULUDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Multiply packed unsigned doubleword integers in <i>xmm1</i> by packed unsigned doubleword integers in <i>xmm2/m128</i> , and store the quadword results in <i>xmm1</i> . |

Description

Multiplies the first operand (destination operand) by the second operand (source operand) and stores the result in the destination operand. The source operand can be an unsigned doubleword integer stored in the low doubleword of an MMX technology register or a 64-bit memory location, or it can be two packed unsigned doubleword integers stored in the first (low) and third doublewords of an XMM register or an 128-bit memory location. The destination operand can be an unsigned doubleword integer stored in the low doubleword an MMX technology register or two packed doubleword integers stored in the first and third doublewords of an XMM register. The result is an unsigned quadword integer stored in the destination an MMX technology register or two packed unsigned quadword integers stored in an XMM register. When a quadword result is too large to be represented in 64 bits (overflow), the result is wrapped around and the low 64 bits are written to the destination element (that is, the carry is ignored).

For 64-bit memory operands, 64 bits are fetched from memory, but only the low doubleword is used in the computation; for 128-bit memory operands, 128 bits are fetched from memory, but only the first and third doublewords are used in the computation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PMULUDQ instruction with 64-Bit operands:

$$\text{DEST}[63:0] \leftarrow \text{DEST}[31:0] * \text{SRC}[31:0];$$

PMULUDQ instruction with 128-Bit operands:

$$\begin{aligned} \text{DEST}[63:0] &\leftarrow \text{DEST}[31:0] * \text{SRC}[31:0]; \\ \text{DEST}[127:64] &\leftarrow \text{DEST}[95:64] * \text{SRC}[95:64]; \end{aligned}$$

Intel C/C++ Compiler Intrinsic Equivalent

PMULUDQ `__m64 _mm_mul_su32` (`__m64 a`, `__m64 b`)
 PMULUDQ `__m128i _mm_mul_epu32` (`__m128i a`, `__m128i b`)

Flags Affected

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
 If CPUID.01H:EDX.SSE2[bit 26] = 0.
 If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
 If any part of the operand lies outside of the effective address space from 0 to FFFFH.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
 If CPUID.01H:EDX.SSE2[bit 26] = 0.
 If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

POP—Pop a Value from the Stack

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|---------------|------------------|-------------|---------------------|--|
| 8F /0 | POP <i>r/m16</i> | Valid | Valid | Pop top of stack into <i>m16</i> ; increment stack pointer. |
| 8F /0 | POP <i>r/m32</i> | N.E. | Valid | Pop top of stack into <i>m32</i> ; increment stack pointer. |
| 8F /0 | POP <i>r/m64</i> | Valid | N.E. | Pop top of stack into <i>m64</i> ; increment stack pointer. Cannot encode 32-bit operand size. |
| 58+ <i>rw</i> | POP <i>r16</i> | Valid | Valid | Pop top of stack into <i>r16</i> ; increment stack pointer. |
| 58+ <i>rd</i> | POP <i>r32</i> | N.E. | Valid | Pop top of stack into <i>r32</i> ; increment stack pointer. |
| 58+ <i>rd</i> | POP <i>r64</i> | Valid | N.E. | Pop top of stack into <i>r64</i> ; increment stack pointer. Cannot encode 32-bit operand size. |
| 1F | POP DS | Invalid | Valid | Pop top of stack into DS; increment stack pointer. |
| 07 | POP ES | Invalid | Valid | Pop top of stack into ES; increment stack pointer. |
| 17 | POP SS | Invalid | Valid | Pop top of stack into SS; increment stack pointer. |
| 0F A1 | POP FS | Valid | Valid | Pop top of stack into FS; increment stack pointer by 16 bits. |
| 0F A1 | POP FS | N.E. | Valid | Pop top of stack into FS; increment stack pointer by 32 bits. |
| 0F A1 | POP FS | Valid | N.E. | Pop top of stack into FS; increment stack pointer by 64 bits. |
| 0F A9 | POP GS | Valid | Valid | Pop top of stack into GS; increment stack pointer by 16 bits. |
| 0F A9 | POP GS | N.E. | Valid | Pop top of stack into GS; increment stack pointer by 32 bits. |
| 0F A9 | POP GS | Valid | N.E. | Pop top of stack into GS; increment stack pointer by 64 bits. |

Description

Loads the value from the top of the stack to the location specified with the destination operand (or explicit opcode) and then increments the stack pointer. The destination operand can be a general-purpose register, memory location, or segment register.

The address-size attribute of the stack segment determines the stack pointer size (16, 32, 64 bits) and the operand-size attribute of the current code segment determines the amount the stack pointer is incremented (2, 4, 8 bytes).

For example, if the address- and operand-size attributes are 32, the 32-bit ESP register (stack pointer) is incremented by 4; if they are 16, the 16-bit SP register is incremented by 2. (The B flag in the stack segment's segment descriptor determines the stack's address-size attribute, and the D flag in the current code segment's segment descriptor, along with prefixes, determines the operand-size attribute and also the address-size attribute of the destination operand.)

If the destination operand is one of the segment registers DS, ES, FS, GS, or SS, the value loaded into the register must be a valid segment selector. In protected mode, popping a segment selector into a segment register automatically causes the descriptor information associated with that segment selector to be loaded into the hidden (shadow) part of the segment register and causes the selector and the descriptor information to be validated (see the "Operation" section below).

A NULL value (0000-0003) may be popped into the DS, ES, FS, or GS register without causing a general protection fault. However, any subsequent attempt to reference a segment whose corresponding segment register is loaded with a NULL value causes a general protection exception (#GP). In this situation, no memory reference occurs and the saved value of the segment register is NULL.

The POP instruction cannot pop a value into the CS register. To load the CS register from the stack, use the RET instruction.

If the ESP register is used as a base register for addressing a destination operand in memory, the POP instruction computes the effective address of the operand after it increments the ESP register. For the case of a 16-bit stack where ESP wraps to 0H as a result of the POP instruction, the resulting location of the memory write is processor-family-specific.

The POP ESP instruction increments the stack pointer (ESP) before data at the old top of stack is written into the destination.

A POP SS instruction inhibits all interrupts, including the NMI interrupt, until after execution of the next instruction. This action allows sequential execution of POP SS and MOV ESP, EBP instructions without the danger of having an invalid stack during an interrupt¹. However, use of the LSS instruction is the preferred method of loading the SS and ESP registers.

-
1. If a code instruction breakpoint (for debug) is placed on an instruction located immediately after a POP SS instruction, the breakpoint may not be triggered. However, in a sequence of instructions that POP the SS register, only the first instruction in the sequence is guaranteed to delay an interrupt.

In the following sequence, interrupts may be recognized before POP ESP executes:

```
POP SS
POP SS
POP ESP
```

In 64-bit mode, using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). When in 64-bit mode, POPs using 32-bit operands are not encodable and POPs to DS, ES, SS are not valid. See the summary chart at the beginning of this section for encoding data and limits.

Operation

```

IF StackAddrSize = 32
  THEN
    IF OperandSize = 32
      THEN
        DEST ← SS:ESP; (* Copy a doubleword *)
        ESP ← ESP + 4;
      ELSE (* OperandSize = 16*)
        DEST ← SS:ESP; (* Copy a word *)
        ESP ← ESP + 2;
      FI;
    ELSE IF StackAddrSize = 64
      THEN
        IF OperandSize = 64
          THEN
            DEST ← SS:RSP; (* Copy quadword *)
            RSP ← RSP + 8;
          ELSE (* OperandSize = 16*)
            DEST ← SS:RSP; (* Copy a word *)
            RSP ← RSP + 2;
          FI;
        FI;
      ELSE StackAddrSize = 16
        THEN
          IF OperandSize = 16
            THEN
              DEST ← SS:SP; (* Copy a word *)
              SP ← SP + 2;
            ELSE (* OperandSize = 32 *)
              DEST ← SS:SP; (* Copy a doubleword *)
              SP ← SP + 4;
            FI;
          FI;
        FI;
    FI;
  
```

Loading a segment register while in protected mode results in special actions, as described in the following listing. These checks are performed on the segment selector and the segment descriptor it points to.

64-BIT_MODE

```

IF FS, or GS is loaded with non-NULL selector;
    THEN
        IF segment selector index is outside descriptor table limits
            OR segment is not a data or readable code segment
            OR ((segment is a data or nonconforming code segment)
                AND (both RPL and CPL > DPL))
                THEN #GP(selector);
            IF segment not marked present
                THEN #NP(selector);
        ELSE
            SegmentRegister ← segment selector;
            SegmentRegister ← segment descriptor;
        FI;
FI;
IF FS, or GS is loaded with a NULL selector;
    THEN
        SegmentRegister ← segment selector;
        SegmentRegister ← segment descriptor;
FI;

```

PROTECTED MODE OR COMPATIBILITY MODE;

```

IF SS is loaded;
    THEN
        IF segment selector is NULL
            THEN #GP(0);
        FI;
        IF segment selector index is outside descriptor table limits
            or segment selector's RPL ≠ CPL
            or segment is not a writable data segment
            or DPL ≠ CPL
                THEN #GP(selector);
        FI;
        IF segment not marked present
            THEN #SS(selector);
            ELSE
                SS ← segment selector;
                SS ← segment descriptor;
        FI;
FI;

```



```

IF DS, ES, FS, or GS is loaded with non-NULL selector;
  THEN
    IF segment selector index is outside descriptor table limits
      or segment is not a data or readable code segment
      or ((segment is a data or nonconforming code segment)
        and (both RPL and CPL > DPL))
      THEN #GP(selector);
  FI;
  IF segment not marked present
    THEN #NP(selector);
  ELSE
    SegmentRegister ← segment selector;
    SegmentRegister ← segment descriptor;
  FI;
FI;

```

```

IF DS, ES, FS, or GS is loaded with a NULL selector
  THEN
    SegmentRegister ← segment selector;
    SegmentRegister ← segment descriptor;
  FI;

```

Flags Affected

None.

Protected Mode Exceptions

| | |
|---------------|---|
| #GP(0) | <p>If attempt is made to load SS register with NULL segment selector.</p> <p>If the destination operand is in a non-writable segment.</p> <p>If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector.</p> |
| #GP(selector) | <p>If segment selector index is outside descriptor table limits.</p> <p>If the SS register is being loaded and the segment selector's RPL and the segment descriptor's DPL are not equal to the CPL.</p> <p>If the SS register is being loaded and the segment pointed to is a non-writable data segment.</p> <p>If the DS, ES, FS, or GS register is being loaded and the segment pointed to is not a data or readable code segment.</p> |

| | |
|-----------------|--|
| | If the DS, ES, FS, or GS register is being loaded and the segment pointed to is a data or nonconforming code segment, but both the RPL and the CPL are greater than the DPL. |
| #SS(0) | If the current top of stack is not within the stack segment. If a memory operand effective address is outside the SS segment limit. |
| #SS(selector) | If the SS register is being loaded and the segment pointed to is marked not present. |
| #NP | If the DS, ES, FS, or GS register is being loaded and the segment pointed to is marked not present. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while the current privilege level is 3 and alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|---------------|--|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(U) | If the stack address is in a non-canonical form. |
| #GP(selector) | If the descriptor is outside the descriptor table limit. If the FS or GS register is being loaded and the segment pointed to is not a data or readable code segment. If the FS or GS register is being loaded and the segment pointed to is a data or nonconforming code segment, but both the RPL and the CPL are greater than the DPL. |

| | |
|-----------------|--|
| #AC(0) | If an unaligned memory reference is made while alignment checking is enabled. |
| #PF(fault-code) | If a page fault occurs. |
| #NP | If the FS or GS register is being loaded and the segment pointed to is marked not present. |
| #UD | If the LOCK prefix is used. |

POPA/POPAD—Pop All General-Purpose Registers

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|--------|-------------|-------------|-----------------|--|
| 61 | POPA | Invalid | Valid | Pop DI, SI, BP, BX, DX, CX, and AX. |
| 61 | POPAD | Invalid | Valid | Pop EDI, ESI, EBP, EBX, EDX, ECX, and EAX. |

Description

Pops doublewords (POPAD) or words (POPA) from the stack into the general-purpose registers. The registers are loaded in the following order: EDI, ESI, EBP, EBX, EDX, ECX, and EAX (if the operand-size attribute is 32) and DI, SI, BP, BX, DX, CX, and AX (if the operand-size attribute is 16). (These instructions reverse the operation of the PUSHA/PUSHAD instructions.) The value on the stack for the ESP or SP register is ignored. Instead, the ESP or SP register is incremented after each register is loaded.

The POPA (pop all) and POPAD (pop all double) mnemonics reference the same opcode. The POPA instruction is intended for use when the operand-size attribute is 16 and the POPAD instruction for when the operand-size attribute is 32. Some assemblers may force the operand size to 16 when POPA is used and to 32 when POPAD is used (using the operand-size override prefix [66H] if necessary). Others may treat these mnemonics as synonyms (POPA/POPAD) and use the current setting of the operand-size attribute to determine the size of values to be popped from the stack, regardless of the mnemonic used. (The D flag in the current code segment's segment descriptor determines the operand-size attribute.)

This instruction executes as described in non-64-bit modes. It is not valid in 64-bit mode.

Operation

```
IF 64-Bit Mode
    THEN
        #UD;
ELSE
    IF OperandSize = 32 (* Instruction = POPAD *)
        THEN
            EDI ← Pop();
            ESI ← Pop();
            EBP ← Pop();
            Increment ESP by 4; (* Skip next 4 bytes of stack *)
            EBX ← Pop();
            EDX ← Pop();
            ECX ← Pop();
            EAX ← Pop();
```

```

ELSE (* OperandSize = 16, instruction = POPA *)
    DI ← Pop();
    SI ← Pop();
    BP ← Pop();
    Increment ESP by 2; (* Skip next 2 bytes of stack *)
    BX ← Pop();
    DX ← Pop();
    CX ← Pop();
    AX ← Pop();
FI;
FI;

```

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If the starting or ending stack address is not within the stack segment. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while the current privilege level is 3 and alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #SS | If the starting or ending stack address is not within the stack segment. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If the starting or ending stack address is not within the stack segment. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----|--------------------|
| #UD | If in 64-bit mode. |
|-----|--------------------|

POPCNT – Return the Count of Number of Bits Set to 1

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------------|--------------------------|-------------|-----------------|------------------------|
| F3 0F B8 /r | POPCNT <i>r16, r/m16</i> | Valid | Valid | POPCNT on <i>r/m16</i> |
| F3 0F B8 /r | POPCNT <i>r32, r/m32</i> | Valid | Valid | POPCNT on <i>r/m32</i> |
| F3 REX.W 0F B8 /r | POPCNT <i>r64, r/m64</i> | Valid | N.E. | POPCNT on <i>r/m64</i> |

Description

This instruction calculates of number of bits set to 1 in the second operand (source) and returns the count in the first operand (a destination register).

Operation

```
Count = 0;
For (i=0; i < OperandSize; i++)
{
    IF (SRC[ i] = 1) // i'th bit
        THEN Count++; FI;
}
DEST ← Count;
```

Flags Affected

OF, SF, ZF, AF, CF, PF are all cleared. ZF is set if SRC == 0, otherwise ZF is cleared

Intel C/C++ Compiler Intrinsic Equivalent

```
POPCNT int _mm_popcnt_u32(unsigned int a);
```

```
POPCNT int64_t _mm_popcnt_u64(unsigned __int64 a);
```

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS or GS segments. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | For a page fault. |
| #UD | If CPUID.01H: ECX.POPCNT [Bit 23] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|---|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CPUID.01H: ECX.POPCNT [Bit 23] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | For a page fault. |
| #UD | If CPUID.01H: ECX.POPCNT [Bit 23] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #UD | If CPUID.01H: ECX.POPCNT [Bit 23] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

POPF/POPFD/POPfq—Pop Stack into EFLAGS Register

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|------------|-------------|-------------|-----------------|--|
| 9D | POPF | Valid | Valid | Pop top of stack into lower 16 bits of EFLAGS. |
| 9D | POPFD | N.E. | Valid | Pop top of stack into EFLAGS. |
| REX.W + 9D | POPfq | Valid | N.E. | Pop top of stack and zero-extend into RFLAGS. |

Description

Pops a doubleword (POPFD) from the top of the stack (if the current operand-size attribute is 32) and stores the value in the EFLAGS register, or pops a word from the top of the stack (if the operand-size attribute is 16) and stores it in the lower 16 bits of the EFLAGS register (that is, the FLAGS register). These instructions reverse the operation of the PUSHF/PUSHFD instructions.

The POPF (pop flags) and POPFD (pop flags double) mnemonics reference the same opcode. The POPF instruction is intended for use when the operand-size attribute is 16; the POPFD instruction is intended for use when the operand-size attribute is 32. Some assemblers may force the operand size to 16 for POPF and to 32 for POPFD. Others may treat the mnemonics as synonyms (POPF/POPFD) and use the setting of the operand-size attribute to determine the size of values to pop from the stack.

The effect of POPF/POPFD on the EFLAGS register changes, depending on the mode of operation. When the processor is operating in protected mode at privilege level 0 (or in real-address mode, the equivalent to privilege level 0), all non-reserved flags in the EFLAGS register except RF¹, VIP, VIF, and VM may be modified. VIP, VIF and VM remain unaffected.

When operating in protected mode with a privilege level greater than 0, but less than or equal to IOPL, all flags can be modified except the IOPL field and VIP, VIF, and VM. Here, the IOPL flags are unaffected, the VIP and VIF flags are cleared, and the VM flag is unaffected. The interrupt flag (IF) is altered only when executing at a level at least as privileged as the IOPL. If a POPF/POPFD instruction is executed with insufficient privilege, an exception does not occur but privileged bits do not change.

When operating in virtual-8086 mode, the IOPL must be equal to 3 to use POPF/POPFD instructions; VM, RF, IOPL, VIP, and VIF are unaffected. If the IOPL is less than 3, POPF/POPFD causes a general-protection exception (#GP).

In 64-bit mode, use REX.W to pop the top of stack to RFLAGS. The mnemonic assigned is POPfq (note that the 32-bit operand is not encodable). POPfq pops 64

1. RF is always zero after the execution of POPF. This is because POPF, like all instructions, clears RF as it begins to execute.

bits from the stack, loads the lower 32 bits into RFLAGS, and zero extends the upper bits of RFLAGS.

See Chapter 3 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for more information about the EFLAGS registers.

Operation

```

IF VM = 0 (* Not in Virtual-8086 Mode *)
  THEN IF CPL = 0
    THEN
      IF OperandSize = 32;
        THEN
          EFLAGS ← Pop(); (* 32-bit pop *)
          (* All non-reserved flags except RF, VIP, VIF, and VM can be modified;
            VIP and VIF are cleared; RF, VM, and all reserved bits are unaffected. *)
        ELSE IF (OperandSize = 64)
          RFLAGS = Pop(); (* 64-bit pop *)
          (* All non-reserved flags except RF, VIP, VIF, and VM can be modified; VIP
            and VIF are cleared; RF, VM, and all reserved bits are unaffected. *)
        ELSE (* OperandSize = 16 *)
          EFLAGS[15:0] ← Pop(); (* 16-bit pop *)
          (* All non-reserved flags can be modified. *)
        FI;
      ELSE (* CPL > 0 *)
        IF OperandSize = 32
          THEN
            IF CPL > IOPL
              THEN
                EFLAGS ← Pop(); (* 32-bit pop *)
                (* All non-reserved bits except IF, IOPL, RF, VIP, and
                  VIF can be modified; IF, IOPL, RF, VM, and all reserved
                  bits are unaffected; VIP and VIF are cleared. *)
              ELSE
                EFLAGS ← Pop(); (* 32-bit pop *)
                (* All non-reserved bits except IOPL, RF, VIP, and VIF can be
                  modified; IOPL, RF, VM, and all reserved bits are
                  unaffected; VIP and VIF are cleared. *)
              FI;
            ELSE IF (OperandSize = 64)
              IF CPL > IOPL
                THEN
                  RFLAGS ← Pop(); (* 64-bit pop *)
                  (* All non-reserved bits except IF, IOPL, RF, VIP, and
                    *)

```

```

        VIF can be modified; IF, IOPL, RF, VM, and all reserved
        bits are unaffected; VIP and VIF are cleared. *)
    ELSE
        RFLAGS ← Pop(); (* 64-bit pop *)
        (* All non-reserved bits except IOPL, RF, VIP, and VIF can be
        modified; IOPL, RF, VM, and all reserved bits are
        unaffected; VIP and VIF are cleared. *)
    FI;
ELSE (* OperandSize = 16 *)
    EFLAGS[15:0] ← Pop(); (* 16-bit pop *)
    (* All non-reserved bits except IOPL can be modified; IOPL and all
    reserved bits are unaffected. *)
    FI;
ELSE (* In Virtual-8086 Mode *)
    IF IOPL = 3
        THEN IF OperandSize = 32
            THEN
                EFLAGS ← Pop();
                (* All non-reserved bits except VM, RF, IOPL, VIP, and VIF can be
                modified; VM, RF, IOPL, VIP, VIF, and all reserved bits are unaffected. *)
            ELSE
                EFLAGS[15:0] ← Pop(); FI;
                (* All non-reserved bits except IOPL can be modified;
                IOPL and all reserved bits are unaffected. *)
        ELSE (* IOPL < 3 *)
            #GP(0); (* Trap to virtual-8086 monitor. *)
        FI;
    FI;
FI;

```

Flags Affected

All flags may be affected; see the Operation section for details.

Protected Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If the top of stack is not within the stack segment. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while the current privilege level is 3 and alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #SS | If the top of stack is not within the stack segment. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the I/O privilege level is less than 3. If an attempt is made to execute the POPF/POPFQ instruction with an operand-size override prefix. |
| #SS(0) | If the top of stack is not within the stack segment. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If the stack address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

POR—Bitwise Logical OR

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---------------------------------------|-------------|------------------|--|
| 0F EB /r | POR <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Bitwise OR of <i>mm/m64</i> and <i>mm</i> . |
| 66 0F EB /r | POR <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Bitwise OR of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical OR operation on the source operand (second operand) and the destination operand (first operand) and stores the result in the destination operand. The source operand can be an MMX technology register or a 64-bit memory location or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. Each bit of the result is set to 1 if either or both of the corresponding bits of the first and second operands are 1; otherwise, it is set to 0.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST ← DEST OR SRC;

Intel C/C++ Compiler Intrinsic Equivalent

POR __m64 __mm_or_si64(__m64 m1, __m64 m2)

POR __m128i __mm_or_si128(__m128i m1, __m128i m2)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

- #GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) If a memory operand effective address is outside the SS segment limit.

| | |
|-----------------|---|
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. 128-bit operations will generate #UD only if CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PREFETCH h —Prefetch Data Into Caches

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|------------------|-------------|------------------|---|
| OF 18 /1 | PREFETCHT0 $m8$ | Valid | Valid | Move data from $m8$ closer to the processor using T0 hint. |
| OF 18 /2 | PREFETCHT1 $m8$ | Valid | Valid | Move data from $m8$ closer to the processor using T1 hint. |
| OF 18 /3 | PREFETCHT2 $m8$ | Valid | Valid | Move data from $m8$ closer to the processor using T2 hint. |
| OF 18 /0 | PREFETCHNTA $m8$ | Valid | Valid | Move data from $m8$ closer to the processor using NTA hint. |

Description

Fetches the line of data from memory that contains the byte specified with the source operand to a location in the cache hierarchy specified by a locality hint:

- T0 (temporal data)—prefetch data into all levels of the cache hierarchy.
 - Pentium III processor—1st- or 2nd-level cache.
 - Pentium 4 and Intel Xeon processors—2nd-level cache.
- T1 (temporal data with respect to first level cache)—prefetch data into level 2 cache and higher.
 - Pentium III processor—2nd-level cache.
 - Pentium 4 and Intel Xeon processors—2nd-level cache.
- T2 (temporal data with respect to second level cache)—prefetch data into level 2 cache and higher.
 - Pentium III processor—2nd-level cache.
 - Pentium 4 and Intel Xeon processors—2nd-level cache.
- NTA (non-temporal data with respect to all cache levels)—prefetch data into non-temporal cache structure and into a location close to the processor, minimizing cache pollution.
 - Pentium III processor—1st-level cache
 - Pentium 4 and Intel Xeon processors—2nd-level cache

The source operand is a byte memory location. (The locality hints are encoded into the machine level instruction using bits 3 through 5 of the ModR/M byte. Use of any ModR/M value other than the specified ones will lead to unpredictable behavior.)

If the line selected is already present in the cache hierarchy at a level closer to the processor, no data movement occurs. Prefetches from uncacheable or WC memory are ignored.

The `PREFETCHh` instruction is merely a hint and does not affect program behavior. If executed, this instruction moves data closer to the processor in anticipation of future use.

The implementation of prefetch locality hints is implementation-dependent, and can be overloaded or ignored by a processor implementation. The amount of data prefetched is also processor implementation-dependent. It will, however, be a minimum of 32 bytes.

It should be noted that processors are free to speculatively fetch and cache data from system memory regions that are assigned a memory-type that permits speculative reads (that is, the WB, WC, and WT memory types). A `PREFETCHh` instruction is considered a hint to this speculative behavior. Because this speculative fetching can occur at any time and is not tied to instruction execution, a `PREFETCHh` instruction is not ordered with respect to the fence instructions (MFENCE, SFENCE, and LFENCE) or locked memory references. A `PREFETCHh` instruction is also unordered with respect to CLFLUSH instructions, other `PREFETCHh` instructions, or any other general instruction. It is ordered with respect to serializing instructions such as CPUID, WRMSR, OUT, and MOV CR.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

FETCH (m8);

Intel C/C++ Compiler Intrinsic Equivalent

```
void _mm_prefetch(char *p, int i)
```

The argument “*p” gives the address of the byte (and corresponding cache line) to be prefetched. The value “i” gives a constant (`_MM_HINT_T0`, `_MM_HINT_T1`, `_MM_HINT_T2`, or `_MM_HINT_NTA`) that specifies the type of prefetch operation to be performed.

Numeric Exceptions

None.

Exceptions (All Operating Modes)

#UD If the LOCK prefix is used.

PSADBW—Compute Sum of Absolute Differences

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F F6 /r | PSADBW <i>mm1</i> , <i>mm2/m64</i> | Valid | Valid | Computes the absolute differences of the packed unsigned byte integers from <i>mm2/m64</i> and <i>mm1</i> ; differences are then summed to produce an unsigned word integer result. |
| 66 0F F6 /r | PSADBW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Computes the absolute differences of the packed unsigned byte integers from <i>xmm2/m128</i> and <i>xmm1</i> ; the 8 low differences and 8 high differences are then summed separately to produce two unsigned word integer results. |

Description

Computes the absolute value of the difference of 8 unsigned byte integers from the source operand (second operand) and from the destination operand (first operand). These 8 differences are then summed to produce an unsigned word integer result that is stored in the destination operand. The source operand can be an MMX technology register or a 64-bit memory location or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. Figure 4-5 shows the operation of the PSADBW instruction when using 64-bit operands.

When operating on 64-bit operands, the word integer result is stored in the low word of the destination operand, and the remaining bytes in the destination operand are cleared to all 0s.

When operating on 128-bit operands, two packed results are computed. Here, the 8 low-order bytes of the source and destination operands are operated on to produce a word result that is stored in the low word of the destination operand, and the 8 high-order bytes are operated on to produce a word result that is stored in bits 64 through 79 of the destination operand. The remaining bytes of the destination operand are cleared.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

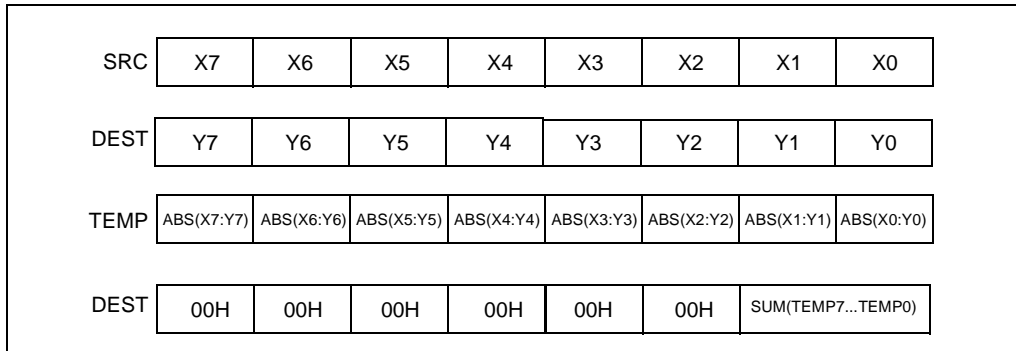


Figure 4-5. PSADBW Instruction Operation Using 64-bit Operands

Operation

PSADBW instructions when using 64-bit operands:

```

TEMP0 ← ABS(DEST[7:0] – SRC[7:0]);
(* Repeat operation for bytes 2 through 6 *)
TEMP7 ← ABS(DEST[63:56] – SRC[63:56]);
DEST[15:0] ← SUM(TEMP0:TEMP7);
DEST[63:16] ← 000000000000H;

```

PSADBW instructions when using 128-bit operands:

```

TEMP0 ← ABS(DEST[7:0] – SRC[7:0]);
(* Repeat operation for bytes 2 through 14 *)
TEMP15 ← ABS(DEST[127:120] – SRC[127:120]);
DEST[15:0] ← SUM(TEMP0:TEMP7);
DEST[63:16] ← 000000000000H;
DEST[79:64] ← SUM(TEMP8:TEMP15);
DEST[127:80] ← 000000000000H;

```

Intel C/C++ Compiler Intrinsic Equivalent

PSADBW `__m64 __mm_sad_pu8(__m64 a, __m64 b)`

PSADBW `__m128i __mm_sad_epu8(__m128i a, __m128i b)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSHUFB — Packed Shuffle Bytes

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|------------------------|-------------|------------------|---|
| 0F 38 00 /r | PSHUFB mm1, mm2/m64 | Valid | Valid | Shuffle bytes in mm1 according to contents of mm2/m64. |
| 66 0F 38 00 /r | PSHUFB xmm1, xmm2/m128 | Valid | Valid | Shuffle bytes in xmm1 according to contents of xmm2/m128. |

Description

PSHUFB performs in-place shuffles of bytes in the destination operand (the first operand) according to the shuffle control mask in the source operand (the second operand). The instruction permutes the data in the destination operand, leaving the shuffle mask unaffected. If the most significant bit (bit[7]) of each byte of the shuffle control mask is set, then constant zero is written in the result byte. Each byte in the shuffle control mask forms an index to permute the corresponding byte in the destination operand. The value of each index is the least significant 4 bits (128-bit operation) or 3 bits (64-bit operation) of the shuffle control byte. Both operands can be MMX register or XMM registers. When the source operand is a 128-bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PSHUFB with 64 bit operands:

```

for i = 0 to 7 {
  if (SRC[(i * 8)+7] == 1 ) then
    DEST[(i*8)+7...(i*8)+0] ← 0;
  else
    index[2..0] ← SRC[(i*8)+2 .. (i*8)+0];
    DEST[(i*8)+7...(i*8)+0] ← DEST[(index*8+7)..(index*8+0)];
  endif;
}

```

PSHUFB with 128 bit operands:

```

for i = 0 to 15 {
  if (SRC[(i * 8)+7] == 1 ) then
    DEST[(i*8)+7...(i*8)+0] ← 0;
  endif;
}

```

```

else
  index[3..0] ← SRC[(i*8)+3 .. (i*8)+0];
  DEST[(i*8)+7 .. (i*8)+0] ← DEST[(index*8+7)..(index*8+0)];
endif
}

```

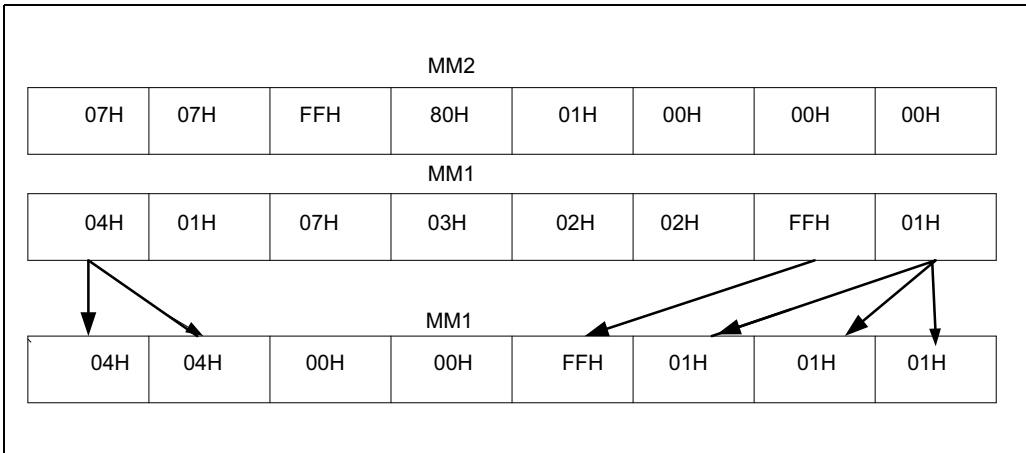


Figure 4-6. PSHUB with 64-Bit Operands

Intel C/C++ Compiler Intrinsic Equivalent

PSHUF8 __m64 _mm_shuffle_pi8 (__m64 a, __m64 b)

PSHUF8 __m128i _mm_shuffle_epi8 (__m128i a, __m128i b)

Protected Mode Exceptions

- #GP(0) If a memory operand effective address is outside the CS, DS, ES, FS or GS segments.
(128-bit operations only) If not aligned on 16-byte boundary, regardless of segment.
- #SS(0) If a memory operand effective address is outside the SS segment limit.
- #PF(fault-code) If a page fault occurs.
- #UD If CR0.EM = 1.
(128-bit operations only) If CR4.OSFXSR(bit 9) = 0.
If CPUID.SSSE3(ECX bit 9) = 0.
If the LOCK prefix is used.
- #NM If TS bit in CR0 is set.

| | |
|--------|--|
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | If any part of the operand lies outside of the effective address space from 0 to 0FFFFH. (128-bit operations only) If not aligned on 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM = 1. (128-bit operations only) If CR4.OSFXSR(bit 9) = 0. If CPUID.SSSE3(ECX bit 9) = 0. If the LOCK prefix is used. |
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |

INSTRUCTION SET REFERENCE, N-Z

#AC(0)

(64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PSHUFD—Shuffle Packed Doublewords

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|--|-------------|------------------|--|
| 66 0F 70 /r ib | PSHUFD <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Shuffle the doublewords in <i>xmm2/m128</i> based on the encoding in <i>imm8</i> and store the result in <i>xmm1</i> . |

Description

Copies doublewords from source operand (second operand) and inserts them in the destination operand (first operand) at the locations selected with the order operand (third operand). Figure 4-7 shows the operation of the PSHUFD instruction and the encoding of the order operand. Each 2-bit field in the order operand selects the contents of one doubleword location in the destination operand. For example, bits 0 and 1 of the order operand select the contents of doubleword 0 of the destination operand. The encoding of bits 0 and 1 of the order operand (see the field encoding in Figure 4-7) determines which doubleword from the source operand will be copied to doubleword 0 of the destination operand.

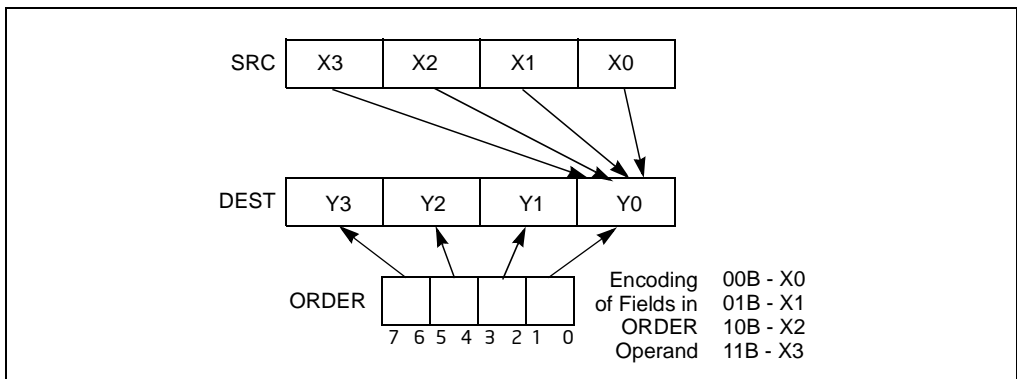


Figure 4-7. PSHUFD Instruction Operation

The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. The order operand is an 8-bit immediate. Note that this instruction permits a doubleword in the source operand to be copied to more than one doubleword location in the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

$DEST[31:0] \leftarrow (SRC \gg (ORDER[1:0] * 32))[31:0];$
 $DEST[63:32] \leftarrow (SRC \gg (ORDER[3:2] * 32))[31:0];$
 $DEST[95:64] \leftarrow (SRC \gg (ORDER[5:4] * 32))[31:0];$
 $DEST[127:96] \leftarrow (SRC \gg (ORDER[7:6] * 32))[31:0];$

Intel C/C++ Compiler Intrinsic Equivalent

PSHUFD `__m128i_mm_shuffle_epi32(__m128i a, int n)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | <p>If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If a memory operand is not aligned on a 16-byte boundary, regardless of segment.</p> |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #NM | If CR0.TS[bit 3] = 1. |
| #PF(fault-code) | If a page fault occurs. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | <p>If a memory operand is not aligned on a 16-byte boundary, regardless of segment.</p> <p>If any part of the operand lies outside of the effective address space from 0 to FFFFH.</p> |
| #UD | <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #NM | If CR0.TS[bit 3] = 1. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.

If CR4.OSFXSR[bit 9] = 0.

If CPUID.01H:EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#PF(fault-code) If a page fault occurs.

PSHUFHW—Shuffle Packed High Words

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------------|--|-------------|-----------------|---|
| F3 0F 70 /r ib | PSHUFHW <i>xmm1</i> , <i>xmm2</i> / <i>m128</i> , <i>imm8</i> | Valid | Valid | Shuffle the high words in <i>xmm2/m128</i> based on the encoding in <i>imm8</i> and store the result in <i>xmm1</i> . |

Description

Copies words from the high quadword of the source operand (second operand) and inserts them in the high quadword of the destination operand (first operand) at word locations selected with the order operand (third operand). This operation is similar to the operation used by the PSHUFD instruction, which is illustrated in Figure 4-7. For the PSHUFHW instruction, each 2-bit field in the order operand selects the contents of one word location in the high quadword of the destination operand. The binary encodings of the order operand fields select words (0, 1, 2 or 3, 4) from the high quadword of the source operand to be copied to the destination operand. The low quadword of the source operand is copied to the low quadword of the destination operand.

The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. The order operand is an 8-bit immediate. Note that this instruction permits a word in the high quadword of the source operand to be copied to more than one word location in the high quadword of the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[63:0] ← SRC[63:0];
DEST[79:64] ← (SRC >> (ORDER[1:0] * 16))[79:64];
DEST[95:80] ← (SRC >> (ORDER[3:2] * 16))[79:64];
DEST[111:96] ← (SRC >> (ORDER[5:4] * 16))[79:64];
DEST[127:112] ← (SRC >> (ORDER[7:6] * 16))[79:64];
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PSHUFHW    __m128i _mm_shufflehi_epi16(__m128i a, int n)
```

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #PF(fault-code) | If a page fault occurs. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|------------------|--|
| | If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #PF (fault-code) | If a page fault occurs. |

PSHUFLW—Shuffle Packed Low Words

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|---|-------------|------------------|--|
| F2 0F 70 /r ib | PSHUFLW <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Shuffle the low words in <i>xmm2/m128</i> based on the encoding in <i>imm8</i> and store the result in <i>xmm1</i> . |

Description

Copies words from the low quadword of the source operand (second operand) and inserts them in the low quadword of the destination operand (first operand) at word locations selected with the order operand (third operand). This operation is similar to the operation used by the PSHUFD instruction, which is illustrated in Figure 4-7. For the PSHUFLW instruction, each 2-bit field in the order operand selects the contents of one word location in the low quadword of the destination operand. The binary encodings of the order operand fields select words (0, 1, 2, or 3) from the low quadword of the source operand to be copied to the destination operand. The high quadword of the source operand is copied to the high quadword of the destination operand.

The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. The order operand is an 8-bit immediate. Note that this instruction permits a word in the low quadword of the source operand to be copied to more than one word location in the low quadword of the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[15:0] ← (SRC >> (ORDER[1:0] * 16))[15:0];
DEST[31:16] ← (SRC >> (ORDER[3:2] * 16))[15:0];
DEST[47:32] ← (SRC >> (ORDER[5:4] * 16))[15:0];
DEST[63:48] ← (SRC >> (ORDER[7:6] * 16))[15:0];
DEST[127:64] ← SRC[127:64];
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PSHUFLW      __m128i _mm_shufflelo_epi16(__m128i a, int n)
```

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #PF(fault-code) | If a page fault occurs. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |

| | |
|------------------|--|
| | If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #PF (fault-code) | If a page fault occurs. |

PSHUFW—Shuffle Packed Words

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|---|
| 0F 70 /r ib | PSHUFW <i>mm1</i> , <i>mm2/m64</i> , <i>imm8</i> | Valid | Valid | Shuffle the words in <i>mm2/m64</i> based on the encoding in <i>imm8</i> and store the result in <i>mm1</i> . |

Description

Copies words from the source operand (second operand) and inserts them in the destination operand (first operand) at word locations selected with the order operand (third operand). This operation is similar to the operation used by the PSHUFD instruction, which is illustrated in Figure 4-7. For the PSHUFW instruction, each 2-bit field in the order operand selects the contents of one word location in the destination operand. The encodings of the order operand fields select words from the source operand to be copied to the destination operand.

The source operand can be an MMX technology register or a 64-bit memory location. The destination operand is an MMX technology register. The order operand is an 8-bit immediate. Note that this instruction permits a word in the source operand to be copied to more than one word location in the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

$$\begin{aligned} \text{DEST}[15:0] &\leftarrow (\text{SRC} \gg (\text{ORDER}[1:0] * 16))[15:0]; \\ \text{DEST}[31:16] &\leftarrow (\text{SRC} \gg (\text{ORDER}[3:2] * 16))[15:0]; \\ \text{DEST}[47:32] &\leftarrow (\text{SRC} \gg (\text{ORDER}[5:4] * 16))[15:0]; \\ \text{DEST}[63:48] &\leftarrow (\text{SRC} \gg (\text{ORDER}[7:6] * 16))[15:0]; \end{aligned}$$

Intel C/C++ Compiler Intrinsic Equivalent

PSHUFW `__m64 _mm_shuffle_pi16(__m64 a, int n)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #UD | If CR0.EM[bit 2] = 1. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSIGNB/PSIGNW/PSIGND — Packed SIGN

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|------------------------|-------------|------------------|---|
| 0F 38 08 /r | PSIGNB mm1, mm2/m64 | Valid | Valid | Negate/zero/preserve packed byte integers in mm1 depending on the corresponding sign in mm2/m64 |
| 66 0F 38 08 /r | PSIGNB xmm1, xmm2/m128 | Valid | Valid | Negate/zero/preserve packed byte integers in xmm1 depending on the corresponding sign in xmm2/m128. |
| 0F 38 09 /r | PSIGNW mm1, mm2/m64 | Valid | Valid | Negate/zero/preserve packed word integers in mm1 depending on the corresponding sign in mm2/m128. |
| 66 0F 38 09 /r | PSIGNW xmm1, xmm2/m128 | Valid | Valid | Negate/zero/preserve packed word integers in xmm1 depending on the corresponding sign in xmm2/m128. |
| 0F 38 0A /r | PSIGND mm1, mm2/m64 | Valid | Valid | Negate/zero/preserve packed doubleword integers in mm1 depending on the corresponding sign in mm2/m128. |
| 66 0F 38 0A /r | PSIGND xmm1, xmm2/m128 | Valid | Valid | Negate/zero/preserve packed doubleword integers in xmm1 depending on the corresponding sign in xmm2/m128. |

Description

PSIGNB/PSIGNW/PSIGND negates each data element of the destination operand (the first operand) if the signed integer value of the corresponding data element in the source operand (the second operand) is less than zero. If the signed integer value of a data element in the source operand is positive, the corresponding data element in the destination operand is unchanged. If a data element in the source operand is zero, the corresponding data element in the destination operand is set to zero.

PSIGNB operates on signed bytes. PSIGNW operates on 16-bit signed words. PSIGND operates on signed 32-bit integers. Both operands can be MMX register or XMM registers. When the source operand is a 128bit memory operand, the operand must be aligned on a 16-byte boundary or a general-protection exception (#GP) will be generated.

In 64-bit mode, use the REX prefix to access additional registers.

Operation

PSIGNB with 64 bit operands:

```

IF (SRC[7:0] < 0 )
    DEST[7:0] ← Neg(DEST[7:0])
ELSEIF (SRC[7:0] == 0 )
    DEST[7:0] ← 0
ELSEIF (SRC[7:0] > 0 )
    DEST[7:0] ← DEST[7:0]
Repeat operation for 2nd through 7th bytes

```

```

IF (SRC[63:56] < 0 )
    DEST[63:56] ← Neg(DEST[63:56])
ELSEIF (SRC[63:56] == 0 )
    DEST[63:56] ← 0
ELSEIF (SRC[63:56] > 0 )
    DEST[63:56] ← DEST[63:56]

```

PSIGNB with 128 bit operands:

```

IF (SRC[7:0] < 0 )
    DEST[7:0] ← Neg(DEST[7:0])
ELSEIF (SRC[7:0] == 0 )
    DEST[7:0] ← 0
ELSEIF (SRC[7:0] > 0 )
    DEST[7:0] ← DEST[7:0]
Repeat operation for 2nd through 15th bytes
IF (SRC[127:120] < 0 )
    DEST[127:120] ← Neg(DEST[127:120])
ELSEIF (SRC[127:120] == 0 )
    DEST[127:120] ← 0
ELSEIF (SRC[127:120] > 0 )
    DEST[127:120] ← DEST[127:120]

```

PSIGNW with 64 bit operands:

```

IF (SRC[15:0] < 0 )
    DEST[15:0] ← Neg(DEST[15:0])
ELSEIF (SRC[15:0] == 0 )
    DEST[15:0] ← 0
ELSEIF (SRC[15:0] > 0 )
    DEST[15:0] ← DEST[15:0]
Repeat operation for 2nd through 3rd words
IF (SRC[63:48] < 0 )
    DEST[63:48] ← Neg(DEST[63:48])
ELSEIF (SRC[63:48] == 0 )
    DEST[63:48] ← 0
ELSEIF (SRC[63:48] > 0 )

```

DEST[63:48] ← DEST[63:48]

PSIGNW with 128 bit operands:

```

IF (SRC[15:0] < 0 )
    DEST[15:0] ← Neg(DEST[15:0])
ELSEIF (SRC[15:0] == 0 )
    DEST[15:0] ← 0
ELSEIF (SRC[15:0] > 0 )
    DEST[15:0] ← DEST[15:0]
Repeat operation for 2nd through 7th words
IF (SRC[127:112] < 0 )
    DEST[127:112] ← Neg(DEST[127:112])
ELSEIF (SRC[127:112] == 0 )
    DEST[127:112] ← 0
ELSEIF (SRC[127:112] > 0 )
    DEST[127:112] ← DEST[127:112]

```

PSIGND with 64 bit operands:

```

IF (SRC[31:0] < 0 )
    DEST[31:0] ← Neg(DEST[31:0])
ELSEIF (SRC[31:0] == 0 )
    DEST[31:0] ← 0
ELSEIF (SRC[31:0] > 0 )
    DEST[31:0] ← DEST[31:0]
IF (SRC[63:32] < 0 )
    DEST[63:32] ← Neg(DEST[63:32])
ELSEIF (SRC[63:32] == 0 )
    DEST[63:32] ← 0
ELSEIF (SRC[63:32] > 0 )
    DEST[63:32] ← DEST[63:32]

```

PSIGND with 128 bit operands:

```

IF (SRC[31:0] < 0 )
    DEST[31:0] ← Neg(DEST[31:0])
ELSEIF (SRC[31:0] == 0 )
    DEST[31:0] ← 0
ELSEIF (SRC[31:0] > 0 )
    DEST[31:0] ← DEST[31:0]
Repeat operation for 2nd through 3rd double words
IF (SRC[127:96] < 0 )
    DEST[127:96] ← Neg(DEST[127:96])
ELSEIF (SRC[127:96] == 0 )

```

```

DEST[127:96] ← 0
ELSEIF (SRC[127:96] > 0)
    DEST[127:96] ← DEST[127:96]

```

Intel C/C++ Compiler Intrinsic Equivalent

```

PSIGNB    __m64 _mm_sign_pi8 (__m64 a, __m64 b)
PSIGNB    __m128i _mm_sign_epi8 (__m128i a, __m128i b)
PSIGNW    __m64 _mm_sign_pi16 (__m64 a, __m64 b)
PSIGNW    __m128i _mm_sign_epi16 (__m128i a, __m128i b)
PSIGND    __m64 _mm_sign_pi32 (__m64 a, __m64 b)
PSIGND    __m128i _mm_sign_epi32 (__m128i a, __m128i b)

```

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS or GS segments.
(128-bit operations only) If not aligned on 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF(fault-code) If a page fault occurs.

#UD If CR0.EM = 1.
(128-bit operations only) If CR4.OSFXSR(bit 9) = 0.
If CPUID.SSSE3(ECX bit 9) = 0.
If the LOCK prefix is used.

#NM If TS bit in CR0 is set.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#AC(0) (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made while the current privilege level is 3.

Real Mode Exceptions

#GP(0) If any part of the operand lies outside of the effective address space from 0 to 0FFFFH.
(128-bit operations only) If not aligned on 16-byte boundary, regardless of segment.

#UD (128-bit operations only) If CR0.EM = 1.
If CR4.OSFXSR(bit 9) = 0.
If CPUID.SSSE3(ECX bit 9) = 0.
If the LOCK prefix is used.

| | |
|-----|---|
| #NM | If TS bit in CR0 is set. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|------------------|---|
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSSE3[bit 9] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSLLDQ—Shift Double Quadword Left Logical

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|-------------------------------------|-------------|------------------|---|
| 66 0F 73 /7 ib | PSLLDQ <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift <i>xmm1</i> left by <i>imm8</i> bytes while shifting in 0s. |

Description

Shifts the destination operand (first operand) to the left by the number of bytes specified in the count operand (second operand). The empty low-order bytes are cleared (set to all 0s). If the value specified by the count operand is greater than 15, the destination operand is set to all 0s. The destination operand is an XMM register. The count operand is an 8-bit immediate.

Operation

```
TEMP ← COUNT;
IF (TEMP > 15) THEN TEMP ← 16; FI;
DEST ← DEST << (TEMP * 8);
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PSLLDQ  __m128i _mm_slli_si128 (__m128i a, int imm)
```

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

```
#UD          If CR0.EM[bit 2] = 1.
              If CR4.OSFXSR[bit 9] = 0.
              If CPUID.01H:EDX.SSE2[bit 26] = 0.
              If the LOCK prefix is used.
#NM          If CR0.TS[bit 3] = 1.
```

Real-Address Mode Exceptions

Same exceptions as in protected mode.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

PSLLW/PSLLD/PSLLQ—Shift Packed Data Left Logical

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|------------------------------|-------------|------------------|---|
| 0F F1 /r | PSLLW <i>mm, mm/m64</i> | Valid | Valid | Shift words in <i>mm</i> left <i>mm/m64</i> while shifting in 0s. |
| 66 0F F1 /r | PSLLW <i>xmm1, xmm2/m128</i> | Valid | Valid | Shift words in <i>xmm1</i> left by <i>xmm2/m128</i> while shifting in 0s. |
| 0F 71 /6 ib | PSLLW <i>xmm1, imm8</i> | Valid | Valid | Shift words in <i>mm</i> left by <i>imm8</i> while shifting in 0s. |
| 66 0F 71 /6 ib | PSLLW <i>xmm1, imm8</i> | Valid | Valid | Shift words in <i>xmm1</i> left by <i>imm8</i> while shifting in 0s. |
| 0F F2 /r | PSLLD <i>mm, mm/m64</i> | Valid | Valid | Shift doublewords in <i>mm</i> left by <i>mm/m64</i> while shifting in 0s. |
| 66 0F F2 /r | PSLLD <i>xmm1, xmm2/m128</i> | Valid | Valid | Shift doublewords in <i>xmm1</i> left by <i>xmm2/m128</i> while shifting in 0s. |
| 0F 72 /6 ib | PSLLD <i>mm, imm8</i> | Valid | Valid | Shift doublewords in <i>mm</i> left by <i>imm8</i> while shifting in 0s. |
| 66 0F 72 /6 ib | PSLLD <i>xmm1, imm8</i> | Valid | Valid | Shift doublewords in <i>xmm1</i> left by <i>imm8</i> while shifting in 0s. |
| 0F F3 /r | PSLLQ <i>mm, mm/m64</i> | Valid | Valid | Shift quadword in <i>mm</i> left by <i>mm/m64</i> while shifting in 0s. |
| 66 0F F3 /r | PSLLQ <i>xmm1, xmm2/m128</i> | Valid | Valid | Shift quadwords in <i>xmm1</i> left by <i>xmm2/m128</i> while shifting in 0s. |
| 0F 73 /6 ib | PSLLQ <i>mm, imm8</i> | Valid | Valid | Shift quadword in <i>mm</i> left by <i>imm8</i> while shifting in 0s. |
| 66 0F 73 /6 ib | PSLLQ <i>xmm1, imm8</i> | Valid | Valid | Shift quadwords in <i>xmm1</i> left by <i>imm8</i> while shifting in 0s. |

Description

Shifts the bits in the individual data elements (words, doublewords, or quadword) in the destination operand (first operand) to the left by the number of bits specified in the count operand (second operand). As the bits in the data elements are shifted left, the empty low-order bits are cleared (set to 0). If the value specified by the count operand is greater than 15 (for words), 31 (for doublewords), or 63 (for a quadword), then the destination operand is set to all 0s. Figure 4-8 gives an example of shifting words in a 64-bit operand.

The destination operand may be an MMX technology register or an XMM register; the count operand can be either an MMX technology register or an 64-bit memory loca-

tion, an XMM register or a 128-bit memory location, or an 8-bit immediate. Note that only the first 64-bits of a 128-bit count operand are checked to compute the count.

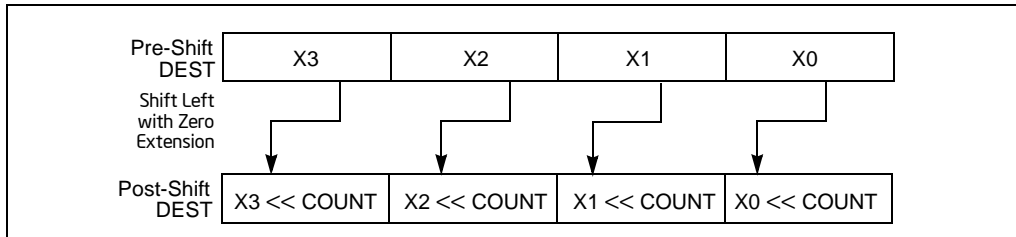


Figure 4-8. PSLW, PSLD, and PSLQ Instruction Operation Using 64-bit Operand

The PSLW instruction shifts each of the words in the destination operand to the left by the number of bits specified in the count operand; the PSLD instruction shifts each of the doublewords in the destination operand; and the PSLQ instruction shifts the quadword (or quadwords) in the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSLW instruction with 64-bit operand:

```
IF (COUNT > 15)
  THEN
    DEST[64:0] ← 0000000000000000H;
  ELSE
    DEST[15:0] ← ZeroExtend(DEST[15:0] << COUNT);
    (* Repeat shift operation for 2nd and 3rd words *)
    DEST[63:48] ← ZeroExtend(DEST[63:48] << COUNT);
  FI;
```

PSLD instruction with 64-bit operand:

```
IF (COUNT > 31)
  THEN
    DEST[64:0] ← 0000000000000000H;
  ELSE
    DEST[31:0] ← ZeroExtend(DEST[31:0] << COUNT);
    DEST[63:32] ← ZeroExtend(DEST[63:32] << COUNT);
  FI;
```

PSLQ instruction with 64-bit operand:

```
IF (COUNT > 63)
  THEN
```

```

    DEST[64:0] ← 0000000000000000H;
ELSE
    DEST ← ZeroExtend(DEST << COUNT);
FI;

```

PSLLW instruction with 128-bit operand:

```

COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 15)
THEN
    DEST[128:0] ← 00000000000000000000000000000000H;
ELSE
    DEST[15:0] ← ZeroExtend(DEST[15:0] << COUNT);
    (* Repeat shift operation for 2nd through 7th words *)
    DEST[127:112] ← ZeroExtend(DEST[127:112] << COUNT);
FI;

```

PSLLD instruction with 128-bit operand:

```

COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 31)
THEN
    DEST[128:0] ← 00000000000000000000000000000000H;
ELSE
    DEST[31:0] ← ZeroExtend(DEST[31:0] << COUNT);
    (* Repeat shift operation for 2nd and 3rd doublewords *)
    DEST[127:96] ← ZeroExtend(DEST[127:96] << COUNT);
FI;

```

PSLLQ instruction with 128-bit operand:

```

COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 63)
THEN
    DEST[128:0] ← 00000000000000000000000000000000H;
ELSE
    DEST[63:0] ← ZeroExtend(DEST[63:0] << COUNT);
    DEST[127:64] ← ZeroExtend(DEST[127:64] << COUNT);
FI;

```

Intel C/C++ Compiler Intrinsic Equivalents

```

PSLLW    __m64 _mm_slli_pi16 (__m64 m, int count)
PSLLW    __m64 _mm_sll_pi16(__m64 m, __m64 count)
PSLLW    __m128i _mm_slli_pi16(__m64 m, int count)
PSLLW    __m128i _mm_slli_pi16(__m128i m, __m128i count)
PSLLD    __m64 _mm_slli_pi32(__m64 m, int count)

```

PSLLD __m64 __mm_sll_pi32(__m64 m, __m64 count)
 PSLLD __m128i __mm_slli_epi32(__m128i m, int count)
 PSLLD __m128i __mm_sll_epi32(__m128i m, __m128i count)
 PSLLQ __m64 __mm_slli_si64(__m64 m, int count)
 PSLLQ __m64 __mm_sll_si64(__m64 m, __m64 count)
 PSLLQ __m128i __mm_slli_epi64(__m128i m, int count)
 PSLLQ __m128i __mm_sll_epi64(__m128i m, __m128i count)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
 If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF (fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
 If any part of the operand lies outside of the effective address space from 0 to FFFFH.

| | |
|-----|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSRAW/PSRAD—Shift Packed Data Right Arithmetic

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|---|-------------|------------------|---|
| 0F E1 /r | PSRAW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Shift words in <i>mm</i> right by <i>mm/m64</i> while shifting in sign bits. |
| 66 0F E1 /r | PSRAW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Shift words in <i>xmm1</i> right by <i>xmm2/m128</i> while shifting in sign bits. |
| 0F 71 /4 ib | PSRAW <i>mm</i> , <i>imm8</i> | Valid | Valid | Shift words in <i>mm</i> right by <i>imm8</i> while shifting in sign bits |
| 66 0F 71 /4 ib | PSRAW <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift words in <i>xmm1</i> right by <i>imm8</i> while shifting in sign bits |
| 0F E2 /r | PSRAD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Shift doublewords in <i>mm</i> right by <i>mm/m64</i> while shifting in sign bits. |
| 66 0F E2 /r | PSRAD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Shift doubleword in <i>xmm1</i> right by <i>xmm2 /m128</i> while shifting in sign bits. |
| 0F 72 /4 ib | PSRAD <i>mm</i> , <i>imm8</i> | Valid | Valid | Shift doublewords in <i>mm</i> right by <i>imm8</i> while shifting in sign bits. |
| 66 0F 72 /4 ib | PSRAD <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift doublewords in <i>xmm1</i> right by <i>imm8</i> while shifting in sign bits. |

Description

Shifts the bits in the individual data elements (words or doublewords) in the destination operand (first operand) to the right by the number of bits specified in the count operand (second operand). As the bits in the data elements are shifted right, the empty high-order bits are filled with the initial value of the sign bit of the data element. If the value specified by the count operand is greater than 15 (for words) or 31 (for doublewords), each destination data element is filled with the initial value of the sign bit of the element. (Figure 4-9 gives an example of shifting words in a 64-bit operand.)

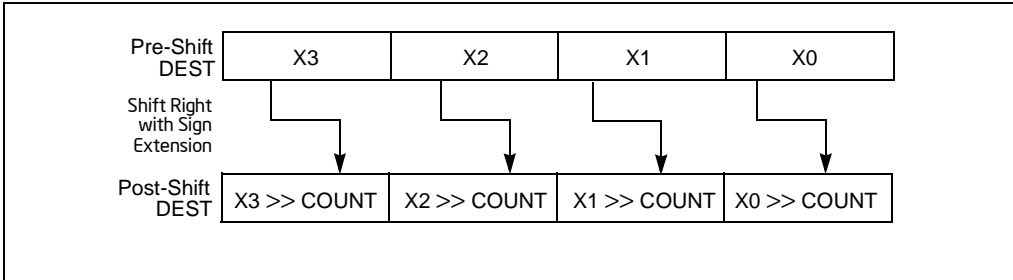


Figure 4-9. PSRAW and PSRAD Instruction Operation Using a 64-bit Operand

The destination operand may be an MMX technology register or an XMM register; the count operand can be either an MMX technology register or a 64-bit memory location, an XMM register or a 128-bit memory location, or an 8-bit immediate. Note that only the first 64-bits of a 128-bit count operand are checked to compute the count.

The PSRAW instruction shifts each of the words in the destination operand to the right by the number of bits specified in the count operand, and the PSRAD instruction shifts each of the doublewords in the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSRAW instruction with 64-bit operand:

```
IF (COUNT > 15)
    THEN COUNT ← 16;
FI;
DEST[15:0] ← SignExtend(DEST[15:0] >> COUNT);
(* Repeat shift operation for 2nd and 3rd words *)
DEST[63:48] ← SignExtend(DEST[63:48] >> COUNT);
```

PSRAD instruction with 64-bit operand:

```
IF (COUNT > 31)
    THEN COUNT ← 32;
FI;
DEST[31:0] ← SignExtend(DEST[31:0] >> COUNT);
DEST[63:32] ← SignExtend(DEST[63:32] >> COUNT);
```

PSRAW instruction with 128-bit operand:

```
COUNT ← COUNT_SOURCE[63:0];
```

INSTRUCTION SET REFERENCE, N-Z

```
IF (COUNT > 15)
    THEN COUNT ← 16;
FI;
DEST[15:0] ← SignExtend(DEST[15:0] >> COUNT);
(* Repeat shift operation for 2nd through 7th words *)
DEST[127:112] ← SignExtend(DEST[127:112] >> COUNT);
```

PSRAD instruction with 128-bit operand:

```
COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 31)
    THEN COUNT ← 32;
FI;
DEST[31:0] ← SignExtend(DEST[31:0] >> COUNT);
(* Repeat shift operation for 2nd and 3rd doublewords *)
DEST[127:96] ← SignExtend(DEST[127:96] >> COUNT);
```

Intel C/C++ Compiler Intrinsic Equivalents

```
PSRAW    __m64 __mm_srai_pi16 (__m64 m, int count)
PSRAW    __m64 __mm_sra_pi16 (__m64 m, __m64 count)
PSRAD    __m64 __mm_srai_pi32 (__m64 m, int count)
PSRAD    __m64 __mm_sra_pi32 (__m64 m, __m64 count)
PSRAW    __m128i __mm_srai_epi16(__m128i m, int count)
PSRAW    __m128i __mm_sra_epi16(__m128i m, __m128i count)
PSRAD    __m128i __mm_srai_epi32 (__m128i m, int count)
PSRAD    __m128i __mm_sra_epi32 (__m128i m, __m128i count)
```

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSRLDQ—Shift Double Quadword Right Logical

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|-------------------------------------|-------------|------------------|--|
| 66 0F 73 /3 1b | PSRLDQ <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift <i>xmm1</i> right by <i>imm8</i> while shifting in 0s. |

Description

Shifts the destination operand (first operand) to the right by the number of bytes specified in the count operand (second operand). The empty high-order bytes are cleared (set to all 0s). If the value specified by the count operand is greater than 15, the destination operand is set to all 0s. The destination operand is an XMM register. The count operand is an 8-bit immediate.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
TEMP ← COUNT;
IF (TEMP > 15) THEN TEMP ← 16; FI;
DEST ← DEST >> (temp * 8);
```

Intel C/C++ Compiler Intrinsic Equivalents

```
PSRLDQ  __m128i _mm_srli_si128 ( __m128i a, int imm)
```

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

```
#UD          If CR0.EM[bit 2] = 1.
              If CR4.OSFXSR[bit 9] = 0.
              If CPUID.01H:EDX.SSE2[bit 26] = 0.
              If the LOCK prefix is used.
#NM          If CR0.TS[bit 3] = 1.
```

Real-Address Mode Exceptions

Same exceptions as in protected mode.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

Numeric Exceptions

None.

PSRLW/PSRLD/PSRLQ—Shift Packed Data Right Logical

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|---|-------------|------------------|--|
| 0F D1 /r | PSRLW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Shift words in <i>mm</i> right by amount specified in <i>mm/m64</i> while shifting in 0s. |
| 66 0F D1 /r | PSRLW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Shift words in <i>xmm1</i> right by amount specified in <i>xmm2/m128</i> while shifting in 0s. |
| 0F 71 /2 ib | PSRLW <i>mm</i> , <i>imm8</i> | Valid | Valid | Shift words in <i>mm</i> right by <i>imm8</i> while shifting in 0s. |
| 66 0F 71 /2 ib | PSRLW <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift words in <i>xmm1</i> right by <i>imm8</i> while shifting in 0s. |
| 0F D2 /r | PSRLD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Shift doublewords in <i>mm</i> right by amount specified in <i>mm/m64</i> while shifting in 0s. |
| 66 0F D2 /r | PSRLD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Shift doublewords in <i>xmm1</i> right by amount specified in <i>xmm2/m128</i> while shifting in 0s. |
| 0F 72 /2 ib | PSRLD <i>mm</i> , <i>imm8</i> | Valid | Valid | Shift doublewords in <i>mm</i> right by <i>imm8</i> while shifting in 0s. |
| 66 0F 72 /2 ib | PSRLD <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift doublewords in <i>xmm1</i> right by <i>imm8</i> while shifting in 0s. |
| 0F D3 /r | PSRLQ <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Shift <i>mm</i> right by amount specified in <i>mm/m64</i> while shifting in 0s. |
| 66 0F D3 /r | PSRLQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Shift quadwords in <i>xmm1</i> right by amount specified in <i>xmm2/m128</i> while shifting in 0s. |
| 0F 73 /2 ib | PSRLQ <i>mm</i> , <i>imm8</i> | Valid | Valid | Shift <i>mm</i> right by <i>imm8</i> while shifting in 0s. |
| 66 0F 73 /2 ib | PSRLQ <i>xmm1</i> , <i>imm8</i> | Valid | Valid | Shift quadwords in <i>xmm1</i> right by <i>imm8</i> while shifting in 0s. |

Description

Shifts the bits in the individual data elements (words, doublewords, or quadword) in the destination operand (first operand) to the right by the number of bits specified in the count operand (second operand). As the bits in the data elements are shifted right, the empty high-order bits are cleared (set to 0). If the value specified by the count operand is greater than 15 (for words), 31 (for doublewords), or 63 (for a

quadword), then the destination operand is set to all 0s. Figure 4-10 gives an example of shifting words in a 64-bit operand.

The destination operand may be an MMX technology register or an XMM register; the count operand can be either an MMX technology register or a 64-bit memory location, an XMM register or a 128-bit memory location, or an 8-bit immediate. Note that only the first 64-bits of a 128-bit count operand are checked to compute the count.

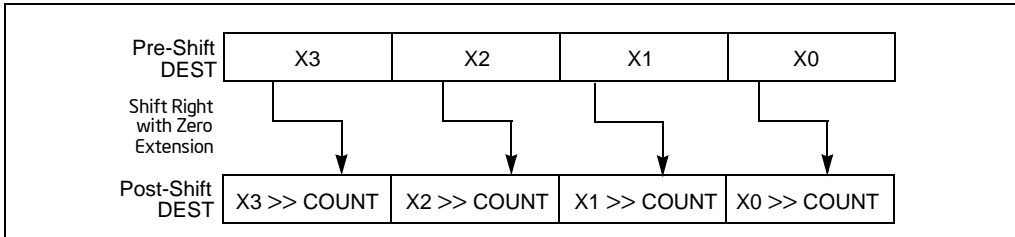


Figure 4-10. PSRLW, PSRLD, and PSRLQ Instruction Operation Using 64-bit Operand

The PSRLW instruction shifts each of the words in the destination operand to the right by the number of bits specified in the count operand; the PSRLD instruction shifts each of the doublewords in the destination operand; and the PSRLQ instruction shifts the quadword (or quadwords) in the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSRLW instruction with 64-bit operand:

```
IF (COUNT > 15)
  THEN
    DEST[64:0] ← 0000000000000000H
  ELSE
    DEST[15:0] ← ZeroExtend(DEST[15:0] >> COUNT);
    (* Repeat shift operation for 2nd and 3rd words *)
    DEST[63:48] ← ZeroExtend(DEST[63:48] >> COUNT);
  FI;
```

PSRLD instruction with 64-bit operand:

```
IF (COUNT > 31)
  THEN
    DEST[64:0] ← 0000000000000000H
  ELSE
    DEST[31:0] ← ZeroExtend(DEST[31:0] >> COUNT);
    DEST[63:32] ← ZeroExtend(DEST[63:32] >> COUNT);
  FI;
```


PSRLQ instruction with 64-bit operand:

```
IF (COUNT > 63)
  THEN
    DEST[64:0] ← 0000000000000000H
  ELSE
    DEST ← ZeroExtend(DEST >> COUNT);
FI;
```

PSRLW instruction with 128-bit operand:

```
COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 15)
  THEN
    DEST[128:0] ← 00000000000000000000000000000000H
  ELSE
    DEST[15:0] ← ZeroExtend(DEST[15:0] >> COUNT);
    (* Repeat shift operation for 2nd through 7th words *)
    DEST[127:112] ← ZeroExtend(DEST[127:112] >> COUNT);
FI;
```

PSRLD instruction with 128-bit operand:

```
COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 31)
  THEN
    DEST[128:0] ← 00000000000000000000000000000000H
  ELSE
    DEST[31:0] ← ZeroExtend(DEST[31:0] >> COUNT);
    (* Repeat shift operation for 2nd and 3rd doublewords *)
    DEST[127:96] ← ZeroExtend(DEST[127:96] >> COUNT);
FI;
```

PSRLQ instruction with 128-bit operand:

```
COUNT ← COUNT_SOURCE[63:0];
IF (COUNT > 15)
  THEN
    DEST[128:0] ← 00000000000000000000000000000000H
  ELSE
    DEST[63:0] ← ZeroExtend(DEST[63:0] >> COUNT);
    DEST[127:64] ← ZeroExtend(DEST[127:64] >> COUNT);
FI;
```

Intel C/C++ Compiler Intrinsic Equivalents

PSRLW `__m64 _mm_srl_pi16(__m64 m, int count)`

PSRLW `__m64 _mm_srl_pi16 (__m64 m, __m64 count)`

| | |
|-------|---|
| PSRLW | __m128i __mm_srli_epi16 (__m128i m, int count) |
| PSRLW | __m128i __mm_srl_epi16 (__m128i m, __m128i count) |
| PSRLD | __m64 __mm_srli_pi32 (__m64 m, int count) |
| PSRLD | __m64 __mm_srl_pi32 (__m64 m, __m64 count) |
| PSRLD | __m128i __mm_srli_epi32 (__m128i m, int count) |
| PSRLD | __m128i __mm_srl_epi32 (__m128i m, __m128i count) |
| PSRLQ | __m64 __mm_srli_si64 (__m64 m, int count) |
| PSRLQ | __m64 __mm_srl_si64 (__m64 m, __m64 count) |
| PSRLQ | __m128i __mm_srli_epi64 (__m128i m, int count) |
| PSRLQ | __m128i __mm_srl_epi64 (__m128i m, __m128i count) |

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSUBB/PSUBW/PSUBD—Subtract Packed Integers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|--|
| 0F F8 /r | PSUBB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract packed byte integers in <i>mm/m64</i> from packed byte integers in <i>mm</i> . |
| 66 0F F8 /r | PSUBB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed byte integers in <i>xmm2/m128</i> from packed byte integers in <i>xmm1</i> . |
| 0F F9 /r | PSUBW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract packed word integers in <i>mm/m64</i> from packed word integers in <i>mm</i> . |
| 66 0F F9 /r | PSUBW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed word integers in <i>xmm2/m128</i> from packed word integers in <i>xmm1</i> . |
| 0F FA /r | PSUBD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract packed doubleword integers in <i>mm/m64</i> from packed doubleword integers in <i>mm</i> . |
| 66 0F FA /r | PSUBD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed doubleword integers in <i>xmm2/mem128</i> from packed doubleword integers in <i>xmm1</i> . |

Description

Performs a SIMD subtract of the packed integers of the source operand (second operand) from the packed integers of the destination operand (first operand), and stores the packed integer results in the destination operand. See Figure 9-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD operation. Overflow is handled with wraparound, as described in the following paragraphs.

These instructions can operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

The PSUBB instruction subtracts packed byte integers. When an individual result is too large or too small to be represented in a byte, the result is wrapped around and the low 8 bits are written to the destination element.

The PSUBW instruction subtracts packed word integers. When an individual result is too large or too small to be represented in a word, the result is wrapped around and the low 16 bits are written to the destination element.

The PSUBD instruction subtracts packed doubleword integers. When an individual result is too large or too small to be represented in a doubleword, the result is wrapped around and the low 32 bits are written to the destination element.

Note that the PSUBB, PSUBW, and PSUBD instructions can operate on either unsigned or signed (two's complement notation) packed integers; however, it does not set bits in the EFLAGS register to indicate overflow and/or a carry. To prevent undetected overflow conditions, software must control the ranges of values upon which it operates.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSUBB instruction with 64-bit operands:

$DEST[7:0] \leftarrow DEST[7:0] - SRC[7:0];$
 (* Repeat subtract operation for 2nd through 7th byte *)
 $DEST[63:56] \leftarrow DEST[63:56] - SRC[63:56];$

PSUBB instruction with 128-bit operands:

$DEST[7:0] \leftarrow DEST[7:0] - SRC[7:0];$
 (* Repeat subtract operation for 2nd through 14th byte *)
 $DEST[127:120] \leftarrow DEST[111:120] - SRC[127:120];$

PSUBW instruction with 64-bit operands:

$DEST[15:0] \leftarrow DEST[15:0] - SRC[15:0];$
 (* Repeat subtract operation for 2nd and 3rd word *)
 $DEST[63:48] \leftarrow DEST[63:48] - SRC[63:48];$

PSUBW instruction with 128-bit operands:

$DEST[15:0] \leftarrow DEST[15:0] - SRC[15:0];$
 (* Repeat subtract operation for 2nd through 7th word *)
 $DEST[127:112] \leftarrow DEST[127:112] - SRC[127:112];$

PSUBD instruction with 64-bit operands:

$DEST[31:0] \leftarrow DEST[31:0] - SRC[31:0];$
 $DEST[63:32] \leftarrow DEST[63:32] - SRC[63:32];$

PSUBD instruction with 128-bit operands:

$DEST[31:0] \leftarrow DEST[31:0] - SRC[31:0];$
 (* Repeat subtract operation for 2nd and 3rd doubleword *)
 $DEST[127:96] \leftarrow DEST[127:96] - SRC[127:96];$

Intel C/C++ Compiler Intrinsic Equivalents

PSUBB `__m64 _mm_sub_pi8(__m64 m1, __m64 m2)`

PSUBW __m64 __mm_sub_pi16(__m64 m1, __m64 m2)
 PSUBD __m64 __mm_sub_pi32(__m64 m1, __m64 m2)
 PSUBB __m128i __mm_sub_epi8 (__m128i a, __m128i b)
 PSUBW __m128i __mm_sub_epi16 (__m128i a, __m128i b)
 PSUBD __m128i __mm_sub_epi32 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
 If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
 If any part of the operand lies outside of the effective address space from 0 to FFFFH.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one

that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

If the LOCK prefix is used.

| | |
|-----|---|
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same as for protected mode exceptions.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSUBQ—Subtract Packed Quadword Integers

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|------------------------------|-------------|-----------------|--|
| 0F FB /r | PSUBQ <i>mm1, mm2/m64</i> | Valid | Valid | Subtract quadword integer in <i>mm1</i> from <i>mm2/m64</i> . |
| 66 0F FB /r | PSUBQ <i>xmm1, xmm2/m128</i> | Valid | Valid | Subtract packed quadword integers in <i>xmm1</i> from <i>xmm2/m128</i> . |

Description

Subtracts the second operand (source operand) from the first operand (destination operand) and stores the result in the destination operand. The source operand can be a quadword integer stored in an MMX technology register or a 64-bit memory location, or it can be two packed quadword integers stored in an XMM register or an 128-bit memory location. The destination operand can be a quadword integer stored in an MMX technology register or two packed quadword integers stored in an XMM register. When packed quadword operands are used, a SIMD subtract is performed. When a quadword result is too large to be represented in 64 bits (overflow), the result is wrapped around and the low 64 bits are written to the destination element (that is, the carry is ignored).

Note that the PSUBQ instruction can operate on either unsigned or signed (two's complement notation) integers; however, it does not set bits in the EFLAGS register to indicate overflow and/or a carry. To prevent undetected overflow conditions, software must control the ranges of the values upon which it operates.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSUBQ instruction with 64-Bit operands:

$$\text{DEST}[63:0] \leftarrow \text{DEST}[63:0] - \text{SRC}[63:0];$$

PSUBQ instruction with 128-Bit operands:

$$\begin{aligned} \text{DEST}[63:0] &\leftarrow \text{DEST}[63:0] - \text{SRC}[63:0]; \\ \text{DEST}[127:64] &\leftarrow \text{DEST}[127:64] - \text{SRC}[127:64]; \end{aligned}$$

Intel C/C++ Compiler Intrinsic Equivalents

PSUBQ `__m64 _mm_sub_si64(__m64 m1, __m64 m2)`

PSUBQ `__m128i _mm_sub_epi64(__m128i m1, __m128i m2)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.
(128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.
(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.
If CPUID.01H:EDX.SSE2[bit 26] = 0.
If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PSUBSB/PSUBSW—Subtract Packed Signed Integers with Signed Saturation

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--|-------------|-----------------|--|
| 0F E8 /r | PSUBSB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract signed packed bytes in <i>mm/m64</i> from signed packed bytes in <i>mm</i> and saturate results. |
| 66 0F E8 /r | PSUBSB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed signed byte integers in <i>xmm2/m128</i> from packed signed byte integers in <i>xmm1</i> and saturate results. |
| 0F E9 /r | PSUBSW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract signed packed words in <i>mm/m64</i> from signed packed words in <i>mm</i> and saturate results. |
| 66 0F E9 /r | PSUBSW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed signed word integers in <i>xmm2/m128</i> from packed signed word integers in <i>xmm1</i> and saturate results. |

Description

Performs a SIMD subtract of the packed signed integers of the source operand (second operand) from the packed signed integers of the destination operand (first operand), and stores the packed integer results in the destination operand. See Figure 9-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD operation. Overflow is handled with signed saturation, as described in the following paragraphs.

These instructions can operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

The PSUBSB instruction subtracts packed signed byte integers. When an individual byte result is beyond the range of a signed byte integer (that is, greater than 7FH or less than 80H), the saturated value of 7FH or 80H, respectively, is written to the destination operand.

The PSUBSW instruction subtracts packed signed word integers. When an individual word result is beyond the range of a signed word integer (that is, greater than 7FFFH or less than 8000H), the saturated value of 7FFFH or 8000H, respectively, is written to the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSUBSB instruction with 64-bit operands:

DEST[7:0] ← SaturateToSignedByte (DEST[7:0] – SRC (7:0));
 (* Repeat subtract operation for 2nd through 7th bytes *)
 DEST[63:56] ← SaturateToSignedByte (DEST[63:56] – SRC[63:56]);

PSUBSB instruction with 128-bit operands:

DEST[7:0] ← SaturateToSignedByte (DEST[7:0] – SRC[7:0]);
 (* Repeat subtract operation for 2nd through 14th bytes *)
 DEST[127:120] ← SaturateToSignedByte (DEST[111:120] – SRC[127:120]);

PSUBSW instruction with 64-bit operands

DEST[15:0] ← SaturateToSignedWord (DEST[15:0] – SRC[15:0]);
 (* Repeat subtract operation for 2nd and 7th words *)
 DEST[63:48] ← SaturateToSignedWord (DEST[63:48] – SRC[63:48]);

PSUBSW instruction with 128-bit operands

DEST[15:0] ← SaturateToSignedWord (DEST[15:0] – SRC[15:0]);
 (* Repeat subtract operation for 2nd through 7th words *)
 DEST[127:112] ← SaturateToSignedWord (DEST[127:112] – SRC[127:112]);

Intel C/C++ Compiler Intrinsic Equivalents

PSUBSB `__m64_mm_subs_pi8(__m64 m1, __m64 m2)`
 PSUBSB `__m128i_mm_subs_epi8(__m128i m1, __m128i m2)`
 PSUBSW `__m64_mm_subs_pi16(__m64 m1, __m64 m2)`
 PSUBSW `__m128i_mm_subs_epi16(__m128i m1, __m128i m2)`

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
|--------|---|

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----------------|---|
| | (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PSUBUSB/PSUBUSW—Subtract Packed Unsigned Integers with Unsigned Saturation

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|---|-------------|-----------------|---|
| 0F D8 /r | PSUBUSB <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract unsigned packed bytes in <i>mm/m64</i> from unsigned packed bytes in <i>mm</i> and saturate result. |
| 66 0F D8 /r | PSUBUSB <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed unsigned byte integers in <i>xmm2/m128</i> from packed unsigned byte integers in <i>xmm1</i> and saturate result. |
| 0F D9 /r | PSUBUSW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Subtract unsigned packed words in <i>mm/m64</i> from unsigned packed words in <i>mm</i> and saturate result. |
| 66 0F D9 /r | PSUBUSW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed unsigned word integers in <i>xmm2/m128</i> from packed unsigned word integers in <i>xmm1</i> and saturate result. |

Description

Performs a SIMD subtract of the packed unsigned integers of the source operand (second operand) from the packed unsigned integers of the destination operand (first operand), and stores the packed unsigned integer results in the destination operand. See Figure 9-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD operation. Overflow is handled with unsigned saturation, as described in the following paragraphs.

These instructions can operate on either 64-bit or 128-bit operands. When operating on 64-bit operands, the destination operand must be an MMX technology register and the source operand can be either an MMX technology register or a 64-bit memory location. When operating on 128-bit operands, the destination operand must be an XMM register and the source operand can be either an XMM register or a 128-bit memory location.

The PSUBUSB instruction subtracts packed unsigned byte integers. When an individual byte result is less than zero, the saturated value of 00H is written to the destination operand.

The PSUBUSW instruction subtracts packed unsigned word integers. When an individual word result is less than zero, the saturated value of 0000H is written to the destination operand.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PSUBUSB instruction with 64-bit operands:

```
DEST[7:0] ← SaturateToUnsignedByte (DEST[7:0] – SRC (7:0) );
(* Repeat add operation for 2nd through 7th bytes *)
DEST[63:56] ← SaturateToUnsignedByte (DEST[63:56] – SRC[63:56]);
```

PSUBUSB instruction with 128-bit operands:

```
DEST[7:0] ← SaturateToUnsignedByte (DEST[7:0] – SRC[7:0]);
(* Repeat add operation for 2nd through 14th bytes *)
DEST[127:120] ← SaturateToUnsignedByte (DEST[127:120] – SRC[127:120]);
```

PSUBUSW instruction with 64-bit operands:

```
DEST[15:0] ← SaturateToUnsignedWord (DEST[15:0] – SRC[15:0] );
(* Repeat add operation for 2nd and 3rd words *)
DEST[63:48] ← SaturateToUnsignedWord (DEST[63:48] – SRC[63:48] );
```

PSUBUSW instruction with 128-bit operands:

```
DEST[15:0] ← SaturateToUnsignedWord (DEST[15:0] – SRC[15:0]);
(* Repeat add operation for 2nd through 7th words *)
DEST[127:112] ← SaturateToUnsignedWord (DEST[127:112] – SRC[127:112]);
```

Intel C/C++ Compiler Intrinsic Equivalents

```
PSUBUSB __m64 __mm_subs_pu8(__m64 m1, __m64 m2)
PSUBUSB __m128i __mm_subs_epu8(__m128i m1, __m128i m2)
PSUBUSW __m64 __mm_subs_pu16(__m64 m1, __m64 m2)
PSUBUSW __m128i __mm_subs_epu16(__m128i m1, __m128i m2)
```

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. |

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

If the LOCK prefix is used.

| | |
|------------------|---|
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|------------------|--|
| #PF (fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|------------------|---|
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PTEST- Logical Compare

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------|---|-------------|------------------|---|
| 66 OF 38 17 /r | PTEST <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Set ZF if <i>xmm2/m128</i> AND <i>xmm1</i> result is all 0s. Set CF if <i>xmm2/m128</i> AND NOT <i>xmm1</i> result is all 0s. |

Description

Performs a bitwise AND of the destination operand (first operand) and the source operand (second operand), then sets the ZF flag only if all bits in the result are 0. PTEST sets the CF flag if all bits in the result are 0 of the bitwise AND of the source operand (second operand) and the bitwise logical NOT of the destination operand.

Operation

```
IF (SRC[127:0] bitwiseAND DEST[127:0] = 0)
    THEN ZF ← 1;
    ELSE ZF ← 0; FI;
IF (SRC[127:0] bitwiseAND (bitwiseNOT DEST[127:0]) = 0)
    THEN CF ← 1;
    ELSE CF ← 0; FI;
DEST[127:0] Unmodified;
AF = OF = PF = SF ← 0;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
PTEST int _mm_testz_si128 (__m128i s1, __m128i s2);
int _mm_testc_si128 (__m128i s1, __m128i s2);
int _mm_testnzc_si128 (__m128i s1, __m128i s2);
```

Flags Affected

The OF, AF, PF, SF flags are cleared and the ZF, CF flags are set according to the operation.

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.

| | |
|------------------|--|
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|------------------|-------------------|
| #PF (fault-code) | For a page fault. |
|------------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. |

Either the prefix REP (F3h) or REPN (F2H) is used.

PUNPCKHBW/PUNPCKHWD/PUNPCKHDQ/PUNPCKHQDQ— Unpack High Data

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|---|
| 0F 68 /r | PUNPCKHBW <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Unpack and interleave high-order bytes from <i>mm</i> and <i>mm/m64</i> into <i>mm</i> . |
| 66 0F 68 /r | PUNPCKHBW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpack and interleave high-order bytes from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |
| 0F 69 /r | PUNPCKHWD <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Unpack and interleave high-order words from <i>mm</i> and <i>mm/m64</i> into <i>mm</i> . |
| 66 0F 69 /r | PUNPCKHWD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpack and interleave high-order words from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |
| 0F 6A /r | PUNPCKHDQ <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Unpack and interleave high-order doublewords from <i>mm</i> and <i>mm/m64</i> into <i>mm</i> . |
| 66 0F 6A /r | PUNPCKHDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpack and interleave high-order doublewords from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |
| 66 0F 6D /r | PUNPCKHQDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpack and interleave high-order quadwords from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |

Description

Unpacks and interleaves the high-order data elements (bytes, words, doublewords, or quadwords) of the destination operand (first operand) and source operand (second operand) into the destination operand. Figure 4-11 shows the unpack operation for bytes in 64-bit operands. The low-order data elements are ignored.

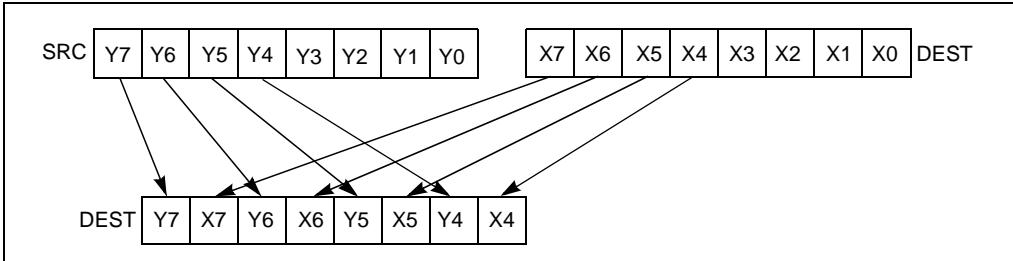


Figure 4-11. PUNPCKHBW Instruction Operation Using 64-bit Operands

The source operand can be an MMX technology register or a 64-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. When the source data comes from a 64-bit memory operand, the full 64-bit operand is accessed from memory, but the instruction uses only the high-order 32 bits. When the source data comes from a 128-bit memory operand, an implementation may fetch only the appropriate 64 bits; however, alignment to a 16-byte boundary and normal segment checking will still be enforced.

The PUNPCKHBW instruction interleaves the high-order bytes of the source and destination operands, the PUNPCKHWD instruction interleaves the high-order words of the source and destination operands, the PUNPCKHDQ instruction interleaves the high-order doubleword (or doublewords) of the source and destination operands, and the PUNPCKHQDQ instruction interleaves the high-order quadwords of the source and destination operands.

These instructions can be used to convert bytes to words, words to doublewords, doublewords to quadwords, and quadwords to double quadwords, respectively, by placing all 0s in the source operand. Here, if the source operand contains all 0s, the result (stored in the destination operand) contains zero extensions of the high-order data elements from the original value in the destination operand. For example, with the PUNPCKHBW instruction the high-order bytes are zero extended (that is, unpacked into unsigned word integers), and with the PUNPCKHWD instruction, the high-order words are zero extended (unpacked into unsigned doubleword integers).

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PUNPCKHBW instruction with 64-bit operands:

```
DEST[7:0] ← DEST[39:32];
DEST[15:8] ← SRC[39:32];
DEST[23:16] ← DEST[47:40];
DEST[31:24] ← SRC[47:40];
```

$\text{DEST}[39:32] \leftarrow \text{DEST}[55:48];$
 $\text{DEST}[47:40] \leftarrow \text{SRC}[55:48];$
 $\text{DEST}[55:48] \leftarrow \text{DEST}[63:56];$
 $\text{DEST}[63:56] \leftarrow \text{SRC}[63:56];$

PUNPCKHW instruction with 64-bit operands:

$\text{DEST}[15:0] \leftarrow \text{DEST}[47:32];$
 $\text{DEST}[31:16] \leftarrow \text{SRC}[47:32];$
 $\text{DEST}[47:32] \leftarrow \text{DEST}[63:48];$
 $\text{DEST}[63:48] \leftarrow \text{SRC}[63:48];$

PUNPCKHDQ instruction with 64-bit operands:

$\text{DEST}[31:0] \leftarrow \text{DEST}[63:32];$
 $\text{DEST}[63:32] \leftarrow \text{SRC}[63:32];$

PUNPCKHBW instruction with 128-bit operands:

$\text{DEST}[7:0] \leftarrow \text{DEST}[71:64];$
 $\text{DEST}[15:8] \leftarrow \text{SRC}[71:64];$
 $\text{DEST}[23:16] \leftarrow \text{DEST}[79:72];$
 $\text{DEST}[31:24] \leftarrow \text{SRC}[79:72];$
 $\text{DEST}[39:32] \leftarrow \text{DEST}[87:80];$
 $\text{DEST}[47:40] \leftarrow \text{SRC}[87:80];$
 $\text{DEST}[55:48] \leftarrow \text{DEST}[95:88];$
 $\text{DEST}[63:56] \leftarrow \text{SRC}[95:88];$
 $\text{DEST}[71:64] \leftarrow \text{DEST}[103:96];$
 $\text{DEST}[79:72] \leftarrow \text{SRC}[103:96];$
 $\text{DEST}[87:80] \leftarrow \text{DEST}[111:104];$
 $\text{DEST}[95:88] \leftarrow \text{SRC}[111:104];$
 $\text{DEST}[103:96] \leftarrow \text{DEST}[119:112];$
 $\text{DEST}[111:104] \leftarrow \text{SRC}[119:112];$
 $\text{DEST}[119:112] \leftarrow \text{DEST}[127:120];$
 $\text{DEST}[127:120] \leftarrow \text{SRC}[127:120];$

PUNPCKHWD instruction with 128-bit operands:

$\text{DEST}[15:0] \leftarrow \text{DEST}[79:64];$
 $\text{DEST}[31:16] \leftarrow \text{SRC}[79:64];$
 $\text{DEST}[47:32] \leftarrow \text{DEST}[95:80];$
 $\text{DEST}[63:48] \leftarrow \text{SRC}[95:80];$
 $\text{DEST}[79:64] \leftarrow \text{DEST}[111:96];$
 $\text{DEST}[95:80] \leftarrow \text{SRC}[111:96];$
 $\text{DEST}[111:96] \leftarrow \text{DEST}[127:112];$
 $\text{DEST}[127:112] \leftarrow \text{SRC}[127:112];$

PUNPCKHDQ instruction with 128-bit operands:

$\text{DEST}[31:0] \leftarrow \text{DEST}[95:64];$
 $\text{DEST}[63:32] \leftarrow \text{SRC}[95:64];$

DEST[95:64] ← DEST[127:96];
 DEST[127:96] ← SRC[127:96];

PUNPCKHQDQ instruction:

DEST[63:0] ← DEST[127:64];
 DEST[127:64] ← SRC[127:64];

Intel C/C++ Compiler Intrinsic Equivalents

PUNPCKHBW __m64 _mm_unpackhi_pi8(__m64 m1, __m64 m2)
 PUNPCKHBW __m128i _mm_unpackhi_epi8(__m128i m1, __m128i m2)
 PUNPCKHWD __m64 _mm_unpackhi_pi16(__m64 m1, __m64 m2)
 PUNPCKHWD __m128i _mm_unpackhi_epi16(__m128i m1, __m128i m2)
 PUNPCKHDQ __m64 _mm_unpackhi_pi32(__m64 m1, __m64 m2)
 PUNPCKHDQ __m128i _mm_unpackhi_epi32(__m128i m1, __m128i m2)
 PUNPCKHQDQ __m128i _mm_unpackhi_epi64 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions (except PUNPCKHQDQ) on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
 (PUNPCKHQDQ only) If CPUID.01H: EDX.SSE2[bit 26] = 0.
 If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF (fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP If any part of the operand lies outside of the effective address space from 0 to FFFFH.

(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions (except PUNPCKHQDQ) on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.

(PUNPCKHQDQ only) If CPUID.01H:EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

(128-bit version only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.

(128-bit operations only) If CR4.OSFXSR[bit 9] = 0.

(128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

| | |
|------------------|---|
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

PUNPCKLBW/PUNPCKLWD/PUNPCKLDQ/PUNPCKLQDQ— Unpack Low Data

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F 60 /r | PUNPCKLBW <i>mm</i> , <i>mm/m32</i> | Valid | Valid | Interleave low-order bytes from <i>mm</i> and <i>mm/m32</i> into <i>mm</i> . |
| 66 0F 60 /r | PUNPCKLBW <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Interleave low-order bytes from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |
| 0F 61 /r | PUNPCKLWD <i>mm</i> , <i>mm/m32</i> | Valid | Valid | Interleave low-order words from <i>mm</i> and <i>mm/m32</i> into <i>mm</i> . |
| 66 0F 61 /r | PUNPCKLWD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Interleave low-order words from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |
| 0F 62 /r | PUNPCKLDQ <i>mm</i> , <i>mm/m32</i> | Valid | Valid | Interleave low-order doublewords from <i>mm</i> and <i>mm/m32</i> into <i>mm</i> . |
| 66 0F 62 /r | PUNPCKLDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Interleave low-order doublewords from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> . |
| 66 0F 6C /r | PUNPCKLQDQ <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Interleave low-order quadword from <i>xmm1</i> and <i>xmm2/m128</i> into <i>xmm1</i> register. |

Description

Unpacks and interleaves the low-order data elements (bytes, words, doublewords, and quadwords) of the destination operand (first operand) and source operand (second operand) into the destination operand. (Figure 4-12 shows the unpack operation for bytes in 64-bit operands.). The high-order data elements are ignored.

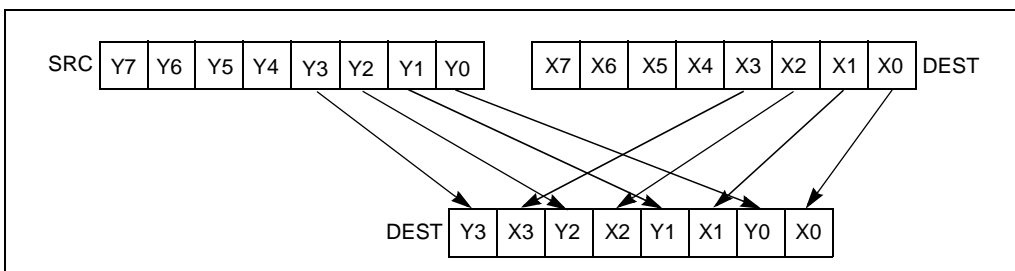


Figure 4-12. PUNPCKLBW Instruction Operation Using 64-bit Operands

The source operand can be an MMX technology register or a 32-bit memory location, or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. When the source data comes from a 128-bit memory operand, an implementation may fetch only the appropriate 64 bits; however, alignment to a 16-byte boundary and normal segment checking will still be enforced.

The PUNPCKLBW instruction interleaves the low-order bytes of the source and destination operands, the PUNPCKLWD instruction interleaves the low-order words of the source and destination operands, the PUNPCKLDQ instruction interleaves the low-order doubleword (or doublewords) of the source and destination operands, and the PUNPCKLQDQ instruction interleaves the low-order quadwords of the source and destination operands.

These instructions can be used to convert bytes to words, words to doublewords, doublewords to quadwords, and quadwords to double quadwords, respectively, by placing all 0s in the source operand. Here, if the source operand contains all 0s, the result (stored in the destination operand) contains zero extensions of the high-order data elements from the original value in the destination operand. For example, with the PUNPCKLBW instruction the high-order bytes are zero extended (that is, unpacked into unsigned word integers), and with the PUNPCKLWD instruction, the high-order words are zero extended (unpacked into unsigned doubleword integers).

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

PUNPCKLBW instruction with 64-bit operands:

```
DEST[63:56] ← SRC[31:24];
DEST[55:48] ← DEST[31:24];
DEST[47:40] ← SRC[23:16];
DEST[39:32] ← DEST[23:16];
DEST[31:24] ← SRC[15:8];
DEST[23:16] ← DEST[15:8];
DEST[15:8] ← SRC[7:0];
DEST[7:0] ← DEST[7:0];
```

PUNPCKLWD instruction with 64-bit operands:

```
DEST[63:48] ← SRC[31:16];
DEST[47:32] ← DEST[31:16];
DEST[31:16] ← SRC[15:0];
DEST[15:0] ← DEST[15:0];
```

PUNPCKLDQ instruction with 64-bit operands:

```
DEST[63:32] ← SRC[31:0];
DEST[31:0] ← DEST[31:0];
```

PUNPCKLBW instruction with 128-bit operands:

```

DEST[7:0] ← DEST[7:0];
DEST[15:8] ← SRC[7:0];
DEST[23:16] ← DEST[15:8];
DEST[31:24] ← SRC[15:8];
DEST[39:32] ← DEST[23:16];
DEST[47:40] ← SRC[23:16];
DEST[55:48] ← DEST[31:24];
DEST[63:56] ← SRC[31:24];
DEST[71:64] ← DEST[39:32];
DEST[79:72] ← SRC[39:32];
DEST[87:80] ← DEST[47:40];
DEST[95:88] ← SRC[47:40];
DEST[103:96] ← DEST[55:48];
DEST[111:104] ← SRC[55:48];
DEST[119:112] ← DEST[63:56];
DEST[127:120] ← SRC[63:56];

```

PUNPCKLWD instruction with 128-bit operands:

```

DEST[15:0] ← DEST[15:0];
DEST[31:16] ← SRC[15:0];
DEST[47:32] ← DEST[31:16];
DEST[63:48] ← SRC[31:16];
DEST[79:64] ← DEST[47:32];
DEST[95:80] ← SRC[47:32];
DEST[111:96] ← DEST[63:48];
DEST[127:112] ← SRC[63:48];

```

PUNPCKLDQ instruction with 128-bit operands:

```

DEST[31:0] ← DEST[31:0];
DEST[63:32] ← SRC[31:0];
DEST[95:64] ← DEST[63:32];
DEST[127:96] ← SRC[63:32];

```

PUNPCKLQDQ

```

DEST[63:0] ← DEST[63:0];
DEST[127:64] ← SRC[63:0];

```

Intel C/C++ Compiler Intrinsic Equivalents

```

PUNPCKLBW    __m64 _mm_unpacklo_pi8 (__m64 m1, __m64 m2)
PUNPCKLBW    __m128i _mm_unpacklo_epi8 (__m128i m1, __m128i m2)
PUNPCKLWD    __m64 _mm_unpacklo_pi16 (__m64 m1, __m64 m2)
PUNPCKLWD    __m128i _mm_unpacklo_epi16 (__m128i m1, __m128i m2)

```

PUNPCKLDQ __m64 _mm_unpacklo_pi32 (__m64 m1, __m64 m2)
 PUNPCKLDQ __m128i _mm_unpacklo_epi32 (__m128i m1, __m128i m2)
 PUNPCKLQDQ __m128i _mm_unpacklo_epi64 (__m128i m1, __m128i m2)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions (PUNPCKLQDQ) on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD.
 (PUNPCKLQDQ only) If CPUID.01H:EDX.SSE2[bit 26] = 0.
 If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.

#MF (64-bit operations only) If there is a pending x87 FPU exception.

#PF(fault-code) If a page fault occurs.

#AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real-Address Mode Exceptions

#GP If any part of the operand lies outside of the effective address space from 0 to 0FFFFH.
 (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#UD If CR0.EM[bit 2] = 1.
 (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions (except PUNPCKLQDQ) on a non-SSE2

capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. (PUNPCKLQDQ only) If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used.

#NM If CR0.TS[bit 3] = 1.
 #MF (64-bit operations only) If there is a pending x87 FPU exception.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.
 #AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.
 #GP(0) If the memory address is in a non-canonical form. (128-bit version only) If memory operand is not aligned on a 16-byte boundary, regardless of segment.
 #UD If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used.
 #NM If CR0.TS[bit 3] = 1.
 #MF (64-bit operations only) If there is a pending x87 FPU exception.
 #PF(fault-code) If a page fault occurs.
 #AC(0) (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

PUSH—Push Word, Doubleword or Quadword Onto the Stack

| Opcode* | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|---------------|-------------------|-------------|-----------------|---|
| FF /6 | PUSH <i>r/m16</i> | Valid | Valid | Push <i>r/m16</i> . |
| FF /6 | PUSH <i>r/m32</i> | N.E. | Valid | Push <i>r/m32</i> . |
| FF /6 | PUSH <i>r/m64</i> | Valid | N.E. | Push <i>r/m64</i> . Default operand size 64-bits. |
| 50+ <i>rw</i> | PUSH <i>r16</i> | Valid | Valid | Push <i>r16</i> . |
| 50+ <i>rd</i> | PUSH <i>r32</i> | N.E. | Valid | Push <i>r32</i> . |
| 50+ <i>rd</i> | PUSH <i>r64</i> | Valid | N.E. | Push <i>r64</i> . Default operand size 64-bits. |
| 6A | PUSH <i>imm8</i> | Valid | Valid | Push sign-extended <i>imm8</i> . <i>Stack pointer is incremented by the size of stack pointer.</i> |
| 68 | PUSH <i>imm16</i> | Valid | Valid | Push sign-extended <i>imm16</i> . <i>Stack pointer is incremented by the size of stack pointer.</i> |
| 68 | PUSH <i>imm32</i> | Valid | Valid | Push sign-extended <i>imm32</i> . <i>Stack pointer is incremented by the size of stack pointer.</i> |
| 0E | PUSH CS | Invalid | Valid | Push CS. |
| 16 | PUSH SS | Invalid | Valid | Push SS. |
| 1E | PUSH DS | Invalid | Valid | Push DS. |
| 06 | PUSH ES | Invalid | Valid | Push ES. |
| 0F A0 | PUSH FS | Valid | Valid | Push FS and decrement stack pointer by 16 bits. |
| 0F A0 | PUSH FS | N.E. | Valid | Push FS and decrement stack pointer by 32 bits. |
| 0F A0 | PUSH FS | Valid | N.E. | Push FS. Default operand size 64-bits. (66H override causes 16-bit operation). |
| 0F A8 | PUSH GS | Valid | Valid | Push GS and decrement stack pointer by 16 bits. |
| 0F A8 | PUSH GS | N.E. | Valid | Push GS and decrement stack pointer by 32 bits. |

| Opcode* | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|---------|-------------|-------------|------------------|--|
| OF A8 | PUSH GS | Valid | N.E. | Push GS, default operand size 64-bits. (66H override causes 16-bit operation). |

NOTES:

* See IA-32 Architecture Compatibility section below.

Description

Decrements the stack pointer and then stores the source operand on the top of the stack. The address-size attribute of the stack segment determines the stack pointer size (16, 32 or 64 bits). The operand-size attribute of the current code segment determines the amount the stack pointer is decremented (2, 4 or 8 bytes).

In non-64-bit modes: if the address-size and operand-size attributes are 32, the 32-bit ESP register (stack pointer) is decremented by 4. If both attributes are 16, the 16-bit SP register (stack pointer) is decremented by 2.

If the source operand is an immediate and its size is less than the address size of the stack, a sign-extended value is pushed on the stack. If the source operand is the FS or GS and its size is less than the address size of the stack, the zero-extended value is pushed on the stack.

The B flag in the stack segment's segment descriptor determines the stack's address-size attribute. The D flag in the current code segment's segment descriptor (with prefixes), determines the operand-size attribute and the address-size attribute of the source operand. Pushing a 16-bit operand when the stack address-size attribute is 32 can result in a misaligned stack pointer (a stack pointer that is not be aligned on a doubleword boundary).

The PUSH ESP instruction pushes the value of the ESP register as it existed before the instruction was executed. Thus if a PUSH instruction uses a memory operand in which the ESP register is used for computing the operand address, the address of the operand is computed before the ESP register is decremented.

In the real-address mode, if the ESP or SP register is 1 when the PUSH instruction is executed, an #SS exception is generated but not delivered (the stack error reported prevents #SS delivery). Next, the processor generates a #DF exception and enters a shutdown state as described in the #DF discussion in Chapter 5 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A*.

In 64-bit mode, the instruction's default operation size is 64 bits. In a push, the 64-bit RSP register (stack pointer) is decremented by 8. A 66H override causes 16-bit operation. Note that pushing a 16-bit operand can result in the stack pointer misaligned to 8-byte boundary.

IA-32 Architecture Compatibility

For IA-32 processors from the Intel 286 on, the PUSH ESP instruction pushes the value of the ESP register as it existed before the instruction was executed. (This is also true for Intel 64 architecture, real-address and virtual-8086 modes of IA-32 architecture.) For the Intel[®] 8086 processor, the PUSH SP instruction pushes the new value of the SP register (that is the value after it has been decremented by 2).

Operation

```

IF StackAddrSize = 64
  THEN
    IF OperandSize = 64
      THEN
        RSP ← (RSP – 8);
        IF (SRC is FS or GS)
          THEN
            TEMP = ZeroExtend64(SRC);
          ELSE IF (SRC is IMMEDIATE)
            TEMP = SignExtend64(SRC); FI;
          ELSE
            TEMP = SRC;
        FI
        RSP ← TEMP; (* Push quadword *)
      ELSE (* OperandSize = 16; 66H used *)
        RSP ← (RSP – 2);
        RSP ← SRC; (* Push word *)
      FI;
    ELSE IF StackAddrSize = 32
      THEN
        IF OperandSize = 32
          THEN
            ESP ← (ESP – 4);
            IF (SRC is FS or GS)
              THEN
                TEMP = ZeroExtend32(SRC);
              ELSE IF (SRC is IMMEDIATE)
                TEMP = SignExtend32(SRC); FI;
              ELSE
                TEMP = SRC;
            FI;
            SS:ESP ← TEMP; (* Push doubleword *)
          ELSE (* OperandSize = 16*)
            ESP ← (ESP – 2);
            SS:ESP ← SRC; (* Push word *)
          FI;
        FI;
    FI;
  FI;

```

```

    FI;
ELSE StackAddrSize = 16
  IF OperandSize = 16
    THEN
      SP ← (SP – 2);
      SS:SP ← SRC; (* Push word *)
    ELSE (* OperandSize = 32 *)
      SP ← (SP – 4);
      SS:SP ← SRC; (* Push doubleword *)
  FI;
FI;
FI;

```

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. If the new value of the SP or ESP register is outside the stack segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|--------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
|--------|---|

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(U) | If the stack address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

PUSHA/PUSHAD—Push All General-Purpose Registers

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|---|
| 60 | PUSHA | Invalid | Valid | Push AX, CX, DX, BX, original SP, BP, SI, and DI. |
| 60 | PUSHAD | Invalid | Valid | Push EAX, ECX, EDX, EBX, original ESP, EBP, ESI, and EDI. |

Description

Pushes the contents of the general-purpose registers onto the stack. The registers are stored on the stack in the following order: EAX, ECX, EDX, EBX, ESP (original value), EBP, ESI, and EDI (if the current operand-size attribute is 32) and AX, CX, DX, BX, SP (original value), BP, SI, and DI (if the operand-size attribute is 16). These instructions perform the reverse operation of the POPA/POPAD instructions. The value pushed for the ESP or SP register is its value before prior to pushing the first register (see the “Operation” section below).

The PUSHA (push all) and PUSHAD (push all double) mnemonics reference the same opcode. The PUSHA instruction is intended for use when the operand-size attribute is 16 and the PUSHAD instruction for when the operand-size attribute is 32. Some assemblers may force the operand size to 16 when PUSHA is used and to 32 when PUSHAD is used. Others may treat these mnemonics as synonyms (PUSHA/PUSHAD) and use the current setting of the operand-size attribute to determine the size of values to be pushed from the stack, regardless of the mnemonic used.

In the real-address mode, if the ESP or SP register is 1, 3, or 5 when PUSHA/PUSHAD executes: an #SS exception is generated but not delivered (the stack error reported prevents #SS delivery). Next, the processor generates a #DF exception and enters a shutdown state as described in the #DF discussion in Chapter 5 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A*.

This instruction executes as described in compatibility mode and legacy mode. It is not valid in 64-bit mode.

Operation

IF 64-bit Mode

THEN #UD

FI;

IF OperandSize = 32 (* PUSHAD instruction *)

THEN

Temp ← (ESP);

Push(EAX);

```

Push(ECX);
Push(EDX);
Push(EBX);
Push(Temp);
Push(EBP);
Push(ESI);
Push(EDI);

```

```
ELSE (* OperandSize = 16, PUSHAD instruction *)
```

```

Temp ← (SP);
Push(AX);
Push(CX);
Push(DX);
Push(BX);
Push(Temp);
Push(BP);
Push(SI);
Push(DI);

```

```
FI;
```

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If the starting or ending stack address is outside the stack segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while the current privilege level is 3 and alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If the ESP or SP register contains 7, 9, 11, 13, or 15. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the ESP or SP register contains 7, 9, 11, 13, or 15. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#UD If in 64-bit mode.

PUSHF/PUSHFD—Push EFLAGS Register onto the Stack

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|--------|-------------|-------------|-----------------|-------------------------------|
| 9C | PUSHF | Valid | Valid | Push lower 16 bits of EFLAGS. |
| 9C | PUSHFD | N.E. | Valid | Push EFLAGS. |
| 9C | PUSHFQ | Valid | N.E. | Push RFLAGS. |

Description

Decrements the stack pointer by 4 (if the current operand-size attribute is 32) and pushes the entire contents of the EFLAGS register onto the stack, or decrements the stack pointer by 2 (if the operand-size attribute is 16) and pushes the lower 16 bits of the EFLAGS register (that is, the FLAGS register) onto the stack. These instructions reverse the operation of the POPF/POPFQ instructions.

When copying the entire EFLAGS register to the stack, the VM and RF flags (bits 16 and 17) are not copied; instead, the values for these flags are cleared in the EFLAGS image stored on the stack. See Chapter 3 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for more information about the EFLAGS register.

The PUSHF (push flags) and PUSHFD (push flags double) mnemonics reference the same opcode. The PUSHF instruction is intended for use when the operand-size attribute is 16 and the PUSHFD instruction for when the operand-size attribute is 32. Some assemblers may force the operand size to 16 when PUSHF is used and to 32 when PUSHFD is used. Others may treat these mnemonics as synonyms (PUSHF/PUSHFD) and use the current setting of the operand-size attribute to determine the size of values to be pushed from the stack, regardless of the mnemonic used.

In 64-bit mode, the instruction's default operation is to decrement the stack pointer (RSP) by 8 and pushes RFLAGS on the stack. 16-bit operation is supported using the operand size override prefix 66H. 32-bit operand size cannot be encoded in this mode. When copying RFLAGS to the stack, the VM and RF flags (bits 16 and 17) are not copied; instead, values for these flags are cleared in the RFLAGS image stored on the stack.

When in virtual-8086 mode and the I/O privilege level (IOPL) is less than 3, the PUSHF/PUSHFD instruction causes a general protection exception (#GP).

In the real-address mode, if the ESP or SP register is 1 when PUSHF/PUSHFD instruction executes: an #SS exception is generated but not delivered (the stack error reported prevents #SS delivery). Next, the processor generates a #DF exception and enters a shutdown state as described in the #DF discussion in Chapter 5 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A*.

Operation

IF (PE = 0) or (PE = 1 and ((VM = 0) or (VM = 1 and IOPL = 3)))

(* Real-Address Mode, Protected mode, or Virtual-8086 mode with IOPL equal to 3 *)

THEN

IF OperandSize = 32

THEN

push (EFLAGS AND 00FCFFFFH);

(* VM and RF EFLAG bits are cleared in image stored on the stack *)

ELSE

push (EFLAGS); (* Lower 16 bits only *)

FI;

ELSE IF 64-bit MODE (* In 64-bit Mode *)

IF OperandSize = 64

THEN

push (RFLAGS AND 00000000_00FCFFFFH);

(* VM and RF RFLAG bits are cleared in image stored on the stack; *)

ELSE

push (EFLAGS); (* Lower 16 bits only *)

FI;

ELSE (* In Virtual-8086 Mode with IOPL less than 3 *)

#GP(0); (* Trap to virtual-8086 monitor *)

FI;

Flags Affected

None.

Protected Mode Exceptions

| | |
|------------------|--|
| #SS(0) | If the new value of the ESP register is outside the stack segment boundary. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while the current privilege level is 3 and alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|-----------------------------|
| #UD | If the LOCK prefix is used. |
|-----|-----------------------------|

Virtual-8086 Mode Exceptions

| | |
|--------|--|
| #GP(0) | If the I/O privilege level is less than 3. |
|--------|--|

| | |
|-----------------|---|
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If the stack address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory reference is made while the current privilege level is 3 and alignment checking is enabled. |
| #UD | If the LOCK prefix is used. |

PXOR—Logical Exclusive OR

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|-------------------------------------|-------------|------------------|---|
| 0F EF /r | PXOR <i>mm</i> , <i>mm/m64</i> | Valid | Valid | Bitwise XOR of <i>mm/m64</i> and <i>mm</i> . |
| 66 0F EF /r | PXOR <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Bitwise XOR of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical exclusive-OR (XOR) operation on the source operand (second operand) and the destination operand (first operand) and stores the result in the destination operand. The source operand can be an MMX technology register or a 64-bit memory location or it can be an XMM register or a 128-bit memory location. The destination operand can be an MMX technology register or an XMM register. Each bit of the result is 1 if the corresponding bits of the two operands are different; each bit is 0 if the corresponding bits of the operands are the same.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST ← DEST XOR SRC;

Intel C/C++ Compiler Intrinsic Equivalent

PXOR __m64 __mm_xor_si64 (__m64 m1, __m64 m2)

PXOR __m128i __mm_xor_si128 (__m128i a, __m128i b)

Flags Affected

None.

Numeric Exceptions

None.

Protected Mode Exceptions

#GP(0)

If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.

(128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|---|
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | (128-bit operations only) If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside of the effective address space from 0 to FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. Execution of 128-bit instructions on a non-SSE2 capable processor (one that is MMX technology capable) will result in the instruction operating on the mm registers, not #UD. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. (128-bit operations only) If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #UD | If CR0.EM[bit 2] = 1. (128-bit operations only) If CR4.OSFXSR[bit 9] = 0. (128-bit operations only) If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #NM | If CR0.TS[bit 3] = 1. |
| #MF | (64-bit operations only) If there is a pending x87 FPU exception. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | (64-bit operations only) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

RCL/RCR/ROL/ROR—Rotate

| Opcode** | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------------------------|-----------------------------------|-------------|-----------------|--|
| D0 /2 | RCL <i>r/m8</i> , 1 | Valid | Valid | Rotate 9 bits (CF, <i>r/m8</i>) left once. |
| REX + D0 /2 | RCL <i>r/m8*</i> , 1 | Valid | N.E. | Rotate 9 bits (CF, <i>r/m8</i>) left once. |
| D2 /2 | RCL <i>r/m8</i> , CL | Valid | Valid | Rotate 9 bits (CF, <i>r/m8</i>) left CL times. |
| REX + D2 /2 | RCL <i>r/m8*</i> , CL | Valid | N.E. | Rotate 9 bits (CF, <i>r/m8</i>) left CL times. |
| C0 /2 <i>ib</i> | RCL <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Rotate 9 bits (CF, <i>r/m8</i>) left <i>imm8</i> times. |
| REX + C0 /2 <i>ib</i> | RCL <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | Rotate 9 bits (CF, <i>r/m8</i>) left <i>imm8</i> times. |
| D1 /2 | RCL <i>r/m16</i> , 1 | Valid | Valid | Rotate 17 bits (CF, <i>r/m16</i>) left once. |
| D3 /2 | RCL <i>r/m16</i> , CL | Valid | Valid | Rotate 17 bits (CF, <i>r/m16</i>) left CL times. |
| C1 /2 <i>ib</i> | RCL <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Rotate 17 bits (CF, <i>r/m16</i>) left <i>imm8</i> times. |
| D1 /2 | RCL <i>r/m32</i> , 1 | Valid | Valid | Rotate 33 bits (CF, <i>r/m32</i>) left once. |
| REX.W + D1 /2 | RCL <i>r/m64</i> , 1 | Valid | N.E. | Rotate 65 bits (CF, <i>r/m64</i>) left once. Uses a 6 bit count. |
| D3 /2 | RCL <i>r/m32</i> , CL | Valid | Valid | Rotate 33 bits (CF, <i>r/m32</i>) left CL times. |
| REX.W + D3 /2 | RCL <i>r/m64</i> , CL | Valid | N.E. | Rotate 65 bits (CF, <i>r/m64</i>) left CL times. Uses a 6 bit count. |
| C1 /2 <i>ib</i> | RCL <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Rotate 33 bits (CF, <i>r/m32</i>) left <i>imm8</i> times. |
| REX.W + C1 /2 <i>ib</i> | RCL <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Rotate 65 bits (CF, <i>r/m64</i>) left <i>imm8</i> times. Uses a 6 bit count. |
| D0 /3 | RCR <i>r/m8</i> , 1 | Valid | Valid | Rotate 9 bits (CF, <i>r/m8</i>) right once. |
| REX + D0 /3 | RCR <i>r/m8*</i> , 1 | Valid | N.E. | Rotate 9 bits (CF, <i>r/m8</i>) right once. |
| D2 /3 | RCR <i>r/m8</i> , CL | Valid | Valid | Rotate 9 bits (CF, <i>r/m8</i>) right CL times. |
| REX + D2 /3 | RCR <i>r/m8*</i> , CL | Valid | N.E. | Rotate 9 bits (CF, <i>r/m8</i>) right CL times. |

| Opcode** | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------------------|-----------------------------------|-------------|------------------|---|
| C0 /3 <i>ib</i> | RCR <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Rotate 9 bits (CF, <i>r/m8</i>) right <i>imm8</i> times. |
| REX + C0 /3 <i>ib</i> | RCR <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | Rotate 9 bits (CF, <i>r/m8</i>) right <i>imm8</i> times. |
| D1 /3 | RCR <i>r/m16</i> , 1 | Valid | Valid | Rotate 17 bits (CF, <i>r/m16</i>) right once. |
| D3 /3 | RCR <i>r/m16</i> , CL | Valid | Valid | Rotate 17 bits (CF, <i>r/m16</i>) right CL times. |
| C1 /3 <i>ib</i> | RCR <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Rotate 17 bits (CF, <i>r/m16</i>) right <i>imm8</i> times. |
| D1 /3 | RCR <i>r/m32</i> , 1 | Valid | Valid | Rotate 33 bits (CF, <i>r/m32</i>) right once. Uses a 6 bit count. |
| REX.W + D1 /3 | RCR <i>r/m64</i> , 1 | Valid | N.E. | Rotate 65 bits (CF, <i>r/m64</i>) right once. Uses a 6 bit count. |
| D3 /3 | RCR <i>r/m32</i> , CL | Valid | Valid | Rotate 33 bits (CF, <i>r/m32</i>) right CL times. |
| REX.W + D3 /3 | RCR <i>r/m64</i> , CL | Valid | N.E. | Rotate 65 bits (CF, <i>r/m64</i>) right CL times. Uses a 6 bit count. |
| C1 /3 <i>ib</i> | RCR <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Rotate 33 bits (CF, <i>r/m32</i>) right <i>imm8</i> times. |
| REX.W + C1 /3 <i>ib</i> | RCR <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Rotate 65 bits (CF, <i>r/m64</i>) right <i>imm8</i> times. Uses a 6 bit count. |
| D0 /0 | ROL <i>r/m8</i> , 1 | Valid | Valid | Rotate 8 bits <i>r/m8</i> left once. |
| REX + D0 /0 | ROL <i>r/m8*</i> , 1 | Valid | N.E. | Rotate 8 bits <i>r/m8</i> left once |
| D2 /0 | ROL <i>r/m8</i> , CL | Valid | Valid | Rotate 8 bits <i>r/m8</i> left CL times. |
| REX + D2 /0 | ROL <i>r/m8*</i> , CL | Valid | N.E. | Rotate 8 bits <i>r/m8</i> left CL times. |
| C0 /0 <i>ib</i> | ROL <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Rotate 8 bits <i>r/m8</i> left <i>imm8</i> times. |
| REX + C0 /0 <i>ib</i> | ROL <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | Rotate 8 bits <i>r/m8</i> left <i>imm8</i> times. |
| D1 /0 | ROL <i>r/m16</i> , 1 | Valid | Valid | Rotate 16 bits <i>r/m16</i> left once. |
| D3 /0 | ROL <i>r/m16</i> , CL | Valid | Valid | Rotate 16 bits <i>r/m16</i> left CL times. |
| C1 /0 <i>ib</i> | ROL <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Rotate 16 bits <i>r/m16</i> left <i>imm8</i> times. |
| D1 /0 | ROL <i>r/m32</i> , 1 | Valid | Valid | Rotate 32 bits <i>r/m32</i> left once. |

| Opcode** | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------------------------|-----------------------------------|-------------|-----------------|--|
| REX.W + D1 /0 | ROL <i>r/m64</i> , 1 | Valid | N.E. | Rotate 64 bits <i>r/m64</i> left once. Uses a 6 bit count. |
| D3 /0 | ROL <i>r/m32</i> , CL | Valid | Valid | Rotate 32 bits <i>r/m32</i> left CL times. |
| REX.W + D3 /0 | ROL <i>r/m64</i> , CL | Valid | N.E. | Rotate 64 bits <i>r/m64</i> left CL times. Uses a 6 bit count. |
| C1 /0 <i>ib</i> | ROL <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Rotate 32 bits <i>r/m32</i> left <i>imm8</i> times. |
| C1 /0 <i>ib</i> | ROL <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Rotate 64 bits <i>r/m64</i> left <i>imm8</i> times. Uses a 6 bit count. |
| D0 /1 | ROR <i>r/m8</i> , 1 | Valid | Valid | Rotate 8 bits <i>r/m8</i> right once. |
| REX + D0 /1 | ROR <i>r/m8*</i> , 1 | Valid | N.E. | Rotate 8 bits <i>r/m8</i> right once. |
| D2 /1 | ROR <i>r/m8</i> , CL | Valid | Valid | Rotate 8 bits <i>r/m8</i> right CL times. |
| REX + D2 /1 | ROR <i>r/m8*</i> , CL | Valid | N.E. | Rotate 8 bits <i>r/m8</i> right CL times. |
| C0 /1 <i>ib</i> | ROR <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Rotate 8 bits <i>r/m16</i> right <i>imm8</i> times. |
| REX + C0 /1 <i>ib</i> | ROR <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | Rotate 8 bits <i>r/m16</i> right <i>imm8</i> times. |
| D1 /1 | ROR <i>r/m16</i> , 1 | Valid | Valid | Rotate 16 bits <i>r/m16</i> right once. |
| D3 /1 | ROR <i>r/m16</i> , CL | Valid | Valid | Rotate 16 bits <i>r/m16</i> right CL times. |
| C1 /1 <i>ib</i> | ROR <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Rotate 16 bits <i>r/m16</i> right <i>imm8</i> times. |
| D1 /1 | ROR <i>r/m32</i> , 1 | Valid | Valid | Rotate 32 bits <i>r/m32</i> right once. |
| REX.W + D1 /1 | ROR <i>r/m64</i> , 1 | Valid | N.E. | Rotate 64 bits <i>r/m64</i> right once. Uses a 6 bit count. |
| D3 /1 | ROR <i>r/m32</i> , CL | Valid | Valid | Rotate 32 bits <i>r/m32</i> right CL times. |
| REX.W + D3 /1 | ROR <i>r/m64</i> , CL | Valid | N.E. | Rotate 64 bits <i>r/m64</i> right CL times. Uses a 6 bit count. |
| C1 /1 <i>ib</i> | ROR <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Rotate 32 bits <i>r/m32</i> right <i>imm8</i> times. |
| REX.W + C1 /1 <i>ib</i> | ROR <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Rotate 64 bits <i>r/m64</i> right <i>imm8</i> times. Uses a 6 bit count. |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

** See IA-32 Architecture Compatibility section below.

Description

Shifts (rotates) the bits of the first operand (destination operand) the number of bit positions specified in the second operand (count operand) and stores the result in the destination operand. The destination operand can be a register or a memory location; the count operand is an unsigned integer that can be an immediate or a value in the CL register. In legacy and compatibility mode, the processor restricts the count to a number between 0 and 31 by masking all the bits in the count operand except the 5 least-significant bits.

The rotate left (ROL) and rotate through carry left (RCL) instructions shift all the bits toward more-significant bit positions, except for the most-significant bit, which is rotated to the least-significant bit location. The rotate right (ROR) and rotate through carry right (RCR) instructions shift all the bits toward less significant bit positions, except for the least-significant bit, which is rotated to the most-significant bit location.

The RCL and RCR instructions include the CF flag in the rotation. The RCL instruction shifts the CF flag into the least-significant bit and shifts the most-significant bit into the CF flag. The RCR instruction shifts the CF flag into the most-significant bit and shifts the least-significant bit into the CF flag. For the ROL and ROR instructions, the original value of the CF flag is not a part of the result, but the CF flag receives a copy of the bit that was shifted from one end to the other.

The OF flag is defined only for the 1-bit rotates; it is undefined in all other cases (except that a zero-bit rotate does nothing, that is affects no flags). For left rotates, the OF flag is set to the exclusive OR of the CF bit (after the rotate) and the most-significant bit of the result. For right rotates, the OF flag is set to the exclusive OR of the two most-significant bits of the result.

In 64-bit mode, using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Use of REX.W promotes the first operand to 64 bits and causes the count operand to become a 6-bit counter.

IA-32 Architecture Compatibility

The 8086 does not mask the rotation count. However, all other IA-32 processors (starting with the Intel 286 processor) do mask the rotation count to 5 bits, resulting in a maximum count of 31. This masking is done in all operating modes (including the virtual-8086 mode) to reduce the maximum execution time of the instructions.

Operation

(* RCL and RCR instructions *)

SIZE ← OperandSize;

CASE (determine count) OF

SIZE ← 8: tempCOUNT ← (COUNT AND 1FH) MOD 9;

SIZE ← 16: tempCOUNT ← (COUNT AND 1FH) MOD 17;

SIZE ← 32: tempCOUNT ← COUNT AND 1FH;

```

    SIZE ← 64:   tempCOUNT ← COUNT AND 3FH;
ESAC;

```

```
(* RCL instruction operation *)
```

```

WHILE (tempCOUNT ≠ 0)
    DO
        tempCF ← MSB(DEST);
        DEST ← (DEST * 2) + CF;
        CF ← tempCF;
        tempCOUNT ← tempCOUNT - 1;
    OD;
ELIHW;
IF COUNT = 1
    THEN OF ← MSB(DEST) XOR CF;
    ELSE OF is undefined;
FI;

```

```
(* RCR instruction operation *)
```

```

IF COUNT = 1
    THEN OF ← MSB(DEST) XOR CF;
    ELSE OF is undefined;
FI;
WHILE (tempCOUNT ≠ 0)
    DO
        tempCF ← LSB(SRC);
        DEST ← (DEST / 2) + (CF * 2SIZE);
        CF ← tempCF;
        tempCOUNT ← tempCOUNT - 1;
    OD;

```

```
(* ROL and ROR instructions *)
```

```

SIZE ← OperandSize;
CASE (determine count) OF
    SIZE ← 8:   tempCOUNT ← (COUNT AND 1FH) MOD 8; (* Mask count before MOD *)
    SIZE ← 16:  tempCOUNT ← (COUNT AND 1FH) MOD 16;
    SIZE ← 32:  tempCOUNT ← (COUNT AND 1FH) MOD 32;
    SIZE ← 64:  tempCOUNT ← (COUNT AND 1FH) MOD 64;
ESAC;

```

```
(* ROL instruction operation *)
```

```

IF (tempCOUNT > 0) (* Prevents updates to CF *)
    WHILE (tempCOUNT ≠ 0)
        DO

```

```

        tempCF ← MSB(DEST);
        DEST ← (DEST * 2) + tempCF;
        tempCOUNT ← tempCOUNT - 1;
    OD;
    ELIHW;
    CF ← LSB(DEST);
    IF COUNT = 1
        THEN OF ← MSB(DEST) XOR CF;
        ELSE OF is undefined;
    FI;
FI;

(* ROR instruction operation *)
IF tempCOUNT > 0 (* Prevent updates to CF *)
    WHILE (tempCOUNT ≠ 0)
        DO
            tempCF ← LSB(SRC);
            DEST ← (DEST / 2) + (tempCF * 2SIZEE);
            tempCOUNT ← tempCOUNT - 1;
        OD;
    ELIHW;
    CF ← MSB(DEST);
    IF COUNT = 1
        THEN OF ← MSB(DEST) XOR MSB - 1(DEST);
        ELSE OF is undefined;
    FI;
FI;

```

Flags Affected

The CF flag contains the value of the bit shifted into it. The OF flag is affected only for single-bit rotates (see “Description” above); it is undefined for multi-bit rotates. The SF, ZF, AF, and PF flags are not affected.

Protected Mode Exceptions

- | | |
|-----------------|---|
| #GP(0) | If the source operand is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |

| | |
|--------|--|
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the source operand is located in a nonwritable segment. If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

RCPPS—Compute Reciprocals of Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|---|-------------|-----------------|---|
| OF 53 /r | RCPPS <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Computes the approximate reciprocals of the packed single-precision floating-point values in <i>xmm2/m128</i> and stores the results in <i>xmm1</i> . |

Description

Performs a SIMD computation of the approximate reciprocals of the four packed single-precision floating-point values in the source operand (second operand) stores the packed single-precision floating-point results in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. See Figure 10-5 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD single-precision floating-point operation.

The relative error for this approximation is:

$$|\text{Relative Error}| \leq 1.5 * 2^{-12}$$

The RCPPS instruction is not affected by the rounding control bits in the MXCSR register. When a source value is a 0.0, an ∞ of the sign of the source value is returned. A denormal source value is treated as a 0.0 (of the same sign). Tiny results are always flushed to 0.0, with the sign of the operand. (Input values greater than or equal to $|1.1111111110100000000000B * 2^{125}|$ are guaranteed to not produce tiny results; input values less than or equal to $|1.0000000000110000000001B * 2^{126}|$ are guaranteed to produce tiny results, which are in turn flushed to 0.0; and input values in between this range may or may not produce tiny results, depending on the implementation.) When a source value is an SNaN or QNaN, the SNaN is converted to a QNaN or the source QNaN is returned.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[31:0] ← APPROXIMATE(1.0/(SRC[31:0]));
DEST[63:32] ← APPROXIMATE(1.0/(SRC[63:32]));
DEST[95:64] ← APPROXIMATE(1.0/(SRC[95:64]));
DEST[127:96] ← APPROXIMATE(1.0/(SRC[127:96]));
```

Intel C/C++ Compiler Intrinsic Equivalent

```
RCCPS    __m128 _mm_rcp_ps(__m128 a)
```

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |

| | |
|------------------|--|
| | If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

RCPSS—Compute Reciprocal of Scalar Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------------|--|-------------|------------------|---|
| F3 OF 53 /r | RCPSS <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Computes the approximate reciprocal of the scalar single-precision floating-point value in <i>xmm2/m32</i> and stores the result in <i>xmm1</i> . |

Description

Computes of an approximate reciprocal of the low single-precision floating-point value in the source operand (second operand) and stores the single-precision floating-point result in the destination operand. The source operand can be an XMM register or a 32-bit memory location. The destination operand is an XMM register. The three high-order doublewords of the destination operand remain unchanged. See Figure 10-6 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a scalar single-precision floating-point operation.

The relative error for this approximation is:

$$|\text{Relative Error}| \leq 1.5 * 2^{-12}$$

The RCPSS instruction is not affected by the rounding control bits in the MXCSR register. When a source value is a 0.0, an ∞ of the sign of the source value is returned. A denormal source value is treated as a 0.0 (of the same sign). Tiny results are always flushed to 0.0, with the sign of the operand. (Input values greater than or equal to $|1.1111111110100000000000B * 2^{125}|$ are guaranteed to not produce tiny results; input values less than or equal to $|1.00000000000110000000001B * 2^{126}|$ are guaranteed to produce tiny results, which are in turn flushed to 0.0; and input values in between this range may or may not produce tiny results, depending on the implementation.) When a source value is an SNaN or QNaN, the SNaN is converted to a QNaN or the source QNaN is returned.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[31:0] ← APPROX (1.0/(SRC[31:0]));
(* DEST[127:32] unchanged *)

Intel C/C++ Compiler Intrinsic Equivalent

RCPSS __m128 _mm_rcp_ss(__m128 a)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---------------------------------|
| #PF(fault-code) | For a page fault. |
| #AC(0) | For unaligned memory reference. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |

| | |
|--------|--|
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

RDMSR—Read from Model Specific Register

| Opcode* | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|---------|-------------|-------------|------------------|---|
| 0F 32 | RDMSR | Valid | Valid | Read MSR specified by ECX into EDX:EAX. |

NOTES:

* See IA-32 Architecture Compatibility section below.

Description

Reads the contents of a 64-bit model specific register (MSR) specified in the ECX register into registers EDX:EAX. (On processors that support the Intel 64 architecture, the high-order 32 bits of RCX are ignored.) The EDX register is loaded with the high-order 32 bits of the MSR and the EAX register is loaded with the low-order 32 bits. (On processors that support the Intel 64 architecture, the high-order 32 bits of each of RAX and RDX are cleared.) If fewer than 64 bits are implemented in the MSR being read, the values returned to EDX:EAX in unimplemented bit locations are undefined.

This instruction must be executed at privilege level 0 or in real-address mode; otherwise, a general protection exception #GP(0) will be generated. Specifying a reserved or unimplemented MSR address in ECX will also cause a general protection exception.

The MSRs control functions for testability, execution tracing, performance-monitoring, and machine check errors. Appendix B, “Model-Specific Registers (MSRs),” in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*, lists all the MSRs that can be read with this instruction and their addresses. Note that each processor family has its own set of MSRs.

The CPUID instruction should be used to determine whether MSRs are supported (CPUID.01H:EDX[5] = 1) before using this instruction.

IA-32 Architecture Compatibility

The MSRs and the ability to read them with the RDMSR instruction were introduced into the IA-32 Architecture with the Pentium processor. Execution of this instruction by an IA-32 processor earlier than the Pentium processor results in an invalid opcode exception #UD.

See “Changes to Instruction Behavior in VMX Non-Root Operation” in Chapter 21 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*, for more information about the behavior of this instruction in VMX non-root operation.

Operation

EDX:EAX ← MSR[ECX];

Flags Affected

None.

Protected Mode Exceptions

| | |
|--------|--|
| #GP(0) | If the current privilege level is not 0. If the value in ECX specifies a reserved or unimplemented MSR address. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If the value in ECX specifies a reserved or unimplemented MSR address. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|--------|---|
| #GP(0) | The RDMSR instruction is not recognized in virtual-8086 mode. |
|--------|---|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|---|
| #GP(0) | If the current privilege level is not 0. If the value in ECX or RCX specifies a reserved or unimplemented MSR address. |
| #UD | If the LOCK prefix is used. |

RDPMC—Read Performance-Monitoring Counters

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|--|
| 0F 33 | RDPMC | Valid | Valid | Read performance-monitoring counter specified by ECX into EDX:EAX. |

Description

Loads the performance-monitoring counter specified in the ECX register into registers EDX:EAX. (On processors that support the Intel 64 architecture, the high-order 32 bits of RCX are ignored.) The EDX register is loaded with the high-order 8 bits of the counter and the EAX register is loaded with the low-order 32 bits. (On processors that support the Intel 64 architecture, the high-order 32 bits of each of RAX and RDX are cleared.) See below for the treatment of the EDX register for “fast” reads.

The ECX register selects one of two type of performance counters, specifies the index relative to the base of each counter type, and selects “fast” read mode if supported. The two counter types are :

- General-purpose or special-purpose performance counters: The number of general-purpose counters is model specific if the processor does not support architectural performance monitoring, see Chapter 18 of *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*. Special-purpose counters are available only in selected processor members, see Section 18.19, 18.20 of *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*. This counter type is selected if ECX[30] is clear.
- Fixed-function performance counter. The number fixed-function performance counters is enumerated by CPUID 0AH leaf. See Chapter 18 of *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*. This counter type is selected if ECX[30] is set.

ECX[29:0] specifies the index. The width of general-purpose performance counters are 40-bits for processors that do not support architectural performance monitoring counters. The width of special-purpose performance counters are implementation specific. The width of fixed-function performance counters and general-purpose performance counters on processor supporting architectural performance monitoring are reported by CPUID 0AH leaf.

Table 4-2 lists valid indices of the general-purpose and special-purpose performance counters according to the derived displayed_family/displayed_model values of CPUID encoding for each processor family.

Table 4-2. Valid General and Special Purpose Performance Counter Index Range for RDPMC

| Processor Family | Displayed_Family_Displayed_Model/ Other Signatures | Valid PMC Index Range | General-purpose Counters |
|---|--|-----------------------|--------------------------|
| P6 | 06H_01H, 06H_03H, 06H_05H, 06H_06H, 06H_07H, 06H_08H, 06H_0AH, 06H_0BH | 0, 1 | 0, 1 |
| Pentium® 4, Intel® Xeon processors | 0FH_00H, 0FH_01H, 0FH_02H | ≥ 0 and ≤ 17 | ≥ 0 and ≤ 17 |
| Pentium 4, Intel Xeon processors | (0FH_03H, 0FH_04H, 0FH_06H) and (L3 is absent) | ≥ 0 and ≤ 17 | ≥ 0 and ≤ 17 |
| Pentium M processors | 06H_09H, 06H_0DH | 0, 1 | 0, 1 |
| 64-bit Intel Xeon processors with L3 | 0FH_03H, 0FH_04H) and (L3 is present) | ≥ 0 and ≤ 25 | ≥ 0 and ≤ 17 |
| Intel® Core™ Solo and Intel® Core™ Duo processors, Dual-core Intel® Xeon® processor LV | 06H_0EH | 0, 1 | 0, 1 |
| Intel® Core™2 Duo processor, Intel Xeon processor 3000, 5100, 5300, 7300 Series - general-purpose PMC | 06H_0FH | 0, 1 | 0, 1 |
| Intel Xeon processors 7100 series with L3 | (0FH_06H) and (L3 is present) | ≥ 0 and ≤ 25 | ≥ 0 and ≤ 17 |
| Intel® Core™2 Duo processor family, Intel Xeon processor family - general-purpose PMC | 06H_17H | 0, 1 | 0, 1 |
| Intel® Atom™ processor family | 06H_0CH | 0, 1 | 0, 1 |

The Pentium 4 and Intel Xeon processors also support “fast” (32-bit) and “slow” (40-bit) reads on the first 18 performance counters. Selected this option using ECX[31]. If bit 31 is set, RDPMC reads only the low 32 bits of the selected performance counter. If bit 31 is clear, all 40 bits are read. A 32-bit result is returned in EAX and EDX is set to 0. A 32-bit read executes faster on Pentium 4 processors and Intel Xeon processors than a full 40-bit read.

On 64-bit Intel Xeon processors with L3, performance counters with indices 18-25 are 32-bit counters. EDX is cleared after executing RDPMC for these counters. On Intel Xeon processor 7100 series with L3, performance counters with indices 18-25 are also 32-bit counters.

In Intel Core 2 processor family, Intel Xeon processor 3000, 5100, and 5300 series, the fixed-function performance counters are 40-bits wide; they can be accessed by RDPMC with ECX between from 4000_0000H and 4000_0002H.

When in protected or virtual 8086 mode, the performance-monitoring counters enabled (PCE) flag in register CR4 restricts the use of the RDPMC instruction as follows. When the PCE flag is set, the RDPMC instruction can be executed at any privilege level; when the flag is clear, the instruction can only be executed at privilege level 0. (When in real-address mode, the RDPMC instruction is always enabled.)

The performance-monitoring counters can also be read with the RDMSR instruction, when executing at privilege level 0.

The performance-monitoring counters are event counters that can be programmed to count events such as the number of instructions decoded, number of interrupts received, or number of cache loads. Appendix A, "Performance Monitoring Events," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B*, lists the events that can be counted for various processors in the Intel 64 and IA-32 architecture families.

The RDPMC instruction is not a serializing instruction; that is, it does not imply that all the events caused by the preceding instructions have been completed or that events caused by subsequent instructions have not begun. If an exact event count is desired, software must insert a serializing instruction (such as the CPUID instruction) before and/or after the RDPCM instruction.

In the Pentium 4 and Intel Xeon processors, performing back-to-back fast reads are not guaranteed to be monotonic. To guarantee monotonicity on back-to-back reads, a serializing instruction must be placed between the two RDPMC instructions.

The RDPMC instruction can execute in 16-bit addressing mode or virtual-8086 mode; however, the full contents of the ECX register are used to select the counter, and the event count is stored in the full EAX and EDX registers. The RDPMC instruction was introduced into the IA-32 Architecture in the Pentium Pro processor and the Pentium processor with MMX technology. The earlier Pentium processors have performance-monitoring counters, but they must be read with the RDMSR instruction.

Operation

(* Intel Core 2 Duo processor family and Intel Xeon processor 3000, 5100, 5300 series*)

Most significant counter bit (MSCB) = 39

```
IF (ECX = 0 or 1) and ((CR4.PCE = 1) or (CPL = 0) or (CR0.PE = 0))
  THEN IF (ECX[30] = 1 and ECX[29:0] in valid fixed-counter range)
    EAX ← IA32_FIXED_CTR(ECX)[30:0];
    EDX ← IA32_FIXED_CTR(ECX)[MSCB:32];
  ELSE IF (ECX[30] = 0 and ECX[29:0] in valid general-purpose counter range)
    EAX ← PMC(ECX[30:0])[31:0];
    EDX ← PMC(ECX[30:0])[MSCB:32];
```



```

ELSE (* ECX is not valid or CR4.PCE is 0 and CPL is 1, 2, or 3 and CR0.PE is 1 *)
    #GP(0);
FI;

(* P6 family processors and Pentium processor with MMX technology *)
IF (ECX = 0 or 1) and ((CR4.PCE = 1) or (CPL = 0) or (CR0.PE = 0))
    THEN
        EAX ← PMC(ECX)[31:0];
        EDX ← PMC(ECX)[39:32];
    ELSE (* ECX is not 0 or 1 or CR4.PCE is 0 and CPL is 1, 2, or 3 and CR0.PE is 1 *)
        #GP(0);
FI;

(* Processors with CPUID family 15 *)
IF ((CR4.PCE = 1) or (CPL = 0) or (CR0.PE = 0))
    THEN IF (ECX[30:0] = 0:17)
        THEN IF ECX[31] = 0
            THEN
                EAX ← PMC(ECX[30:0])[31:0]; (* 40-bit read *)
                EDX ← PMC(ECX[30:0])[39:32];
            ELSE (* ECX[31] = 1*)
                THEN
                    EAX ← PMC(ECX[30:0])[31:0]; (* 32-bit read *)
                    EDX ← 0;
            FI;
        ELSE IF (*64-bit Intel Xeon processor with L3 *)
            THEN IF (ECX[30:0] = 18:25 )
                EAX ← PMC(ECX[30:0])[31:0]; (* 32-bit read *)
                EDX ← 0;
            FI;
        ELSE IF (*Intel Xeon processor 7100 series with L3 *)
            THEN IF (ECX[30:0] = 18:25 )
                EAX ← PMC(ECX[30:0])[31:0]; (* 32-bit read *)
                EDX ← 0;
            FI;
        ELSE (* Invalid PMC index in ECX[30:0], see Table 4-5. *)
            GP(0);
        FI;
    ELSE (* CR4.PCE = 0 and (CPL = 1, 2, or 3) and CR0.PE = 1 *)
        #GP(0);
    FI;
FI;

```

Flags Affected

None.

Protected Mode Exceptions

- #GP(0) If the current privilege level is not 0 and the PCE flag in the CR4 register is clear.
If an invalid performance counter index is specified (see Table 4-2).
(Pentium 4 and Intel Xeon processors) If the value in ECX[30:0] is not within the valid range.
- #UD If the LOCK prefix is used.

Real-Address Mode Exceptions

- #GP If an invalid performance counter index is specified (see Table 4-2).
(Pentium 4 and Intel Xeon processors) If the value in ECX[30:0] is not within the valid range.
- #UD If the LOCK prefix is used.

Virtual-8086 Mode Exceptions

- #GP(0) If the PCE flag in the CR4 register is clear.
If an invalid performance counter index is specified (see Table 4-2).
(Pentium 4 and Intel Xeon processors) If the value in ECX[30:0] is not within the valid range.
- #UD If the LOCK prefix is used.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

- #GP(0) If the current privilege level is not 0 and the PCE flag in the CR4 register is clear.
If an invalid performance counter index is specified in ECX[30:0] (see Table 4-2).
- #UD If the LOCK prefix is used.

RDTSC—Read Time-Stamp Counter

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|---------------------------------------|
| OF 31 | RDTSC | Valid | Valid | Read time-stamp counter into EDX:EAX. |

Description

Loads the current value of the processor's time-stamp counter (a 64-bit MSR) into the EDX:EAX registers. The EDX register is loaded with the high-order 32 bits of the MSR and the EAX register is loaded with the low-order 32 bits. (On processors that support the Intel 64 architecture, the high-order 32 bits of each of RAX and RDX are cleared.)

The processor monotonically increments the time-stamp counter MSR every clock cycle and resets it to 0 whenever the processor is reset. See "Time Stamp Counter" in Chapter 18 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B*, for specific details of the time stamp counter behavior.

When in protected or virtual 8086 mode, the time stamp disable (TSD) flag in register CR4 restricts the use of the RDTSC instruction as follows. When the TSD flag is clear, the RDTSC instruction can be executed at any privilege level; when the flag is set, the instruction can only be executed at privilege level 0. (When in real-address mode, the RDTSC instruction is always enabled.)

The time-stamp counter can also be read with the RDMSR instruction, when executing at privilege level 0.

The RDTSC instruction is not a serializing instruction. Thus, it does not necessarily wait until all previous instructions have been executed before reading the counter. Similarly, subsequent instructions may begin execution before the read operation is performed.

This instruction was introduced by the Pentium processor.

See "Changes to Instruction Behavior in VMX Non-Root Operation" in Chapter 21 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B*, for more information about the behavior of this instruction in VMX non-root operation.

Operation

```
IF (CR4.TSD = 0) or (CPL = 0) or (CR0.PE = 0)
    THEN EDX:EAX ← TimeStampCounter;
    ELSE (* CR4.TSD = 1 and (CPL = 1, 2, or 3) and CR0.PE = 1 *)
        #GP(0);
FI;
```

Flags Affected

None.

Protected Mode Exceptions

- #GP(0) If the TSD flag in register CR4 is set and the CPL is greater than 0.
- #UD If the LOCK prefix is used.

Real-Address Mode Exceptions

- #UD If the LOCK prefix is used.

Virtual-8086 Mode Exceptions

- #GP(0) If the TSD flag in register CR4 is set.
- #UD If the LOCK prefix is used.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

REP/REPE/REPZ/REPNE/REPNZ—Repeat String Operation Prefix

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|----------------------------------|-------------|------------------|---|
| F3 6C | REP INS <i>m8</i> , DX | Valid | Valid | Input (E)CX bytes from port DX into ES:[(E)DI]. |
| F3 6C | REP INS <i>m8</i> , DX | Valid | N.E. | Input RCX bytes from port DX into [RDI]. |
| F3 6D | REP INS <i>m16</i> , DX | Valid | Valid | Input (E)CX words from port DX into ES:[(E)DI]. |
| F3 6D | REP INS <i>m32</i> , DX | Valid | Valid | Input (E)CX doublewords from port DX into ES:[(E)DI]. |
| F3 6D | REP INS <i>r/m32</i> , DX | Valid | N.E. | Input RCX default size from port DX into [RDI]. |
| F3 A4 | REP MOVS <i>m8</i> , <i>m8</i> | Valid | Valid | Move (E)CX bytes from DS:[(E)SI] to ES:[(E)DI]. |
| F3 REX.W A4 | REP MOVS <i>m8</i> , <i>m8</i> | Valid | N.E. | Move RCX bytes from [RSI] to [RDI]. |
| F3 A5 | REP MOVS <i>m16</i> , <i>m16</i> | Valid | Valid | Move (E)CX words from DS:[(E)SI] to ES:[(E)DI]. |
| F3 A5 | REP MOVS <i>m32</i> , <i>m32</i> | Valid | Valid | Move (E)CX doublewords from DS:[(E)SI] to ES:[(E)DI]. |
| F3 REX.W A5 | REP MOVS <i>m64</i> , <i>m64</i> | Valid | N.E. | Move RCX quadwords from [RSI] to [RDI]. |
| F3 6E | REP OUTS DX, <i>r/m8</i> | Valid | Valid | Output (E)CX bytes from DS:[(E)SI] to port DX. |
| F3 REX.W 6E | REP OUTS DX, <i>r/m8</i> * | Valid | N.E. | Output RCX bytes from [RSI] to port DX. |
| F3 6F | REP OUTS DX, <i>r/m16</i> | Valid | Valid | Output (E)CX words from DS:[(E)SI] to port DX. |
| F3 6F | REP OUTS DX, <i>r/m32</i> | Valid | Valid | Output (E)CX doublewords from DS:[(E)SI] to port DX. |
| F3 REX.W 6F | REP OUTS DX, <i>r/m32</i> | Valid | N.E. | Output RCX default size from [RSI] to port DX. |
| F3 AC | REP LODS AL | Valid | Valid | Load (E)CX bytes from DS:[(E)SI] to AL. |
| F3 REX.W AC | REP LODS AL | Valid | N.E. | Load RCX bytes from [RSI] to AL. |
| F3 AD | REP LODS AX | Valid | Valid | Load (E)CX words from DS:[(E)SI] to AX. |

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---------------------------|-------------|---------------------|--|
| F3 AD | REP LODS EAX | Valid | Valid | Load (E)CX doublewords from DS:[(E)SI] to EAX. |
| F3 REX.W AD | REP LODS RAX | Valid | N.E. | Load RCX quadwords from [RSI] to RAX. |
| F3 AA | REP STOS <i>m8</i> | Valid | Valid | Fill (E)CX bytes at ES:[(E)DI] with AL. |
| F3 REX.W AA | REP STOS <i>m8</i> | Valid | N.E. | Fill RCX bytes at [RDI] with AL. |
| F3 AB | REP STOS <i>m16</i> | Valid | Valid | Fill (E)CX words at ES:[(E)DI] with AX. |
| F3 AB | REP STOS <i>m32</i> | Valid | Valid | Fill (E)CX doublewords at ES:[(E)DI] with EAX. |
| F3 REX.W AB | REP STOS <i>m64</i> | Valid | N.E. | Fill RCX quadwords at [RDI] with RAX. |
| F3 A6 | REPE CMPS <i>m8, m8</i> | Valid | Valid | Find nonmatching bytes in ES:[(E)DI] and DS:[(E)SI]. |
| F3 REX.W A6 | REPE CMPS <i>m8, m8</i> | Valid | N.E. | Find non-matching bytes in [RDI] and [RSI]. |
| F3 A7 | REPE CMPS <i>m16, m16</i> | Valid | Valid | Find nonmatching words in ES:[(E)DI] and DS:[(E)SI]. |
| F3 A7 | REPE CMPS <i>m32, m32</i> | Valid | Valid | Find nonmatching doublewords in ES:[(E)DI] and DS:[(E)SI]. |
| F3 REX.W A7 | REPE CMPS <i>m64, m64</i> | Valid | N.E. | Find non-matching quadwords in [RDI] and [RSI]. |
| F3 AE | REPE SCAS <i>m8</i> | Valid | Valid | Find non-AL byte starting at ES:[(E)DI]. |
| F3 REX.W AE | REPE SCAS <i>m8</i> | Valid | N.E. | Find non-AL byte starting at [RDI]. |
| F3 AF | REPE SCAS <i>m16</i> | Valid | Valid | Find non-AX word starting at ES:[(E)DI]. |
| F3 AF | REPE SCAS <i>m32</i> | Valid | Valid | Find non-EAX doubleword starting at ES:[(E)DI]. |
| F3 REX.W AF | REPE SCAS <i>m64</i> | Valid | N.E. | Find non-RAX quadword starting at [RDI]. |
| F2 A6 | REPNE CMPS <i>m8, m8</i> | Valid | Valid | Find matching bytes in ES:[(E)DI] and DS:[(E)SI]. |
| F2 REX.W A6 | REPNE CMPS <i>m8, m8</i> | Valid | N.E. | Find matching bytes in [RDI] and [RSI]. |

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---------------------------------------|-------------|------------------|---|
| F2 A7 | REPNE CMPS <i>m16</i> , <i>m16</i> | Valid | Valid | Find matching words in ES:[(E)DI] and DS:[(E)SI]. |
| F2 A7 | REPNE CMPS <i>m32</i> , <i>m32</i> | Valid | Valid | Find matching doublewords in ES:[(E)DI] and DS:[(E)SI]. |
| F2 REX.W A7 | REPNE CMPS <i>m64</i> , <i>m64</i> | Valid | N.E. | Find matching doublewords in [RDI] and [RSI]. |
| F2 AE | REPNE SCAS <i>m8</i> | Valid | Valid | Find AL, starting at ES:[(E)DI]. |
| F2 REX.W AE | REPNE SCAS <i>m8</i> | Valid | N.E. | Find AL, starting at [RDI]. |
| F2 AF | REPNE SCAS <i>m16</i> | Valid | Valid | Find AX, starting at ES:[(E)DI]. |
| F2 AF | REPNE SCAS <i>m32</i> | Valid | Valid | Find EAX, starting at ES:[(E)DI]. |
| F2 REX.W AF | REPNE SCAS <i>m64</i> | Valid | N.E. | Find RAX, starting at [RDI]. |

NOTES:

- * In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Repeats a string instruction the number of times specified in the count register or until the indicated condition of the ZF flag is no longer met. The REP (repeat), REPE (repeat while equal), REPNE (repeat while not equal), REPZ (repeat while zero), and REPNZ (repeat while not zero) mnemonics are prefixes that can be added to one of the string instructions. The REP prefix can be added to the INS, OUTS, MOVSB, LODSB, and STOSB instructions, and the REPE, REPNE, REPZ, and REPNZ prefixes can be added to the CMPS and SCAS instructions. (The REPZ and REPNZ prefixes are synonymous forms of the REPE and REPNE prefixes, respectively.) The behavior of the REP prefix is undefined when used with non-string instructions.

The REP prefixes apply only to one string instruction at a time. To repeat a block of instructions, use the LOOP instruction or another looping construct. All of these repeat prefixes cause the associated instruction to be repeated until the count in register is decremented to 0. See Table 4-3.

Table 4-3. Repeat Prefixes

| Repeat Prefix | Termination Condition 1* | Termination Condition 2 |
|---------------|--------------------------|-------------------------|
| REP | RCX or (E)CX = 0 | None |
| REPE/REPZ | RCX or (E)CX = 0 | ZF = 0 |
| REPNE/REPNZ | RCX or (E)CX = 0 | ZF = 1 |

NOTES:

- * Count register is CX, ECX or RCX by default, depending on attributes of the operating modes. In 64-bit mode, if default operation size is 32 bits, the count register becomes RCX when a REX.W prefix is used.

The REPE, REPNE, REPZ, and REPNZ prefixes also check the state of the ZF flag after each iteration and terminate the repeat loop if the ZF flag is not in the specified state. When both termination conditions are tested, the cause of a repeat termination can be determined either by testing the count register with a JECXZ instruction or by testing the ZF flag (with a JZ, JNZ, or JNE instruction).

When the REPE/REPZ and REPNE/REPZ prefixes are used, the ZF flag does not require initialization because both the CMPS and SCAS instructions affect the ZF flag according to the results of the comparisons they make.

A repeating string operation can be suspended by an exception or interrupt. When this happens, the state of the registers is preserved to allow the string operation to be resumed upon a return from the exception or interrupt handler. The source and destination registers point to the next string elements to be operated on, the EIP register points to the string instruction, and the ECX register has the value it held following the last successful iteration of the instruction. This mechanism allows long string operations to proceed without affecting the interrupt response time of the system.

When a fault occurs during the execution of a CMPS or SCAS instruction that is prefixed with REPE or REPNE, the EFLAGS value is restored to the state prior to the execution of the instruction. Since the SCAS and CMPS instructions do not use EFLAGS as an input, the processor can resume the instruction after the page fault handler.

If a debug exception occurs, non-enabled debug breakpoints matched on previous iterations of the REP operation may or may not be reported in the DR6 register.

Use the REP INS and REP OUTS instructions with caution. Not all I/O ports can handle the rate at which these instructions execute. Note that a REP STOS instruction is the fastest way to initialize a large block of memory.

In 64-bit mode, default operation size is 32 bits. The default count register is RCX for REP INS and REP OUTS; it is ECX for other instructions. REX.W does not promote operation to 64-bit for REP INS and REP OUTS. However, using a REX prefix in the form of REX.W does promote operation to 64-bit operands for other

REP/REPNE/REPZ/REPZ instructions. See the summary chart at the beginning of this section for encoding data and limits.

Operation

```

IF AddressSize = 16
  THEN
    Use CX for CountReg;
  ELSE IF AddressSize = 64 and REX.W used
    THEN Use RCX for CountReg; FI;
  ELSE
    Use ECX for CountReg;
FI;
WHILE CountReg ≠ 0
  DO
    Service pending interrupts (if any);
    Execute associated string instruction;
    CountReg ← (CountReg - 1);
    IF CountReg = 0
      THEN exit WHILE loop; FI;
    IF (Repeat prefix is REPZ or REPE) and (ZF = 0)
      or (Repeat prefix is REPZ or REPNE) and (ZF = 1)
      THEN exit WHILE loop; FI;
  OD;

```

Flags Affected

None; however, the CMPS and SCAS instructions do set the status flags in the EFLAGS register.

Exceptions (All Operating Modes)

Exceptions may be generated by an instruction associated with the prefix.

64-Bit Mode Exceptions

#GP(0) If the memory address is in a non-canonical form.

RET—Return from Procedure

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|--------------|------------------|-------------|-----------------|---|
| C3 | RET | Valid | Valid | Near return to calling procedure. |
| CB | RET | Valid | Valid | Far return to calling procedure. |
| C2 <i>iw</i> | RET <i>imm16</i> | Valid | Valid | Near return to calling procedure and pop <i>imm16</i> bytes from stack. |
| CA <i>iw</i> | RET <i>imm16</i> | Valid | Valid | Far return to calling procedure and pop <i>imm16</i> bytes from stack. |

Description

Transfers program control to a return address located on the top of the stack. The address is usually placed on the stack by a CALL instruction, and the return is made to the instruction that follows the CALL instruction.

The optional source operand specifies the number of stack bytes to be released after the return address is popped; the default is none. This operand can be used to release parameters from the stack that were passed to the called procedure and are no longer needed. It must be used when the CALL instruction used to switch to a new procedure uses a call gate with a non-zero word count to access the new procedure. Here, the source operand for the RET instruction must specify the same number of bytes as is specified in the word count field of the call gate.

The RET instruction can be used to execute three different types of returns:

- **Near return** — A return to a calling procedure within the current code segment (the segment currently pointed to by the CS register), sometimes referred to as an intrasegment return.
- **Far return** — A return to a calling procedure located in a different segment than the current code segment, sometimes referred to as an intersegment return.
- **Inter-privilege-level far return** — A far return to a different privilege level than that of the currently executing program or procedure.

The inter-privilege-level return type can only be executed in protected mode. See the section titled “Calling Procedures Using Call and RET” in Chapter 6 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 1*, for detailed information on near, far, and inter-privilege-level returns.

When executing a near return, the processor pops the return instruction pointer (offset) from the top of the stack into the EIP register and begins program execution at the new instruction pointer. The CS register is unchanged.

When executing a far return, the processor pops the return instruction pointer from the top of the stack into the EIP register, then pops the segment selector from the top of the stack into the CS register. The processor then begins program execution in the new code segment at the new instruction pointer.

The mechanics of an inter-privilege-level far return are similar to an intersegment return, except that the processor examines the privilege levels and access rights of the code and stack segments being returned to determine if the control transfer is allowed to be made. The DS, ES, FS, and GS segment registers are cleared by the RET instruction during an inter-privilege-level return if they refer to segments that are not allowed to be accessed at the new privilege level. Since a stack switch also occurs on an inter-privilege level return, the ESP and SS registers are loaded from the stack.

If parameters are passed to the called procedure during an inter-privilege level call, the optional source operand must be used with the RET instruction to release the parameters on the return. Here, the parameters are released both from the called procedure's stack and the calling procedure's stack (that is, the stack being returned to).

In 64-bit mode, the default operation size of this instruction is the stack size, i.e. 64 bits.

Operation

(* Near return *)

IF instruction = Near return

THEN;

IF OperandSize = 32

THEN

IF top 4 bytes of stack not within stack limits

THEN #SS(0); FI;

EIP ← Pop();

ELSE

IF OperandSize = 64

THEN

IF top 8 bytes of stack not within stack limits

THEN #SS(0); FI;

RIP ← Pop();

ELSE (* OperandSize = 16 *)

IF top 2 bytes of stack not within stack limits

THEN #SS(0); FI;

tempEIP ← Pop();

tempEIP ← tempEIP AND 0000FFFFH;

IF tempEIP not within code segment limits

THEN #GP(0); FI;

EIP ← tempEIP;

FI;

FI;

```

IF instruction has immediate operand
  THEN IF StackAddressSize = 32
    THEN
      ESP ← ESP + SRC; (* Release parameters from stack *)
    ELSE
      IF StackAddressSize = 64
        THEN
          RSP ← RSP + SRC; (* Release parameters from stack *)
        ELSE (* StackAddressSize = 16 *)
          SP ← SP + SRC; (* Release parameters from stack *)
      FI;
    FI;
  FI;
FI;

```

(* Real-address mode or virtual-8086 mode *)

```

IF ((PE = 0) or (PE = 1 AND VM = 1)) and instruction = far return
  THEN
    IF OperandSize = 32
      THEN
        IF top 12 bytes of stack not within stack limits
          THEN #SS(0); FI;
        EIP ← Pop();
        CS ← Pop(); (* 32-bit pop, high-order 16 bits discarded *)
      ELSE (* OperandSize = 16 *)
        IF top 6 bytes of stack not within stack limits
          THEN #SS(0); FI;
        tempEIP ← Pop();
        tempEIP ← tempEIP AND 0000FFFFH;
        IF tempEIP not within code segment limits
          THEN #GP(0); FI;
        EIP ← tempEIP;
        CS ← Pop(); (* 16-bit pop *)
      FI;
    FI;

```

```

IF instruction has immediate operand
  THEN
    SP ← SP + (SRC AND FFFFH); (* Release parameters from stack *)
  FI;
FI;

```

(* Protected mode, not virtual-8086 mode *)

```

IF (PE = 1 and VM = 0 and IA32_EFER.LMA = 0) and instruction = far RET
  THEN

```

```

IF OperandSize = 32
    THEN
        IF second doubleword on stack is not within stack limits
            THEN #SS(0); FI;
        ELSE (* OperandSize = 16 *)
            IF second word on stack is not within stack limits
                THEN #SS(0); FI;
    FI;
IF return code segment selector is NULL
    THEN #GP(0); FI;
IF return code segment selector addresses descriptor beyond descriptor table limit
    THEN #GP(selector); FI;
Obtain descriptor to which return code segment selector points from descriptor table;
IF return code segment descriptor is not a code segment
    THEN #GP(selector); FI;
IF return code segment selector RPL < CPL
    THEN #GP(selector); FI;
IF return code segment descriptor is conforming
and return code segment DPL > return code segment selector RPL
    THEN #GP(selector); FI;
IF return code segment descriptor is non-conforming and return code
segment DPL ≠ return code segment selector RPL
    THEN #GP(selector); FI;
IF return code segment descriptor is not present
    THEN #NP(selector); FI;
IF return code segment selector RPL > CPL
    THEN GOTO RETURN-OUTER-PRIVILEGE-LEVEL;
    ELSE GOTO RETURN-TO-SAME-PRIVILEGE-LEVEL;
FI;
FI;

RETURN-SAME-PRIVILEGE-LEVEL:
    IF the return instruction pointer is not within the return code segment limit
        THEN #GP(0); FI;
    IF OperandSize = 32
        THEN
            EIP ← Pop();
            CS ← Pop(); (* 32-bit pop, high-order 16 bits discarded *)
            ESP ← ESP + SRC; (* Release parameters from stack *)
        ELSE (* OperandSize = 16 *)
            EIP ← Pop();
            EIP ← EIP AND 0000FFFFH;
            CS ← Pop(); (* 16-bit pop *)
            ESP ← ESP + SRC; (* Release parameters from stack *)

```

FI;

RETURN-OUTER-PRIVILEGE-LEVEL:

IF top (16 + SRC) bytes of stack are not within stack limits (OperandSize = 32)
or top (8 + SRC) bytes of stack are not within stack limits (OperandSize = 16)

THEN #SS(0); FI;

Read return segment selector;

IF stack segment selector is NULL

THEN #GP(0); FI;

IF return stack segment selector index is not within its descriptor table limits

THEN #GP(selector); FI;

Read segment descriptor pointed to by return segment selector;

IF stack segment selector RPL \neq RPL of the return code segment selector

or stack segment is not a writable data segment

or stack segment descriptor DPL \neq RPL of the return code segment selector

THEN #GP(selector); FI;

IF stack segment not present

THEN #SS(StackSegmentSelector); FI;

IF the return instruction pointer is not within the return code segment limit

THEN #GP(0); FI;

CPL \leftarrow ReturnCodeSegmentSelector(RPL);

IF OperandSize = 32

THEN

EIP \leftarrow Pop();

CS \leftarrow Pop(); (* 32-bit pop, high-order 16 bits discarded; segment descriptor information also loaded *)

CS(RPL) \leftarrow CPL;

ESP \leftarrow ESP + SRC; (* Release parameters from called procedure's stack *)

tempESP \leftarrow Pop();

tempSS \leftarrow Pop(); (* 32-bit pop, high-order 16 bits discarded; segment descriptor information also loaded *)

ESP \leftarrow tempESP;

SS \leftarrow tempSS;

ELSE (* OperandSize = 16 *)

EIP \leftarrow Pop();

EIP \leftarrow EIP AND 0000FFFFH;

CS \leftarrow Pop(); (* 16-bit pop; segment descriptor information also loaded *)

CS(RPL) \leftarrow CPL;

ESP \leftarrow ESP + SRC; (* Release parameters from called procedure's stack *)

tempESP \leftarrow Pop();

tempSS \leftarrow Pop(); (* 16-bit pop; segment descriptor information also loaded *)

ESP \leftarrow tempESP;

SS \leftarrow tempSS;

FI;

FOR each of segment register (ES, FS, GS, and DS)

DO

IF segment register points to data or non-conforming code segment
and CPL > segment descriptor DPL (* DPL in hidden part of segment register *)
THEN SegmentSelector ← 0; (* Segment selector invalid *)

FI;

OD;

For each of ES, FS, GS, and DS

DO

IF segment selector index is not within descriptor table limits
or segment descriptor indicates the segment is not a data or
readable code segment
or if the segment is a data or non-conforming code segment
and the segment descriptor's DPL < CPL or RPL of code segment's
segment selector

THEN SegmentSelector ← 0; (* Segment selector invalid *)

OD;

ESP ← ESP + SRC; (* Release parameters from calling procedure's stack *)

(* IA-32e Mode *)

IF (PE = 1 and VM = 0 and IA32_EFER.LMA = 1) and instruction = far RET

THEN

IF OperandSize = 32

THEN

IF second doubleword on stack is not within stack limits

THEN #SS(0); FI;

IF first or second doubleword on stack is not in canonical space

THEN #SS(0); FI;

ELSE

IF OperandSize = 16

THEN

IF second word on stack is not within stack limits

THEN #SS(0); FI;

IF first or second word on stack is not in canonical space

THEN #SS(0); FI;

ELSE (* OperandSize = 64 *)

IF first or second quadword on stack is not in canonical space

THEN #SS(0); FI;

FI

FI;

IF return code segment selector is NULL

```

    THEN GP(0); FI;
IF return code segment selector addresses descriptor beyond descriptor table limit
    THEN GP(selector); FI;
IF return code segment selector addresses descriptor in non-canonical space
    THEN GP(selector); FI;
Obtain descriptor to which return code segment selector points from descriptor table;
IF return code segment descriptor is not a code segment
    THEN #GP(selector); FI;
IF return code segment descriptor has L-bit = 1 and D-bit = 1
    THEN #GP(selector); FI;
IF return code segment selector RPL < CPL
    THEN #GP(selector); FI;
IF return code segment descriptor is conforming
and return code segment DPL > return code segment selector RPL
    THEN #GP(selector); FI;
IF return code segment descriptor is non-conforming
and return code segment DPL ≠ return code segment selector RPL
    THEN #GP(selector); FI;
IF return code segment descriptor is not present
    THEN #NP(selector); FI;
IF return code segment selector RPL > CPL
    THEN GOTO IA-32E-MODE-RETURN-OUTER-PRIVILEGE-LEVEL;
    ELSE GOTO IA-32E-MODE-RETURN-SAME-PRIVILEGE-LEVEL;
FI;
FI;

```

IA-32E-MODE-RETURN-SAME-PRIVILEGE-LEVEL:

```

IF the return instruction pointer is not within the return code segment limit
    THEN #GP(0); FI;
IF the return instruction pointer is not within canonical address space
    THEN #GP(0); FI;
IF OperandSize = 32
    THEN
        EIP ← Pop();
        CS ← Pop(); (* 32-bit pop, high-order 16 bits discarded *)
        ESP ← ESP + SRC; (* Release parameters from stack *)
    ELSE
        IF OperandSize = 16
            THEN
                EIP ← Pop();
                EIP ← EIP AND 0000FFFFH;
                CS ← Pop(); (* 16-bit pop *)
                ESP ← ESP + SRC; (* Release parameters from stack *)

```



```

ELSE (* OperandSize = 64 *)
    RIP ← Pop();
    CS ← Pop(); (* 64-bit pop, high-order 48 bits discarded *)
    ESP ← ESP + SRC; (* Release parameters from stack *)

```

```

FI;

```

```

FI;

```

IA-32E-MODE-RETURN-OUTER-PRIVILEGE-LEVEL:

```

IF top (16 + SRC) bytes of stack are not within stack limits (OperandSize = 32)
or top (8 + SRC) bytes of stack are not within stack limits (OperandSize = 16)

```

```

    THEN #SS(0); FI;

```

```

IF top (16 + SRC) bytes of stack are not in canonical address space (OperandSize = 32)
or top (8 + SRC) bytes of stack are not in canonical address space (OperandSize = 16)
or top (32 + SRC) bytes of stack are not in canonical address space (OperandSize = 64)

```

```

    THEN #SS(0); FI;

```

```

Read return stack segment selector;

```

```

IF stack segment selector is NULL

```

```

    THEN

```

```

        IF new CS descriptor L-bit = 0

```

```

            THEN #GP(selector);

```

```

        IF stack segment selector RPL = 3

```

```

            THEN #GP(selector);

```

```

FI;

```

```

IF return stack segment descriptor is not within descriptor table limits

```

```

    THEN #GP(selector); FI;

```

```

IF return stack segment descriptor is in non-canonical address space

```

```

    THEN #GP(selector); FI;

```

```

Read segment descriptor pointed to by return segment selector;

```

```

IF stack segment selector RPL ≠ RPL of the return code segment selector
or stack segment is not a writable data segment

```

```

or stack segment descriptor DPL ≠ RPL of the return code segment selector

```

```

    THEN #GP(selector); FI;

```

```

IF stack segment not present

```

```

    THEN #SS(StackSegmentSelector); FI;

```

```

IF the return instruction pointer is not within the return code segment limit

```

```

    THEN #GP(0); FI;

```

```

IF the return instruction pointer is not within canonical address space

```

```

    THEN #GP(0); FI;

```

```

CPL ← ReturnCodeSegmentSelector(RPL);

```

```

IF OperandSize = 32

```

```

    THEN

```

```

        EIP ← Pop();

```

```

        CS ← Pop(); (* 32-bit pop, high-order 16 bits discarded, segment descriptor

```

```

information also loaded *)
CS(RPL) ← CPL;
ESP ← ESP + SRC; (* Release parameters from called procedure's stack *)
tempESP ← Pop();
tempSS ← Pop(); (* 32-bit pop, high-order 16 bits discarded, segment descriptor
information also loaded *)
ESP ← tempESP;
SS ← tempSS;
ELSE
  IF OperandSize = 16
    THEN
      EIP ← Pop();
      EIP ← EIP AND 0000FFFFH;
      CS ← Pop(); (* 16-bit pop; segment descriptor information also loaded *)
      CS(RPL) ← CPL;
      ESP ← ESP + SRC; (* release parameters from called
      procedure's stack *)
      tempESP ← Pop();
      tempSS ← Pop(); (* 16-bit pop; segment descriptor information loaded *)
      ESP ← tempESP;
      SS ← tempSS;
    ELSE (* OperandSize = 64 *)
      RIP ← Pop();
      CS ← Pop(); (* 64-bit pop; high-order 48 bits discarded; segment
      descriptor information loaded *)
      CS(RPL) ← CPL;
      ESP ← ESP + SRC; (* Release parameters from called procedure's
      stack *)
      tempESP ← Pop();
      tempSS ← Pop(); (* 64-bit pop; high-order 48 bits discarded; segment
      descriptor information also loaded *)
      ESP ← tempESP;
      SS ← tempSS;
  FI;
FI;

FOR each of segment register (ES, FS, GS, and DS)
  DO
    IF segment register points to data or non-conforming code segment
    and CPL > segment descriptor DPL; (* DPL in hidden part of segment register *)
    THEN SegmentSelector ← 0; (* SegmentSelector invalid *)
  FI;
OD;

```

For each of ES, FS, GS, and DS

DO

IF segment selector index is not within descriptor table limits
 or segment descriptor indicates the segment is not a data or readable code segment
 or if the segment is a data or non-conforming code segment
 and the segment descriptor's DPL < CPL or RPL of code segment's segment selector
 THEN SegmentSelector ← 0; (* SegmentSelector invalid *)

OD;

ESP ESP + SRC; (* Release parameters from calling procedure's stack *)

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the return code or stack segment selector NULL. If the return instruction pointer is not within the return code segment limit |
| #GP(selector) | If the RPL of the return code segment selector is less than the CPL. If the return code or stack segment selector index is not within its descriptor table limits. If the return code segment descriptor does not indicate a code segment. If the return code segment is non-conforming and the segment selector's DPL is not equal to the RPL of the code segment's segment selector If the return code segment is conforming and the segment selector's DPL greater than the RPL of the code segment's segment selector If the stack segment is not a writable data segment. If the stack segment selector RPL is not equal to the RPL of the return code segment selector. If the stack segment descriptor DPL is not equal to the RPL of the return code segment selector. |
| #SS(0) | If the top bytes of stack are not within stack limits. If the return stack segment is not present. |
| #NP(selector) | If the return code segment is not present. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory access occurs when the CPL is 3 and alignment checking is enabled. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If the return instruction pointer is not within the return code segment limit |
| #SS | If the top bytes of stack are not within stack limits. |

Virtual-8086 Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If the return instruction pointer is not within the return code segment limit |
| #SS(0) | If the top bytes of stack are not within stack limits. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | If an unaligned memory access occurs when alignment checking is enabled. |

Compatibility Mode Exceptions

Same as 64-bit mode exceptions.

64-Bit Mode Exceptions

| | |
|---------------|--|
| #GP(0) | <p>If the return instruction pointer is non-canonical.</p> <p>If the return instruction pointer is not within the return code segment limit.</p> <p>If the stack segment selector is NULL going back to compatibility mode.</p> <p>If the stack segment selector is NULL going back to CPL3 64-bit mode.</p> <p>If a NULL stack segment selector RPL is not equal to CPL going back to non-CPL3 64-bit mode.</p> <p>If the return code segment selector is NULL.</p> |
| #GP(selector) | <p>If the proposed segment descriptor for a code segment does not indicate it is a code segment.</p> <p>If the proposed new code segment descriptor has both the D-bit and L-bit set.</p> <p>If the DPL for a nonconforming-code segment is not equal to the RPL of the code segment selector.</p> <p>If CPL is greater than the RPL of the code segment selector.</p> <p>If the DPL of a conforming-code segment is greater than the return code segment selector RPL.</p> <p>If a segment selector index is outside its descriptor table limits.</p> <p>If a segment descriptor memory address is non-canonical.</p> <p>If the stack segment is not a writable data segment.</p> |

If the stack segment descriptor DPL is not equal to the RPL of the return code segment selector.

If the stack segment selector RPL is not equal to the RPL of the return code segment selector.

#SS(0)

If an attempt to pop a value off the stack violates the SS limit.

If an attempt to pop a value off the stack causes a non-canonical address to be referenced.

#NP(selector)

If the return code or stack segment is not present.

#PF(fault-code)

If a page fault occurs.

#AC(0)

If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

ROUNDPD — Round Packed Double Precision Floating-Point Values

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|----------------------|---|-------------|-----------------|--|
| 66 OF 3A 09 /r ib | ROUNDPD <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Round packed double precision floating-point values in <i>xmm2/m128</i> and place the result in <i>xmm1</i> . The rounding mode is determined by <i>imm8</i> . |

Description

Round the 2 double-precision floating-point values in the source operand (second operand) using the rounding mode specified in the immediate operand (third operand) and place the results in the destination operand (first operand). The rounding process rounds each input floating-point value to an integer value and returns the integer result as a single-precision floating-point value.

The immediate operand specifies control fields for the rounding operation, three bit fields are defined and shown in Figure 4-13. Bit 3 of the immediate byte controls processor behavior for a precision exception, bit 2 selects the source of rounding mode control. Bits 1:0 specify a non-sticky rounding-mode value (Table 4-4 lists the encoded values for rounding-mode field).

The Precision Floating-Point Exception is signaled according to the immediate operand. If any source operand is an SNaN then it will be converted to a QNaN. If DAZ is set to '1 then denormals will be converted to zero before rounding.

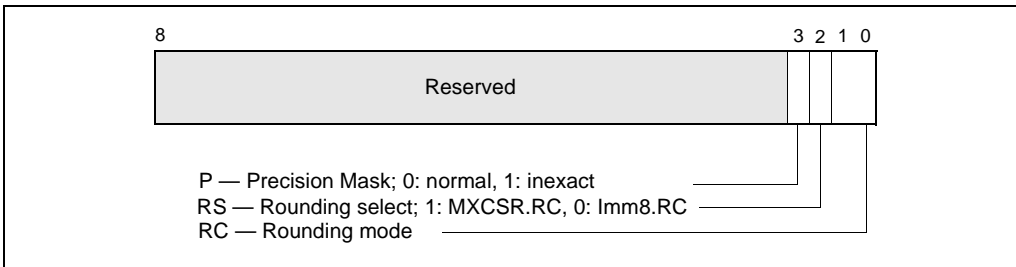


Figure 4-13. Bit Control Fields of Immediate Byte for ROUNDxx Instruction

Table 4-4. Rounding Modes and Encoding of Rounding Control (RC) Field

| Rounding Mode | RC Field Setting | Description |
|--------------------------------|------------------|---|
| Round to nearest (even) | 00B | Rounded result is the closest to the infinitely precise result. If two values are equally close, the result is the even value (i.e., the integer value with the least-significant bit of zero). |
| Round down (toward $-\infty$) | 01B | Rounded result is closest to but no greater than the infinitely precise result. |
| Round up (toward $+\infty$) | 10B | Rounded result is closest to but no less than the infinitely precise result. |
| Round toward zero (Truncate) | 11B | Rounded result is closest to but no greater in absolute value than the infinitely precise result. |

Operation

```

IF (imm[2] == '1')
    THEN // rounding mode is determined by MXCSR.RC
        DEST[63:0] ← ConvertDPFPToInteger_M(SRC[63:0]);
        DEST[127:64] ← ConvertDPFPToInteger_M(SRC[127:64]);
    ELSE // rounding mode is determined by IMM8.RC
        DEST[63:0] ← ConvertDPFPToInteger_Imm(SRC[63:0]);
        DEST[127:64] ← ConvertDPFPToInteger_Imm(SRC[127:64]);
FI

```

Intel C/C++ Compiler Intrinsic Equivalent

```

ROUNDPD __m128 mm_round_pd(__m128d s1, int iRoundMode);
        __m128 mm_floor_pd(__m128d s1);
        __m128 mm_ceil_pd(__m128d s1);

```

SIMD Floating-Point Exceptions

Invalid (signaled only if SRC = SNaN)

Precision (signaled only if imm[3] == '0'; if imm[3] == '1', then the Precision Mask in the MXCSR is ignored and precision exception is not signaled.)

Note that Denormal is not signaled by ROUNDPD.

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.

If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

| | |
|-----------------|--|
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. |

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

ROUNDPS — Round Packed Single Precision Floating-Point Values

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------------|---|-------------|------------------|--|
| 66 OF 3A 08 /r ib | ROUNDPS <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Round packed single precision floating-point values in <i>xmm2/m128</i> and place the result in <i>xmm1</i> . The rounding mode is determined by <i>imm8</i> . |

Description

Round the 4 single-precision floating-point values in the source operand (second operand) using the rounding mode specified in the immediate operand (third operand) and place the results in the destination operand (first operand). The rounding process rounds each input floating-point value to an integer value and returns the integer result as a single-precision floating-point value.

The immediate operand specifies control fields for the rounding operation, three bit fields are defined and shown in Figure 4-13. Bit 3 of the immediate byte controls processor behavior for a precision exception, bit 2 selects the source of rounding mode control. Bits 1:0 specify a non-sticky rounding-mode value (Table 4-4 lists the encoded values for rounding-mode field).

The Precision Floating-Point Exception is signaled according to the immediate operand. If any source operand is an SNaN then it will be converted to a QNaN. If DAZ is set to '1 then denormals will be converted to zero before rounding.

Operation

```
IF (imm[2] == '1)
    THEN // rounding mode is determined by MXCSR.RC
        DEST[31:0] ← ConvertSPFPToInteger_M(SRC[31:0]);
        DEST[63:32] ← ConvertSPFPToInteger_M(SRC[63:32]);
        DEST[95:64] ← ConvertSPFPToInteger_M(SRC[95:64]);
        DEST[127:96] ← ConvertSPFPToInteger_M(SRC[127:96]);
    ELSE // rounding mode is determined by IMM8.RC
        DEST[31:0] ← ConvertSPFPToInteger_Imm(SRC[31:0]);
        DEST[63:32] ← ConvertSPFPToInteger_Imm(SRC[63:32]);
        DEST[95:64] ← ConvertSPFPToInteger_Imm(SRC[95:64]);
        DEST[127:96] ← ConvertSPFPToInteger_Imm(SRC[127:96]);
FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
ROUNDPS  __m128 mm_round_ps(__m128 s1, int iRoundMode);
          __m128 mm_floor_ps(__m128 s1);
          __m128 mm_ceil_ps(__m128 s1);
```

SIMD Floating-Point Exceptions

Invalid (signaled only if SRC = SNaN)

Precision (signaled only if imm[3] == '0'; if imm[3] == '1', then the Precision Mask in the MXSCSR is ignored and precision exception is not signaled.)

Note that Denormal is not signaled by ROUNDPS.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

#GP(0) If the memory address is in a non-canonical form.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#PF(fault-code) For a page fault.

#NM If TS in CR0 is set.

#UD If EM in CR0 is set.
If OSFXSR in CR4 is 0.
If CPUID feature flag ECX.SSE4_1 is 0.
If LOCK prefix is used.
Either the prefix REP (F3h) or REPN (F2H) is used.

ROUNDSD — Round Scalar Double Precision Floating-Point Values

| Opcode | Instruction | 64-bit Mode | Compat/ Leg Mode | Description |
|----------------------|--|-------------|------------------|--|
| 66 OF 3A 0B /r ib | ROUNDSD <i>xmm1</i> , <i>xmm2/m64</i> , <i>imm8</i> | Valid | Valid | Round the low packed double precision floating-point value in <i>xmm2/m64</i> and place the result in <i>xmm1</i> . The rounding mode is determined by <i>imm8</i> . |

Description

Round the DP FP value in the lower qword of the source operand (second operand) using the rounding mode specified in the immediate operand (third operand) and place the result in the destination operand (first operand). The rounding process rounds a double-precision floating-point input to an integer value and returns the integer result as a double precision floating-point value in the lowest position. The upper double precision floating-point value in the destination is retained.

The immediate operand specifies control fields for the rounding operation, three bit fields are defined and shown in Figure 4-13. Bit 3 of the immediate byte controls processor behavior for a precision exception, bit 2 selects the source of rounding mode control. Bits 1:0 specify a non-sticky rounding-mode value (Table 4-4 lists the encoded values for rounding-mode field).

The Precision Floating-Point Exception is signaled according to the immediate operand. If any source operand is an SNaN then it will be converted to a QNaN. If DAZ is set to '1' then denormals will be converted to zero before rounding.

Operation

```
IF (imm[2] == '1')
    THEN // rounding mode is determined by MXCSR.RC
        DEST[63:0] ← ConvertDPFPToInteger_M(SRC[63:0]);
    ELSE // rounding mode is determined by IMM8.RC
        DEST[63:0] ← ConvertDPFPToInteger_Imm(SRC[63:0]);
FI;
DEST[127:63] remains unchanged ;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
ROUNDSD __m128d mm_round_sd(__m128d dst, __m128d s1, int iRoundMode);
        __m128d mm_floor_sd(__m128d dst, __m128d s1);
        __m128d mm_ceil_sd(__m128d dst, __m128d s1);
```

SIMD Floating-Point Exceptions

Invalid (signaled only if SRC = SNaN)

Precision (signaled only if imm[3] == '0'; if imm[3] == '1', then the Precision Mask in the MXCSR is ignored and precision exception is not signaled.)

Note that Denormal is not signaled by ROUNDSD.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real Mode Exceptions

| | |
|--------|--|
| #GP(0) | if any part of the operand lies outside of the effective address space from 0 to 0FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: ECX.SSE4_1[bit 19] = 0. If LOCK prefix is used. Either the prefix REP (F3h) or REPN (F2H) is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

| | |
|-----------------|--|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. |
| | Either the prefix REP (F3h) or REPN (F2H) is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

ROUNDSS — Round Scalar Single Precision Floating-Point Values

| Opcode | Instruction | 64-bit Mode | Compat/Leg Mode | Description |
|----------------------|--|-------------|-----------------|--|
| 66 OF 3A 0A /r ib | ROUNDSS <i>xmm1</i> , <i>xmm2/m32</i> , <i>imm8</i> | Valid | Valid | Round the low packed single precision floating-point value in <i>xmm2/m32</i> and place the result in <i>xmm1</i> . The rounding mode is determined by <i>imm8</i> . |

Description

Round the single-precision floating-point value in the lowest dword of the source operand (second operand) using the rounding mode specified in the immediate operand (third operand) and place the result in the destination operand (first operand). The rounding process rounds a single-precision floating-point input to an integer value and returns the result as a single-precision floating-point value in the lowest position. The upper three single-precision floating-point values in the destination are retained.

The immediate operand specifies control fields for the rounding operation, three bit fields are defined and shown in Figure 4-13. Bit 3 of the immediate byte controls processor behavior for a precision exception, bit 2 selects the source of rounding mode control. Bits 1:0 specify a non-sticky rounding-mode value (Table 4-4 lists the encoded values for rounding-mode field).

The Precision Floating-Point Exception is signaled according to the immediate operand. If any source operand is an SNaN then it will be converted to a QNaN. If DAZ is set to '1 then denormals will be converted to zero before rounding.

Operation

```
IF (imm[2] == '1)
    THEN // rounding mode is determined by MXCSR.RC
        DEST[31:0] ← ConvertSPFPToInteger_M(SRC[31:0]);
    ELSE // rounding mode is determined by IMM8.RC
        DEST[31:0] ← ConvertSPFPToInteger_Imm(SRC[31:0]);
FI;
DEST[127:32] remains unchanged ;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
ROUNDSS    __m128 mm_round_ss(__m128 dst, __m128 s1, int iRoundMode);
           __m128 mm_floor_ss(__m128 dst, __m128 s1);
           __m128 mm_ceil_ss(__m128 dst, __m128 s1);
```


SIMD Floating-Point Exceptions

Invalid (signaled only if SRC = SNaN)

Precision (signaled only if imm[3] == '0'; if imm[3] == '1', then the Precision Mask in the MXSCSR is ignored and precision exception is not signaled.)

Note that Denormal is not signaled by ROUNDSS.

Protected Mode Exceptions

#GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments.

#SS(0) For an illegal address in the SS segment.

#PF(fault:code) For a page fault.

#NM If CR0.TS[bit 3] = 1.

#UD If CR0.EM[bit 2] = 1.

If CR4.OSFXSR[bit 9] = 0.

If CPUID.01H: ECX.SSE4_1[bit 19] = 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Real Mode Exceptions

#GP if any part of the operand lies outside of the effective address space from 0 to 0FFFFH.

#NM If CR0.TS[bit 3] = 1.

#UD If CR0.EM[bit 2] = 1.

If CR4.OSFXSR[bit 9] = 0.

If CPUID.01H: ECX.SSE4_1[bit 19] = 0.

If LOCK prefix is used.

Either the prefix REP (F3h) or REPN (F2H) is used.

Virtual 8086 Mode Exceptions

Same exceptions as in Real Address Mode.

#PF(fault-code) For a page fault.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

Compatibility Mode Exceptions

Same exceptions as in Protected Mode.

64-Bit Mode Exceptions

| | |
|------------------|--|
| #GP(0) | If the memory address is in a non-canonical form. |
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #PF (fault-code) | For a page fault. |
| #NM | If TS in CR0 is set. |
| #UD | If EM in CR0 is set. If OSFXSR in CR4 is 0. If CPUID feature flag ECX.SSE4_1 is 0. If LOCK prefix is used. |
| #AC(0) | Either the prefix REP (F3h) or REPN (F2H) is used. If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

RSM—Resume from System Management Mode

| Opcode | Instruction | Non-SMM Mode | SMM Mode | Description |
|--------|-------------|--------------|----------|--|
| 0F AA | RSM | Invalid | Valid | Resume operation of interrupted program. |

Description

Returns program control from system management mode (SMM) to the application program or operating-system procedure that was interrupted when the processor received an SMM interrupt. The processor's state is restored from the dump created upon entering SMM. If the processor detects invalid state information during state restoration, it enters the shutdown state. The following invalid information can cause a shutdown:

- Any reserved bit of CR4 is set to 1.
- Any illegal combination of bits in CR0, such as (PG=1 and PE=0) or (NW=1 and CD=0).
- (Intel Pentium and Intel486™ processors only.) The value stored in the state dump base field is not a 32-KByte aligned address.

The contents of the model-specific registers are not affected by a return from SMM.

The SMM state map used by RSM supports resuming processor context for non-64-bit modes and 64-bit mode.

See Chapter 26, "System Management," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B*, for more information about SMM and the behavior of the RSM instruction.

Operation

ReturnFromSMM;

IF (IA-32e mode supported) or (CPUID_DisplayFamily_DisplayModleSignature = 06H_0CH)

THEN

ProcessorState ← Restore(SMMDump(IA-32e SMM STATE MAP));

Else

ProcessorState ← Restore(SMMDump(Non-32-Bit-Mode SMM STATE MAP));

FI

Flags Affected

All.

Protected Mode Exceptions

#UD If an attempt is made to execute this instruction when the processor is not in SMM.
 If the LOCK prefix is used.

Real-Address Mode Exceptions

Same exceptions as in protected mode.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

RSQRTPS—Compute Reciprocals of Square Roots of Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|---|-------------|-----------------|---|
| OF 52 /r | RSQRTPS <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Computes the approximate reciprocals of the square roots of the packed single-precision floating-point values in <i>xmm2/m128</i> and stores the results in <i>xmm1</i> . |

Description

Performs a SIMD computation of the approximate reciprocals of the square roots of the four packed single-precision floating-point values in the source operand (second operand) and stores the packed single-precision floating-point results in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. See Figure 10-5 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD single-precision floating-point operation.

The relative error for this approximation is:

$$|\text{Relative Error}| \leq 1.5 * 2^{-12}$$

The RSQRTPS instruction is not affected by the rounding control bits in the MXCSR register. When a source value is a 0.0, an ∞ of the sign of the source value is returned. A denormal source value is treated as a 0.0 (of the same sign). When a source value is a negative value (other than -0.0), a floating-point indefinite is returned. When a source value is an SNaN or QNaN, the SNaN is converted to a QNaN or the source QNaN is returned.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[31:0] ← APPROXIMATE(1.0/SQRT(SRC[31:0]));
DEST[63:32] ← APPROXIMATE(1.0/SQRT(SRC[63:32]));
DEST[95:64] ← APPROXIMATE(1.0/SQRT(SRC[95:64]));
DEST[127:96] ← APPROXIMATE(1.0/SQRT(SRC[127:96]));
```

Intel C/C++ Compiler Intrinsic Equivalent

```
RSQRTPS __m128 __mm_rsqrtps(__m128 a)
```

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
|--------|--|

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

RSQRTSS—Compute Reciprocal of Square Root of Scalar Single-Precision Floating-Point Value

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--|-------------|-----------------|--|
| F3 0F 52 /r | RSQRTSS <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Computes the approximate reciprocal of the square root of the low single-precision floating-point value in <i>xmm2/m32</i> and stores the results in <i>xmm1</i> . |

Description

Computes an approximate reciprocal of the square root of the low single-precision floating-point value in the source operand (second operand) stores the single-precision floating-point result in the destination operand. The source operand can be an XMM register or a 32-bit memory location. The destination operand is an XMM register. The three high-order doublewords of the destination operand remain unchanged. See Figure 10-6 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a scalar single-precision floating-point operation.

The relative error for this approximation is:

$$|\text{Relative Error}| \leq 1.5 * 2^{-12}$$

The RSQRTSS instruction is not affected by the rounding control bits in the MXCSR register. When a source value is a 0.0, an ∞ of the sign of the source value is returned. A denormal source value is treated as a 0.0 (of the same sign). When a source value is a negative value (other than -0.0), a floating-point indefinite is returned. When a source value is an SNaN or QNaN, the SNaN is converted to a QNaN or the source QNaN is returned.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[31:0] ← APPROXIMATE(1.0/SQRT(SRC[31:0]));
(* DEST[127:32] unchanged *)

Intel C/C++ Compiler Intrinsic Equivalent

RSQRTSS __m128 _mm_rsqrt_ss(__m128 a)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|--|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|--------|--|
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

SAHF—Store AH into Flags

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|--------|-------------|-------------|-----------------|--|
| 9E | SAHF | Invalid* | Valid | Loads SF, ZF, AF, PF, and CF from AH into EFLAGS register. |

NOTES:

* Valid in specific steppings. See Description section.

Description

Loads the SF, ZF, AF, PF, and CF flags of the EFLAGS register with values from the corresponding bits in the AH register (bits 7, 6, 4, 2, and 0, respectively). Bits 1, 3, and 5 of register AH are ignored; the corresponding reserved bits (1, 3, and 5) in the EFLAGS register remain as shown in the “Operation” section below.

This instruction executes as described above in compatibility mode and legacy mode. It is valid in 64-bit mode only if CPUID.80000001H:ECX.LAHF-SAHF[bit 0] = 1.

Operation

```
IF IA-64 Mode
  THEN
    IF CPUID.80000001.ECX[0] = 1;
      THEN
        RFLAGS(SF:ZF:0:AF:0:PF:1:CF) ← AH;
      ELSE
        #UD;
    FI
  ELSE
    EFLAGS(SF:ZF:0:AF:0:PF:1:CF) ← AH;
FI;
```

Flags Affected

The SF, ZF, AF, PF, and CF flags are loaded with values from the AH register. Bits 1, 3, and 5 of the EFLAGS register are unaffected, with the values remaining 1, 0, and 0, respectively.

Protected Mode Exceptions

None.

Real-Address Mode Exceptions

None.

Virtual-8086 Mode Exceptions

None.

Compatibility Mode Exceptions

None.

64-Bit Mode Exceptions

#UD If CPUID.80000001.ECX[0] = 0.
 If the LOCK prefix is used.

SAL/SAR/SHL/SHR—Shift

| Opcode*** | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|---------------------------------|-------------|---------------------|---|
| D0 /4 | SAL <i>r/m8</i> , 1 | Valid | Valid | Multiply <i>r/m8</i> by 2, once. |
| REX + D0 /4 | SAL <i>r/m8**</i> , 1 | Valid | N.E. | Multiply <i>r/m8</i> by 2, once. |
| D2 /4 | SAL <i>r/m8</i> , CL | Valid | Valid | Multiply <i>r/m8</i> by 2, CL times. |
| REX + D2 /4 | SAL <i>r/m8**</i> , CL | Valid | N.E. | Multiply <i>r/m8</i> by 2, CL times. |
| C0 /4 <i>ib</i> | SAL <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Multiply <i>r/m8</i> by 2, <i>imm8</i> times. |
| REX + C0 /4 <i>ib</i> | SAL <i>r/m8**</i> , <i>imm8</i> | Valid | N.E. | Multiply <i>r/m8</i> by 2, <i>imm8</i> times. |
| D1 /4 | SAL <i>r/m16</i> , 1 | Valid | Valid | Multiply <i>r/m16</i> by 2, once. |
| D3 /4 | SAL <i>r/m16</i> , CL | Valid | Valid | Multiply <i>r/m16</i> by 2, CL times. |
| C1 /4 <i>ib</i> | SAL <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Multiply <i>r/m16</i> by 2, <i>imm8</i> times. |
| D1 /4 | SAL <i>r/m32</i> , 1 | Valid | Valid | Multiply <i>r/m32</i> by 2, once. |
| REX.W + D1 /4 | SAL <i>r/m64</i> , 1 | Valid | N.E. | Multiply <i>r/m64</i> by 2, once. |
| D3 /4 | SAL <i>r/m32</i> , CL | Valid | Valid | Multiply <i>r/m32</i> by 2, CL times. |
| REX.W + D3 /4 | SAL <i>r/m64</i> , CL | Valid | N.E. | Multiply <i>r/m64</i> by 2, CL times. |
| C1 /4 <i>ib</i> | SAL <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Multiply <i>r/m32</i> by 2, <i>imm8</i> times. |
| REX.W + C1 /4 <i>ib</i> | SAL <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Multiply <i>r/m64</i> by 2, <i>imm8</i> times. |
| D0 /7 | SAR <i>r/m8</i> , 1 | Valid | Valid | Signed divide* <i>r/m8</i> by 2, once. |
| REX + D0 /7 | SAR <i>r/m8**</i> , 1 | Valid | N.E. | Signed divide* <i>r/m8</i> by 2, once. |
| D2 /7 | SAR <i>r/m8</i> , CL | Valid | Valid | Signed divide* <i>r/m8</i> by 2, CL times. |
| REX + D2 /7 | SAR <i>r/m8**</i> , CL | Valid | N.E. | Signed divide* <i>r/m8</i> by 2, CL times. |
| C0 /7 <i>ib</i> | SAR <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Signed divide* <i>r/m8</i> by 2, <i>imm8</i> time. |
| REX + C0 /7 <i>ib</i> | SAR <i>r/m8**</i> , <i>imm8</i> | Valid | N.E. | Signed divide* <i>r/m8</i> by 2, <i>imm8</i> times. |
| D1 /7 | SAR <i>r/m16</i> , 1 | Valid | Valid | Signed divide* <i>r/m16</i> by 2, once. |

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|---------------------------------|-------------|------------------|--|
| D3 /7 | SAR <i>r/m16</i> , CL | Valid | Valid | Signed divide* <i>r/m16</i> by 2, CL times. |
| C1 /7 <i>ib</i> | SAR <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Signed divide* <i>r/m16</i> by 2, <i>imm8</i> times. |
| D1 /7 | SAR <i>r/m32</i> , 1 | Valid | Valid | Signed divide* <i>r/m32</i> by 2, once. |
| REX.W + D1 /7 | SAR <i>r/m64</i> , 1 | Valid | N.E. | Signed divide* <i>r/m64</i> by 2, once. |
| D3 /7 | SAR <i>r/m32</i> , CL | Valid | Valid | Signed divide* <i>r/m32</i> by 2, CL times. |
| REX.W + D3 /7 | SAR <i>r/m64</i> , CL | Valid | N.E. | Signed divide* <i>r/m64</i> by 2, CL times. |
| C1 /7 <i>ib</i> | SAR <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Signed divide* <i>r/m32</i> by 2, <i>imm8</i> times. |
| REX.W + C1 /7 <i>ib</i> | SAR <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Signed divide* <i>r/m64</i> by 2, <i>imm8</i> times |
| D0 /4 | SHL <i>r/m8</i> , 1 | Valid | Valid | Multiply <i>r/m8</i> by 2, once. |
| REX + D0 /4 | SHL <i>r/m8**</i> , 1 | Valid | N.E. | Multiply <i>r/m8</i> by 2, once. |
| D2 /4 | SHL <i>r/m8</i> , CL | Valid | Valid | Multiply <i>r/m8</i> by 2, CL times. |
| REX + D2 /4 | SHL <i>r/m8**</i> , CL | Valid | N.E. | Multiply <i>r/m8</i> by 2, CL times. |
| C0 /4 <i>ib</i> | SHL <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Multiply <i>r/m8</i> by 2, <i>imm8</i> times. |
| REX + C0 /4 <i>ib</i> | SHL <i>r/m8**</i> , <i>imm8</i> | Valid | N.E. | Multiply <i>r/m8</i> by 2, <i>imm8</i> times. |
| D1 /4 | SHL <i>r/m16</i> , 1 | Valid | Valid | Multiply <i>r/m16</i> by 2, once. |
| D3 /4 | SHL <i>r/m16</i> , CL | Valid | Valid | Multiply <i>r/m16</i> by 2, CL times. |
| C1 /4 <i>ib</i> | SHL <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Multiply <i>r/m16</i> by 2, <i>imm8</i> times. |
| D1 /4 | SHL <i>r/m32</i> , 1 | Valid | Valid | Multiply <i>r/m32</i> by 2, once. |
| REX.W + D1 /4 | SHL <i>r/m64</i> , 1 | Valid | N.E. | Multiply <i>r/m64</i> by 2, once. |
| D3 /4 | SHL <i>r/m32</i> , CL | Valid | Valid | Multiply <i>r/m32</i> by 2, CL times. |
| REX.W + D3 /4 | SHL <i>r/m64</i> , CL | Valid | N.E. | Multiply <i>r/m64</i> by 2, CL times. |
| C1 /4 <i>ib</i> | SHL <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Multiply <i>r/m32</i> by 2, <i>imm8</i> times. |
| REX.W + C1 /4 <i>ib</i> | SHL <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Multiply <i>r/m64</i> by 2, <i>imm8</i> times. |

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|---------------------------------|-------------|------------------|---|
| D0 /5 | SHR <i>r/m8</i> ,1 | Valid | Valid | Unsigned divide <i>r/m8</i> by 2, once. |
| REX + D0 /5 | SHR <i>r/m8</i> **, 1 | Valid | N.E. | Unsigned divide <i>r/m8</i> by 2, once. |
| D2 /5 | SHR <i>r/m8</i> , CL | Valid | Valid | Unsigned divide <i>r/m8</i> by 2, CL times. |
| REX + D2 /5 | SHR <i>r/m8</i> **, CL | Valid | N.E. | Unsigned divide <i>r/m8</i> by 2, CL times. |
| C0 /5 <i>ib</i> | SHR <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Unsigned divide <i>r/m8</i> by 2, <i>imm8</i> times. |
| REX + C0 /5 <i>ib</i> | SHR <i>r/m8</i> **, <i>imm8</i> | Valid | N.E. | Unsigned divide <i>r/m8</i> by 2, <i>imm8</i> times. |
| D1 /5 | SHR <i>r/m16</i> , 1 | Valid | Valid | Unsigned divide <i>r/m16</i> by 2, once. |
| D3 /5 | SHR <i>r/m16</i> , CL | Valid | Valid | Unsigned divide <i>r/m16</i> by 2, CL times |
| C1 /5 <i>ib</i> | SHR <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Unsigned divide <i>r/m16</i> by 2, <i>imm8</i> times. |
| D1 /5 | SHR <i>r/m32</i> , 1 | Valid | Valid | Unsigned divide <i>r/m32</i> by 2, once. |
| REX.W + D1 /5 | SHR <i>r/m64</i> , 1 | Valid | N.E. | Unsigned divide <i>r/m64</i> by 2, once. |
| D3 /5 | SHR <i>r/m32</i> , CL | Valid | Valid | Unsigned divide <i>r/m32</i> by 2, CL times. |
| REX.W + D3 /5 | SHR <i>r/m64</i> , CL | Valid | N.E. | Unsigned divide <i>r/m64</i> by 2, CL times. |
| C1 /5 <i>ib</i> | SHR <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Unsigned divide <i>r/m32</i> by 2, <i>imm8</i> times. |
| REX.W + C1 /5 <i>ib</i> | SHR <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Unsigned divide <i>r/m64</i> by 2, <i>imm8</i> times. |

NOTES:

* Not the same form of division as IDIV; rounding is toward negative infinity.

** In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

***See IA-32 Architecture Compatibility section below.

Description

Shifts the bits in the first operand (destination operand) to the left or right by the number of bits specified in the second operand (count operand). Bits shifted beyond the destination operand boundary are first shifted into the CF flag, then discarded. At the end of the shift operation, the CF flag contains the last bit shifted out of the destination operand.

The destination operand can be a register or a memory location. The count operand can be an immediate value or the CL register. The count is masked to 5 bits (or 6 bits if in 64-bit mode and REX.W is used). The count range is limited to 0 to 31 (or 63 if 64-bit mode and REX.W is used). A special opcode encoding is provided for a count of 1.

The shift arithmetic left (SAL) and shift logical left (SHL) instructions perform the same operation; they shift the bits in the destination operand to the left (toward more significant bit locations). For each shift count, the most significant bit of the destination operand is shifted into the CF flag, and the least significant bit is cleared (see Figure 7-7 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*).

The shift arithmetic right (SAR) and shift logical right (SHR) instructions shift the bits of the destination operand to the right (toward less significant bit locations). For each shift count, the least significant bit of the destination operand is shifted into the CF flag, and the most significant bit is either set or cleared depending on the instruction type. The SHR instruction clears the most significant bit (see Figure 7-8 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*); the SAR instruction sets or clears the most significant bit to correspond to the sign (most significant bit) of the original value in the destination operand. In effect, the SAR instruction fills the empty bit position's shifted value with the sign of the unshifted value (see Figure 7-9 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*).

The SAR and SHR instructions can be used to perform signed or unsigned division, respectively, of the destination operand by powers of 2. For example, using the SAR instruction to shift a signed integer 1 bit to the right divides the value by 2.

Using the SAR instruction to perform a division operation does not produce the same result as the IDIV instruction. The quotient from the IDIV instruction is rounded toward zero, whereas the "quotient" of the SAR instruction is rounded toward negative infinity. This difference is apparent only for negative numbers. For example, when the IDIV instruction is used to divide -9 by 4, the result is -2 with a remainder of -1. If the SAR instruction is used to shift -9 right by two bits, the result is -3 and the "remainder" is +3; however, the SAR instruction stores only the most significant bit of the remainder (in the CF flag).

The OF flag is affected only on 1-bit shifts. For left shifts, the OF flag is set to 0 if the most-significant bit of the result is the same as the CF flag (that is, the top two bits of the original operand were the same); otherwise, it is set to 1. For the SAR instruction, the OF flag is cleared for all 1-bit shifts. For the SHR instruction, the OF flag is set to the most-significant bit of the original operand.

In 64-bit mode, the instruction's default operation size is 32 bits and the mask width for CL is 5 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64-bits and sets the mask width for CL to 6 bits. See the summary chart at the beginning of this section for encoding data and limits.

IA-32 Architecture Compatibility

The 8086 does not mask the shift count. However, all other IA-32 processors (starting with the Intel 286 processor) do mask the shift count to 5 bits, resulting in a maximum count of 31. This masking is done in all operating modes (including the virtual-8086 mode) to reduce the maximum execution time of the instructions.

Operation

IF 64-Bit Mode and using REX.W

THEN

countMASK \leftarrow 3FH;

ELSE

countMASK \leftarrow 1FH;

FI

tempCOUNT \leftarrow (COUNT AND countMASK);

tempDEST \leftarrow DEST;

WHILE (tempCOUNT \neq 0)

DO

IF instruction is SAL or SHL

THEN

CF \leftarrow MSB(DEST);

ELSE (* Instruction is SAR or SHR *)

CF \leftarrow LSB(DEST);

FI;

IF instruction is SAL or SHL

THEN

DEST \leftarrow DEST * 2;

ELSE

IF instruction is SAR

THEN

DEST \leftarrow DEST / 2; (* Signed divide, rounding toward negative infinity *)

ELSE (* Instruction is SHR *)

DEST \leftarrow DEST / 2; (* Unsigned divide *)

FI;

FI;

tempCOUNT \leftarrow tempCOUNT - 1;

OD;

```

(* Determine overflow for the various instructions *)
IF (COUNT and countMASK) = 1
  THEN
    IF instruction is SAL or SHL
      THEN
        OF ← MSB(DEST) XOR CF;
      ELSE
        IF instruction is SAR
          THEN
            OF ← 0;
          ELSE (* Instruction is SHR *)
            OF ← MSB(tempDEST);
        FI;
      FI;
    ELSE IF (COUNT AND countMASK) = 0
      THEN
        All flags unchanged;
      ELSE (* COUNT not 1 or 0 *)
        OF ← undefined;
      FI;
    FI;
  FI;

```

Flags Affected

The CF flag contains the value of the last bit shifted out of the destination operand; it is undefined for SHL and SHR instructions where the count is greater than or equal to the size (in bits) of the destination operand. The OF flag is affected only for 1-bit shifts (see “Description” above); otherwise, it is undefined. The SF, ZF, and PF flags are set according to the result. If the count is 0, the flags are not affected. For a non-zero count, the AF flag is undefined.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | <p>If the destination is located in a non-writable segment.</p> <p>If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register contains a NULL segment selector.</p> |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |

| | |
|--------|--|
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

SBB—Integer Subtraction with Borrow

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------------------|---------------------------------|-------------|-----------------|--|
| 1C <i>ib</i> | SBB AL, <i>imm8</i> | Valid | Valid | Subtract with borrow <i>imm8</i> from AL. |
| 1D <i>iw</i> | SBB AX, <i>imm16</i> | Valid | Valid | Subtract with borrow <i>imm16</i> from AX. |
| 1D <i>id</i> | SBB EAX, <i>imm32</i> | Valid | Valid | Subtract with borrow <i>imm32</i> from EAX. |
| REX.W + 1D <i>id</i> | SBB RAX, <i>imm32</i> | Valid | N.E. | Subtract with borrow sign-extended <i>imm.32 to 64-bits</i> from RAX. |
| 80 /3 <i>ib</i> | SBB <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Subtract with borrow <i>imm8</i> from <i>r/m8</i> . |
| REX + 80 /3 <i>ib</i> | SBB <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | Subtract with borrow <i>imm8</i> from <i>r/m8</i> . |
| 81 /3 <i>iw</i> | SBB <i>r/m16</i> , <i>imm16</i> | Valid | Valid | Subtract with borrow <i>imm16</i> from <i>r/m16</i> . |
| 81 /3 <i>id</i> | SBB <i>r/m32</i> , <i>imm32</i> | Valid | Valid | Subtract with borrow <i>imm32</i> from <i>r/m32</i> . |
| REX.W + 81 /3 <i>id</i> | SBB <i>r/m64</i> , <i>imm32</i> | Valid | N.E. | Subtract with borrow sign-extended <i>imm32 to 64-bits</i> from <i>r/m64</i> . |
| 83 /3 <i>ib</i> | SBB <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Subtract with borrow sign-extended <i>imm8</i> from <i>r/m16</i> . |
| 83 /3 <i>ib</i> | SBB <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Subtract with borrow sign-extended <i>imm8</i> from <i>r/m32</i> . |
| REX.W + 83 /3 <i>ib</i> | SBB <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Subtract with borrow sign-extended <i>imm8</i> from <i>r/m64</i> . |
| 18 /r | SBB <i>r/m8</i> , <i>r8</i> | Valid | Valid | Subtract with borrow <i>r8</i> from <i>r/m8</i> . |
| REX + 18 /r | SBB <i>r/m8*</i> , <i>r8</i> | Valid | N.E. | Subtract with borrow <i>r8</i> from <i>r/m8</i> . |
| 19 /r | SBB <i>r/m16</i> , <i>r16</i> | Valid | Valid | Subtract with borrow <i>r16</i> from <i>r/m16</i> . |
| 19 /r | SBB <i>r/m32</i> , <i>r32</i> | Valid | Valid | Subtract with borrow <i>r32</i> from <i>r/m32</i> . |
| REX.W + 19 /r | SBB <i>r/m64</i> , <i>r64</i> | Valid | N.E. | Subtract with borrow <i>r64</i> from <i>r/m64</i> . |

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|---------------|-----------------------|-------------|-----------------|---|
| 1A /r | SBB <i>r8, r/m8</i> | Valid | Valid | Subtract with borrow <i>r/m8</i> from <i>r8</i> . |
| REX + 1A /r | SBB <i>r8*, r/m8*</i> | Valid | N.E. | Subtract with borrow <i>r/m8</i> from <i>r8</i> . |
| 1B /r | SBB <i>r16, r/m16</i> | Valid | Valid | Subtract with borrow <i>r/m16</i> from <i>r16</i> . |
| 1B /r | SBB <i>r32, r/m32</i> | Valid | Valid | Subtract with borrow <i>r/m32</i> from <i>r32</i> . |
| REX.W + 1B /r | SBB <i>r64, r/m64</i> | Valid | N.E. | Subtract with borrow <i>r/m64</i> from <i>r64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Adds the source operand (second operand) and the carry (CF) flag, and subtracts the result from the destination operand (first operand). The result of the subtraction is stored in the destination operand. The destination operand can be a register or a memory location; the source operand can be an immediate, a register, or a memory location. (However, two memory operands cannot be used in one instruction.) The state of the CF flag represents a borrow from a previous subtraction.

When an immediate value is used as an operand, it is sign-extended to the length of the destination operand format.

The SBB instruction does not distinguish between signed or unsigned operands. Instead, the processor evaluates the result for both data types and sets the OF and CF flags to indicate a borrow in the signed or unsigned result, respectively. The SF flag indicates the sign of the signed result.

The SBB instruction is usually executed as part of a multibyte or multiword subtraction in which a SUB instruction is followed by a SBB instruction.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

DEST ← (DEST - (SRC + CF));

Flags Affected

The OF, SF, ZF, AF, PF, and CF flags are set according to the result.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

SCAS/SCASB/SCASW/SCASD—Scan String

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|------------|-----------------|-------------|-----------------|--|
| AE | SCAS <i>m8</i> | Valid | Valid | Compare AL with byte at ES:(E)DI or RDI, then set status flags.* |
| AF | SCAS <i>m16</i> | Valid | Valid | Compare AX with word at ES:(E)DI or RDI, then set status flags.* |
| AF | SCAS <i>m32</i> | Valid | Valid | Compare EAX with doubleword at ES:(E)DI or RDI then set status flags.* |
| REX.W + AF | SCAS <i>m64</i> | Valid | N.E. | Compare RAX with quadword at RDI or EDI then set status flags. |
| AE | SCASB | Valid | Valid | Compare AL with byte at ES:(E)DI or RDI then set status flags.* |
| AF | SCASW | Valid | Valid | Compare AX with word at ES:(E)DI or RDI then set status flags.* |
| AF | SCASD | Valid | Valid | Compare EAX with doubleword at ES:(E)DI or RDI then set status flags.* |
| REX.W + AF | SCASQ | Valid | N.E. | Compare RAX with quadword at RDI or EDI then set status flags. |

NOTES:

* In 64-bit mode, only 64-bit (RDI) and 32-bit (EDI) address sizes are supported. In non-64-bit mode, only 32-bit (EDI) and 16-bit (DI) address sizes are supported.

Description

In non-64-bit modes and in default 64-bit mode: this instruction compares a byte, word, doubleword or quadword specified using a memory operand with the value in AL, AX, or EAX. It then sets status flags in EFLAGS recording the results. The memory operand address is read from ES: (E)DI register (depending on the address-size attribute of the instruction and the current operational mode). Note that ES cannot be overridden with a segment override prefix.

At the assembly-code level, two forms of this instruction are allowed. The explicit-operand form and the no-operands form. The explicit-operand form (specified using the SCAS mnemonic) allows a memory operand to be specified explicitly. The memory operand must be a symbol that indicates the size and location of the operand value. The register operand is then automatically selected to match the size of the memory operand (AL register for byte comparisons, AX for word comparisons, EAX for doubleword comparisons). The explicit-operand form is provided to allow documentation. Note that the documentation provided by this form can be misleading. That is, the memory operand symbol must specify the correct type (size) of the operand (byte, word, or doubleword) but it does not have to specify the correct location. The location is always specified by ES: (E)DI.

The no-operands form of the instruction uses a short form of SCAS. Again, ES:(E)DI is assumed to be the memory operand and AL, AX, or EAX is assumed to be the register operand. The size of operands is selected by the mnemonic: SCASB (byte comparison), SCASW (word comparison), or SCASD (doubleword comparison).

After the comparison, the (E)DI register is incremented or decremented automatically according to the setting of the DF flag in the EFLAGS register. If the DF flag is 0, the (E)DI register is incremented; if the DF flag is 1, the (E)DI register is decremented. The register is incremented or decremented by 1 for byte operations, by 2 for word operations, and by 4 for doubleword operations.

SCAS, SCASB, SCASW, SCASD, and SCASQ can be preceded by the REP prefix for block comparisons of ECX bytes, words, doublewords, or quadwords. Often, however, these instructions will be used in a LOOP construct that takes some action based on the setting of status flags. See “REP/REPE/REPZ/REPNE/REPNZ—Repeat String Operation Prefix” in this chapter for a description of the REP prefix.

In 64-bit mode, the instruction’s default address size is 64-bits, 32-bit address size is supported using the prefix 67H. Using a REX prefix in the form of REX.W promotes operation on doubleword operand to 64 bits. The 64-bit no-operand mnemonic is SCASQ. Address of the memory operand is specified in either RDI or EDI, and AL/AX/EAX/RAX may be used as the register operand. After a comparison, the destination register is incremented or decremented by the current operand size (depending on the value of the DF flag). See the summary chart at the beginning of this section for encoding data and limits.

Operation

Non-64-bit Mode:

```

IF (Byte comparison)
    THEN
        temp ← AL – SRC;
        SetStatusFlags(temp);
        THEN IF DF = 0
            THEN (E)DI ← (E)DI + 1;
            ELSE (E)DI ← (E)DI - 1; FI;
    ELSE IF (Word comparison)
        THEN
            temp ← AX – SRC;
            SetStatusFlags(temp);
            IF DF = 0
                THEN (E)DI ← (E)DI + 2;
                ELSE (E)DI ← (E)DI - 2; FI;
        FI;
    ELSE IF (Doubleword comparison)
        THEN

```

INSTRUCTION SET REFERENCE, N-Z

```
temp ← EAX - SRC;
SetStatusFlags(temp);
IF DF = 0
    THEN (E)DI ← (E)DI + 4;
    ELSE (E)DI ← (E)DI - 4; FI;
FI;
```

64-bit Mode:

```
IF (Byte comparison)
    THEN
        temp ← AL - SRC;
        SetStatusFlags(temp);
        THEN IF DF = 0
            THEN (R)E)DI ← (R)E)DI + 1;
            ELSE (R)E)DI ← (R)E)DI - 1; FI;
    ELSE IF (Word comparison)
        THEN
            temp ← AX - SRC;
            SetStatusFlags(temp);
            IF DF = 0
                THEN (R)E)DI ← (R)E)DI + 2;
                ELSE (R)E)DI ← (R)E)DI - 2; FI;
        FI;
    ELSE IF (Doubleword comparison)
        THEN
            temp ← EAX - SRC;
            SetStatusFlags(temp);
            IF DF = 0
                THEN (R)E)DI ← (R)E)DI + 4;
                ELSE (R)E)DI ← (R)E)DI - 4; FI;
        FI;
    ELSE IF (Quadword comparison using REX.W)
        THEN
            temp ← RAX - SRC;
            SetStatusFlags(temp);
            IF DF = 0
                THEN (R)E)DI ← (R)E)DI + 8;
                ELSE (R)E)DI ← (R)E)DI - 8;
            FI;
    FI;
FI;
```

F

Flags Affected

The OF, SF, ZF, AF, PF, and CF flags are set according to the temporary result of the comparison.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the limit of the ES segment. If the ES register contains a NULL segment selector. If an illegal memory operand effective address in the ES segment is given. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|--------|--|
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

SETcc—Set Byte on Condition

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---------------------|-------------|---------------------|--|
| 0F 97 | SETA <i>r/m8</i> | Valid | Valid | Set byte if above (CF=0 and ZF=0). |
| REX + 0F 97 | SETA <i>r/m8</i> * | Valid | N.E. | Set byte if above (CF=0 and ZF=0). |
| 0F 93 | SETAE <i>r/m8</i> | Valid | Valid | Set byte if above or equal (CF=0). |
| REX + 0F 93 | SETAE <i>r/m8</i> * | Valid | N.E. | Set byte if above or equal (CF=0). |
| 0F 92 | SETB <i>r/m8</i> | Valid | Valid | Set byte if below (CF=1). |
| REX + 0F 92 | SETB <i>r/m8</i> * | Valid | N.E. | Set byte if below (CF=1). |
| 0F 96 | SETBE <i>r/m8</i> | Valid | Valid | Set byte if below or equal (CF=1 or ZF=1). |
| REX + 0F 96 | SETBE <i>r/m8</i> * | Valid | N.E. | Set byte if below or equal (CF=1 or ZF=1). |
| 0F 92 | SETC <i>r/m8</i> | Valid | Valid | Set byte if carry (CF=1). |
| REX + 0F 92 | SETC <i>r/m8</i> * | Valid | N.E. | Set byte if carry (CF=1). |
| 0F 94 | SETE <i>r/m8</i> | Valid | Valid | Set byte if equal (ZF=1). |
| REX + 0F 94 | SETE <i>r/m8</i> * | Valid | N.E. | Set byte if equal (ZF=1). |
| 0F 9F | SETG <i>r/m8</i> | Valid | Valid | Set byte if greater (ZF=0 and SF=0F). |
| REX + 0F 9F | SETG <i>r/m8</i> * | Valid | N.E. | Set byte if greater (ZF=0 and SF=0F). |
| 0F 9D | SETGE <i>r/m8</i> | Valid | Valid | Set byte if greater or equal (SF=0F). |
| REX + 0F 9D | SETGE <i>r/m8</i> * | Valid | N.E. | Set byte if greater or equal (SF=0F). |
| 0F 9C | SETL <i>r/m8</i> | Valid | Valid | Set byte if less (SF≠0F). |
| REX + 0F 9C | SETL <i>r/m8</i> * | Valid | N.E. | Set byte if less (SF≠0F). |
| 0F 9E | SETLE <i>r/m8</i> | Valid | Valid | Set byte if less or equal (ZF=1 or SF≠0F). |
| REX + 0F 9E | SETLE <i>r/m8</i> * | Valid | N.E. | Set byte if less or equal (ZF=1 or SF≠0F). |
| 0F 96 | SETNA <i>r/m8</i> | Valid | Valid | Set byte if not above (CF=1 or ZF=1). |
| REX + 0F 96 | SETNA <i>r/m8</i> * | Valid | N.E. | Set byte if not above (CF=1 or ZF=1). |

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|----------------------|-------------|------------------|---|
| 0F 92 | SETNAE <i>r/m8</i> | Valid | Valid | Set byte if not above or equal (CF=1). |
| REX + 0F 92 | SETNAE <i>r/m8</i> * | Valid | N.E. | Set byte if not above or equal (CF=1). |
| 0F 93 | SETNB <i>r/m8</i> | Valid | Valid | Set byte if not below (CF=0). |
| REX + 0F 93 | SETNB <i>r/m8</i> * | Valid | N.E. | Set byte if not below (CF=0). |
| 0F 97 | SETNBE <i>r/m8</i> | Valid | Valid | Set byte if not below or equal (CF=0 and ZF=0). |
| REX + 0F 97 | SETNBE <i>r/m8</i> * | Valid | N.E. | Set byte if not below or equal (CF=0 and ZF=0). |
| 0F 93 | SETNC <i>r/m8</i> | Valid | Valid | Set byte if not carry (CF=0). |
| REX + 0F 93 | SETNC <i>r/m8</i> * | Valid | N.E. | Set byte if not carry (CF=0). |
| 0F 95 | SETNE <i>r/m8</i> | Valid | Valid | Set byte if not equal (ZF=0). |
| REX + 0F 95 | SETNE <i>r/m8</i> * | Valid | N.E. | Set byte if not equal (ZF=0). |
| 0F 9E | SETNG <i>r/m8</i> | Valid | Valid | Set byte if not greater (ZF=1 or SF≠0F) |
| REX + 0F 9E | SETNG <i>r/m8</i> * | Valid | N.E. | Set byte if not greater (ZF=1 or SF≠0F). |
| 0F 9C | SETNGE <i>r/m8</i> | Valid | Valid | Set byte if not greater or equal (SF≠0F). |
| REX + 0F 9C | SETNGE <i>r/m8</i> * | Valid | N.E. | Set byte if not greater or equal (SF≠0F). |
| 0F 9D | SETNL <i>r/m8</i> | Valid | Valid | Set byte if not less (SF=0F). |
| REX + 0F 9D | SETNL <i>r/m8</i> * | Valid | N.E. | Set byte if not less (SF=0F). |
| 0F 9F | SETNLE <i>r/m8</i> | Valid | Valid | Set byte if not less or equal (ZF=0 and SF=0F). |
| REX + 0F 9F | SETNLE <i>r/m8</i> * | Valid | N.E. | Set byte if not less or equal (ZF=0 and SF=0F). |
| 0F 91 | SETNO <i>r/m8</i> | Valid | Valid | Set byte if not overflow (OF=0). |
| REX + 0F 91 | SETNO <i>r/m8</i> * | Valid | N.E. | Set byte if not overflow (OF=0). |
| 0F 9B | SETNP <i>r/m8</i> | Valid | Valid | Set byte if not parity (PF=0). |
| REX + 0F 9B | SETNP <i>r/m8</i> * | Valid | N.E. | Set byte if not parity (PF=0). |
| 0F 99 | SETNS <i>r/m8</i> | Valid | Valid | Set byte if not sign (SF=0). |
| REX + 0F 99 | SETNS <i>r/m8</i> * | Valid | N.E. | Set byte if not sign (SF=0). |
| 0F 95 | SETNZ <i>r/m8</i> | Valid | Valid | Set byte if not zero (ZF=0). |

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---------------------|-------------|------------------|---------------------------------|
| REX + 0F 95 | SETNZ <i>r/m8</i> * | Valid | N.E. | Set byte if not zero (ZF=0). |
| 0F 90 | SETO <i>r/m8</i> | Valid | Valid | Set byte if overflow (OF=1) |
| REX + 0F 90 | SETO <i>r/m8</i> * | Valid | N.E. | Set byte if overflow (OF=1). |
| 0F 9A | SETP <i>r/m8</i> | Valid | Valid | Set byte if parity (PF=1). |
| REX + 0F 9A | SETP <i>r/m8</i> * | Valid | N.E. | Set byte if parity (PF=1). |
| 0F 9A | SETPE <i>r/m8</i> | Valid | Valid | Set byte if parity even (PF=1). |
| REX + 0F 9A | SETPE <i>r/m8</i> * | Valid | N.E. | Set byte if parity even (PF=1). |
| 0F 9B | SETPO <i>r/m8</i> | Valid | Valid | Set byte if parity odd (PF=0). |
| REX + 0F 9B | SETPO <i>r/m8</i> * | Valid | N.E. | Set byte if parity odd (PF=0). |
| 0F 98 | SETS <i>r/m8</i> | Valid | Valid | Set byte if sign (SF=1). |
| REX + 0F 98 | SETS <i>r/m8</i> * | Valid | N.E. | Set byte if sign (SF=1). |
| 0F 94 | SETZ <i>r/m8</i> | Valid | Valid | Set byte if zero (ZF=1). |
| REX + 0F 94 | SETZ <i>r/m8</i> * | Valid | N.E. | Set byte if zero (ZF=1). |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Sets the destination operand to 0 or 1 depending on the settings of the status flags (CF, SF, OF, ZF, and PF) in the EFLAGS register. The destination operand points to a byte register or a byte in memory. The condition code suffix (*cc*) indicates the condition being tested for.

The terms “above” and “below” are associated with the CF flag and refer to the relationship between two unsigned integer values. The terms “greater” and “less” are associated with the SF and OF flags and refer to the relationship between two signed integer values.

Many of the SET*cc* instruction opcodes have alternate mnemonics. For example, SETG (set byte if greater) and SETNLE (set if not less or equal) have the same opcode and test for the same condition: ZF equals 0 and SF equals 0F. These alternate mnemonics are provided to make code more intelligible. Appendix B, “EFLAGS Condition Codes,” in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 1*, shows the alternate mnemonics for various test conditions.

Some languages represent a logical one as an integer with all bits set. This representation can be obtained by choosing the logically opposite condition for the SET*cc* instruction, then decrementing the result. For example, to test for overflow, use the SETNO instruction, then decrement the result.

In IA-64 mode, the operand size is fixed at 8 bits. Use of REX prefix enable uniform addressing to additional byte registers. Otherwise, this instruction's operation is the same as in legacy mode and compatibility mode.

Operation

IF condition
 THEN DEST ← 1;
 ELSE DEST ← 0;
 FI;

Flags Affected

None.

Protected Mode Exceptions

| | |
|------------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|------------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF (fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

SFENCE—Store Fence

| Opcode | Instruction | 64-Bit Mode | Compat /Leg Mode | Description |
|----------|-------------|-------------|------------------|------------------------------|
| OF AE /7 | SFENCE | Valid | Valid | Serializes store operations. |

Description

Performs a serializing operation on all store-to-memory instructions that were issued prior the SFENCE instruction. This serializing operation guarantees that every store instruction that precedes in program order the SFENCE instruction is globally visible before any store instruction that follows the SFENCE instruction is globally visible. The SFENCE instruction is ordered with respect store instructions, other SFENCE instructions, any MFENCE instructions, and any serializing instructions (such as the CPUID instruction). It is not ordered with respect to load instructions or the LFENCE instruction.

Weakly ordered memory types can be used to achieve higher processor performance through such techniques as out-of-order issue, write-combining, and write-collapsing. The degree to which a consumer of data recognizes or knows that the data is weakly ordered varies among applications and may be unknown to the producer of this data. The SFENCE instruction provides a performance-efficient way of insuring store ordering between routines that produce weakly-ordered results and routines that consume this data.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

Wait_On_Following_Stores_Until(preceding_stores_globally_visible);

Intel C/C++ Compiler Intrinsic Equivalent

`void _mm_sfence(void)`

Exceptions (All Operating Modes)

#UD If the LOCK prefix is used.

SGDT—Store Global Descriptor Table Register

| Opcode* | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|---------------|-------------|------------------|--------------------------|
| OF 01 /0 | SGDT <i>m</i> | Valid | Valid | Store GDTR to <i>m</i> . |

NOTES:

* See IA-32 Architecture Compatibility section below.

Description

Stores the content of the global descriptor table register (GDTR) in the destination operand. The destination operand specifies a memory location.

In legacy or compatibility mode, the destination operand is a 6-byte memory location. If the operand-size attribute is 16 bits, the limit is stored in the low 2 bytes and the 24-bit base address is stored in bytes 3-5, and byte 6 is zero-filled. If the operand-size attribute is 32 bits, the 16-bit limit field of the register is stored in the low 2 bytes of the memory location and the 32-bit base address is stored in the high 4 bytes.

In IA-32e mode, the operand size is fixed at 8+2 bytes. The instruction stores an 8-byte base and a 2-byte limit.

SGDT is useful only by operating-system software. However, it can be used in application programs without causing an exception to be generated. See “LGDT/LIDT—Load Global/Interrupt Descriptor Table Register” in Chapter 3, *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A*, for information on loading the GDTR and IDTR.

IA-32 Architecture Compatibility

The 16-bit form of the SGDT is compatible with the Intel 286 processor if the upper 8 bits are not referenced. The Intel 286 processor fills these bits with 1s; the Pentium 4, Intel Xeon, P6 processor family, Pentium, Intel486, and Intel386™ processors fill these bits with 0s.

Operation

IF instruction is SGDT

IF OperandSize = 16

THEN

DEST[0:15] ← GDTR(Limit);

DEST[16:39] ← GDTR(Base); (* 24 bits of base address stored *)

DEST[40:47] ← 0;

ELSE IF (32-bit Operand Size)

DEST[0:15] ← GDTR(Limit);

DEST[16:47] ← GDTR(Base); (* Full 32-bit base address stored *)

```

        FI;
    ELSE (* 64-bit Operand Size *)
        DEST[0:15] ← GDTR(Limit);
        DEST[16:79] ← GDTR(Base); (* Full 64-bit base address stored *)
    FI;
FI;

```

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #UD | If the destination operand is a register. If the LOCK prefix is used. |
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | If the destination operand is a register. If the LOCK prefix is used. |
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #UD | If the destination operand is a register. If the LOCK prefix is used. |
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |

#AC(0) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#UD If the destination operand is a register.
If the LOCK prefix is used.

#GP(0) If the memory address is in a non-canonical form.

#PF(fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

SHLD—Double Precision Shift Left

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|---------------|------------------------------|-------------|-----------------|--|
| OF A4 | SHLD <i>r/m16, r16, imm8</i> | Valid | Valid | Shift <i>r/m16</i> to left <i>imm8</i> places while shifting bits from <i>r16</i> in from the right. |
| OF A5 | SHLD <i>r/m16, r16, CL</i> | Valid | Valid | Shift <i>r/m16</i> to left CL places while shifting bits from <i>r16</i> in from the right. |
| OF A4 | SHLD <i>r/m32, r32, imm8</i> | Valid | Valid | Shift <i>r/m32</i> to left <i>imm8</i> places while shifting bits from <i>r32</i> in from the right. |
| REX.W + OF A4 | SHLD <i>r/m64, r64, imm8</i> | Valid | N.E. | Shift <i>r/m64</i> to left <i>imm8</i> places while shifting bits from <i>r64</i> in from the right. |
| OF A5 | SHLD <i>r/m32, r32, CL</i> | Valid | Valid | Shift <i>r/m32</i> to left CL places while shifting bits from <i>r32</i> in from the right. |
| REX.W + OF A5 | SHLD <i>r/m64, r64, CL</i> | Valid | N.E. | Shift <i>r/m64</i> to left CL places while shifting bits from <i>r64</i> in from the right. |

Description

The SHLD instruction is used for multi-precision shifts of 64 bits or more.

The instruction shifts the first operand (destination operand) to the left the number of bits specified by the third operand (count operand). The second operand (source operand) provides bits to shift in from the right (starting with bit 0 of the destination operand).

The destination operand can be a register or a memory location; the source operand is a register. The count operand is an unsigned integer that can be stored in an immediate byte or in the CL register. If the count operand is CL, the shift count is the logical AND of CL and a count mask. In non-64-bit modes and default 64-bit mode; only bits 0 through 4 of the count are used. This masks the count to a value between 0 and 31. If a count is greater than the operand size, the result is undefined.

If the count is 1 or greater, the CF flag is filled with the last bit shifted out of the destination operand. For a 1-bit shift, the OF flag is set if a sign change occurred; otherwise, it is cleared. If the count operand is 0, flags are not affected.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits (upgrading the count mask

to 6 bits). See the summary chart at the beginning of this section for encoding data and limits.

Operation

```

IF (In 64-Bit Mode and REX.W = 1)
    THEN COUNT ← COUNT MOD 64;
    ELSE COUNT ← COUNT MOD 32;
FI
SIZE ← OperandSize;
IF COUNT = 0
    THEN
        No operation;
    ELSE
        IF COUNT > SIZE
            THEN (* Bad parameters *)
                DEST is undefined;
                CF, OF, SF, ZF, AF, PF are undefined;
            ELSE (* Perform the shift *)
                CF ← BIT[DEST, SIZE - COUNT];
                (* Last bit shifted out on exit *)
                FOR i ← SIZE - 1 DOWN TO COUNT
                    DO
                        Bit(DEST, i) ← Bit(DEST, i - COUNT);
                    OD;
                FOR i ← COUNT - 1 DOWN TO 0
                    DO
                        BIT[DEST, i] ← BIT[SRC, i - COUNT + SIZE];
                    OD;
            FI;
        FI;
FI;

```

Flags Affected

If the count is 1 or greater, the CF flag is filled with the last bit shifted out of the destination operand and the SF, ZF, and PF flags are set according to the value of the result. For a 1-bit shift, the OF flag is set if a sign change occurred; otherwise, it is cleared. For shifts greater than 1 bit, the OF flag is undefined. If a shift occurs, the AF flag is undefined. If the count operand is 0, the flags are not affected. If the count is greater than the operand size, the flags are undefined.

Protected Mode Exceptions

#GP(0) If the destination is located in a non-writable segment.

| | |
|-----------------|--|
| | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| | If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

SHRD—Double Precision Shift Right

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|---------------|---|-------------|-----------------|--|
| OF AC | SHRD <i>r/m16</i> , <i>r16</i> , <i>imm8</i> | Valid | Valid | Shift <i>r/m16</i> to right <i>imm8</i> places while shifting bits from <i>r16</i> in from the left. |
| OF AD | SHRD <i>r/m16</i> , <i>r16</i> , CL | Valid | Valid | Shift <i>r/m16</i> to right CL places while shifting bits from <i>r16</i> in from the left. |
| OF AC | SHRD <i>r/m32</i> , <i>r32</i> , <i>imm8</i> | Valid | Valid | Shift <i>r/m32</i> to right <i>imm8</i> places while shifting bits from <i>r32</i> in from the left. |
| REX.W + OF AC | SHRD <i>r/m64</i> , <i>r64</i> , <i>imm8</i> | Valid | N.E. | Shift <i>r/m64</i> to right <i>imm8</i> places while shifting bits from <i>r64</i> in from the left. |
| OF AD | SHRD <i>r/m32</i> , <i>r32</i> , CL | Valid | Valid | Shift <i>r/m32</i> to right CL places while shifting bits from <i>r32</i> in from the left. |
| REX.W + OF AD | SHRD <i>r/m64</i> , <i>r64</i> , CL | Valid | N.E. | Shift <i>r/m64</i> to right CL places while shifting bits from <i>r64</i> in from the left. |

Description

The SHRD instruction is useful for multi-precision shifts of 64 bits or more.

The instruction shifts the first operand (destination operand) to the right the number of bits specified by the third operand (count operand). The second operand (source operand) provides bits to shift in from the left (starting with the most significant bit of the destination operand).

The destination operand can be a register or a memory location; the source operand is a register. The count operand is an unsigned integer that can be stored in an immediate byte or the CL register. If the count operand is CL, the shift count is the logical AND of CL and a count mask. In non-64-bit modes and default 64-bit mode, the width of the count mask is 5 bits. Only bits 0 through 4 of the count register are used (masking the count to a value between 0 and 31). If the count is greater than the operand size, the result is undefined.

If the count is 1 or greater, the CF flag is filled with the last bit shifted out of the destination operand. For a 1-bit shift, the OF flag is set if a sign change occurred; otherwise, it is cleared. If the count operand is 0, flags are not affected.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits (upgrading the count mask

to 6 bits). See the summary chart at the beginning of this section for encoding data and limits.

Operation

```

IF (In 64-Bit Mode and REX.W = 1)
    THEN COUNT ← COUNT MOD 64;
    ELSE COUNT ← COUNT MOD 32;
FI
SIZE ← OperandSize;
IF COUNT = 0
    THEN
        No operation;
    ELSE
        IF COUNT > SIZE
            THEN (* Bad parameters *)
                DEST is undefined;
                CF, OF, SF, ZF, AF, PF are undefined;
            ELSE (* Perform the shift *)
                CF ← BIT[DEST, COUNT - 1]; (* Last bit shifted out on exit *)
                FOR i ← 0 TO SIZE - 1 - COUNT
                    DO
                        BIT[DEST, i] ← BIT[DEST, i + COUNT];
                    OD;
                FOR i ← SIZE - COUNT TO SIZE - 1
                    DO
                        BIT[DEST, i] ← BIT[DEST, i + COUNT - SIZE];
                    OD;
            FI;
        FI;

```

Flags Affected

If the count is 1 or greater, the CF flag is filled with the last bit shifted out of the destination operand and the SF, ZF, and PF flags are set according to the value of the result. For a 1-bit shift, the OF flag is set if a sign change occurred; otherwise, it is cleared. For shifts greater than 1 bit, the OF flag is undefined. If a shift occurs, the AF flag is undefined. If the count operand is 0, the flags are not affected. If the count is greater than the operand size, the flags are undefined.

Protected Mode Exceptions

#GP(0) If the destination is located in a non-writable segment.
 If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.

| | |
|-----------------|--|
| | If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

SHUFPD—Shuffle Packed Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------------|--|-------------|-----------------|--|
| 66 0F C6 /r ib | SHUFPD <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Shuffle packed double-precision floating-point values selected by <i>imm8</i> from <i>xmm1</i> and <i>xmm2/m128</i> to <i>xmm1</i> . |

Description

Moves either of the two packed double-precision floating-point values from destination operand (first operand) into the low quadword of the destination operand; moves either of the two packed double-precision floating-point values from the source operand into to the high quadword of the destination operand (see Figure 4-14). The select operand (third operand) determines which values are moved to the destination operand.

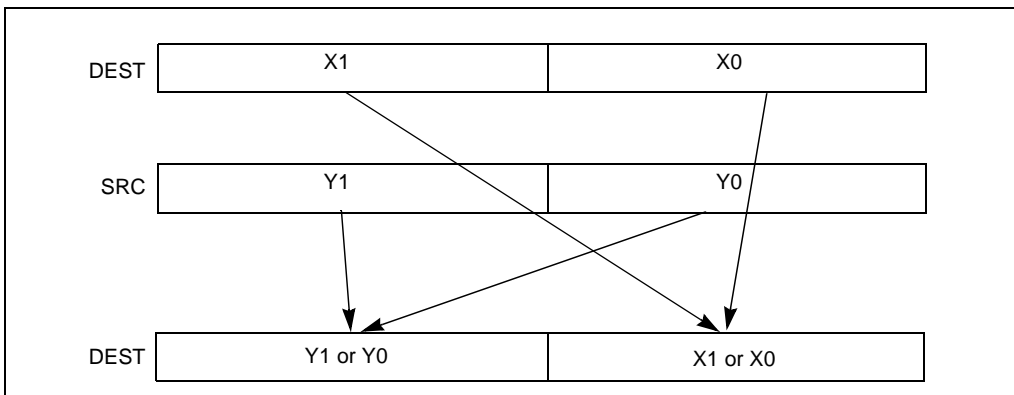


Figure 4-14. SHUFPD Shuffle Operation

The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. The select operand is an 8-bit immediate: bit 0 selects which value is moved from the destination operand to the result (where 0 selects the low quadword and 1 selects the high quadword) and bit 1 selects which value is moved from the source operand to the result. Bits 2 through 7 of the select operand are reserved and must be set to 0.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
IF SELECT[0] = 0
    THEN DEST[63:0] ← DEST[63:0];
    ELSE DEST[63:0] ← DEST[127:64]; FI;
```

```
IF SELECT[1] = 0
    THEN DEST[127:64] ← SRC[63:0];
    ELSE DEST[127:64] ← SRC[127:64]; FI;
```

Intel C/C++ Compiler Intrinsic Equivalent

```
SHUFPD  __m128d _mm_shuffle_pd(__m128d a, __m128d b, unsigned int imm8)
```

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If memory operand is not aligned on a 16-byte boundary, regardless of segment.

If the memory address is in a non-canonical form.

#PF(fault-code) For a page fault.

#NM If CR0.TS[bit 3] = 1.

#UD If CR0.EM[bit 2] = 1.

If CR4.OSFXSR[bit 9] = 0.

If CPUID.01H: EDX.SSE2[bit 26] = 0.

If the LOCK prefix is used.

SHUFPS—Shuffle Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 0F C6 /r ib | SHUFPS <i>xmm1</i> , <i>xmm2/m128</i> , <i>imm8</i> | Valid | Valid | Shuffle packed single-precision floating-point values selected by <i>imm8</i> from <i>xmm1</i> and <i>xmm1/m128</i> to <i>xmm1</i> . |

Description

Moves two of the four packed single-precision floating-point values from the destination operand (first operand) into the low quadword of the destination operand; moves two of the four packed single-precision floating-point values from the source operand (second operand) into to the high quadword of the destination operand (see Figure 4-15). The select operand (third operand) determines which values are moved to the destination operand.

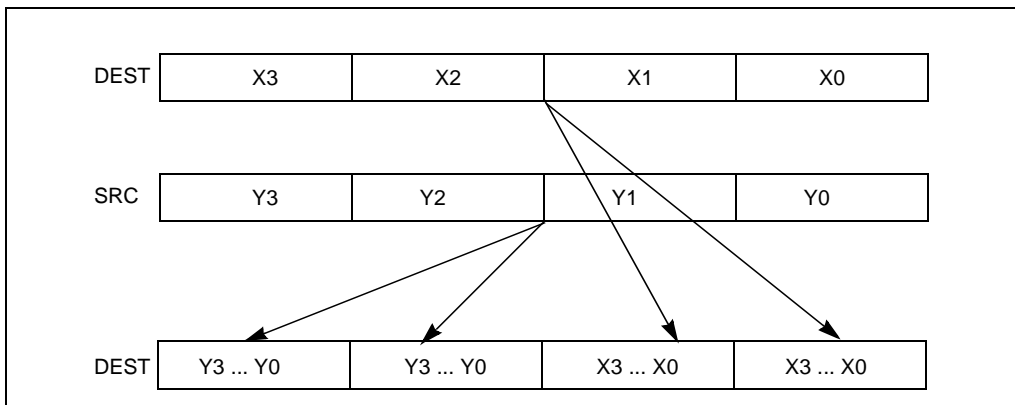


Figure 4-15. SHUFPS Shuffle Operation

The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. The select operand is an 8-bit immediate: bits 0 and 1 select the value to be moved from the destination operand to the low doubleword of the result, bits 2 and 3 select the value to be moved from the destination operand to the second doubleword of the result, bits 4 and 5 select the value to be moved from the source operand to the third doubleword of the result, and bits 6 and 7 select the value to be moved from the source operand to the high doubleword of the result.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

CASE (SELECT[1:0]) OF

- 0: DEST[31:0] ← DEST[31:0];
- 1: DEST[31:0] ← DEST[63:32];
- 2: DEST[31:0] ← DEST[95:64];
- 3: DEST[31:0] ← DEST[127:96];

ESAC;

CASE (SELECT[3:2]) OF

- 0: DEST[63:32] ← DEST[31:0];
- 1: DEST[63:32] ← DEST[63:32];
- 2: DEST[63:32] ← DEST[95:64];
- 3: DEST[63:32] ← DEST[127:96];

ESAC;

CASE (SELECT[5:4]) OF

- 0: DEST[95:64] ← SRC[31:0];
- 1: DEST[95:64] ← SRC[63:32];
- 2: DEST[95:64] ← SRC[95:64];
- 3: DEST[95:64] ← SRC[127:96];

ESAC;

CASE (SELECT[7:6]) OF

- 0: DEST[127:96] ← SRC[31:0];
- 1: DEST[127:96] ← SRC[63:32];
- 2: DEST[127:96] ← SRC[95:64];
- 3: DEST[127:96] ← SRC[127:96];

ESAC;

Intel C/C++ Compiler Intrinsic Equivalent

SHUFFPS __m128 __mm_shuffle_ps(__m128 a, __m128 b, unsigned int imm8)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.
- #PF(fault-code) For a page fault.

| | |
|-----|--|
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If memory operand is not aligned on a 16-byte boundary, regardless of segment. If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

SIDT—Store Interrupt Descriptor Table Register

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|---------------|-------------|------------------|--------------------------|
| OF 01 /1 | SIDT <i>m</i> | Valid | Valid | Store IDTR to <i>m</i> . |

Description

Stores the content the interrupt descriptor table register (IDTR) in the destination operand. The destination operand specifies a 6-byte memory location.

In non-64-bit modes, if the operand-size attribute is 32 bits, the 16-bit limit field of the register is stored in the low 2 bytes of the memory location and the 32-bit base address is stored in the high 4 bytes. If the operand-size attribute is 16 bits, the limit is stored in the low 2 bytes and the 24-bit base address is stored in the third, fourth, and fifth byte, with the sixth byte filled with 0s.

In 64-bit mode, the operand size fixed at 8+2 bytes. The instruction stores 8-byte base and 2-byte limit values.

SIDT is only useful in operating-system software; however, it can be used in application programs without causing an exception to be generated. See “LGDT/LIDT—Load Global/Interrupt Descriptor Table Register” in Chapter 3, *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A*, for information on loading the GDTR and IDTR.

IA-32 Architecture Compatibility

The 16-bit form of SIDT is compatible with the Intel 286 processor if the upper 8 bits are not referenced. The Intel 286 processor fills these bits with 1s; the Pentium 4, Intel Xeon, P6 processor family, Pentium, Intel486, and Intel386 processors fill these bits with 0s.

Operation

IF instruction is SIDT

THEN

IF OperandSize = 16

THEN

DEST[0:15] ← IDTR(Limit);

DEST[16:39] ← IDTR(Base); (* 24 bits of base address stored; *)

DEST[40:47] ← 0;

ELSE IF (32-bit Operand Size)

DEST[0:15] ← IDTR(Limit);

DEST[16:47] ← IDTR(Base); FI; (* Full 32-bit base address stored *)

ELSE (* 64-bit Operand Size *)

DEST[0:15] ← IDTR(Limit);

DEST[16:79] ← IDTR(Base); (* Full 64-bit base address stored *)

FI;

FI;

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #UD | If the destination operand is a register. If the LOCK prefix is used. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

SLDT—Store Local Descriptor Table Register

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|------------------|---------------------|-------------|-----------------|---|
| 0F 00 /0 | SLDT <i>r/m16</i> | Valid | Valid | Stores segment selector from LDTR in <i>r/m16</i> . |
| REX.W + 0F 00 /0 | SLDT <i>r64/m16</i> | Valid | Valid | Stores segment selector from LDTR in <i>r64/m16</i> . |

Description

Stores the segment selector from the local descriptor table register (LDTR) in the destination operand. The destination operand can be a general-purpose register or a memory location. The segment selector stored with this instruction points to the segment descriptor (located in the GDT) for the current LDT. This instruction can only be executed in protected mode.

Outside IA-32e mode, when the destination operand is a 32-bit register, the 16-bit segment selector is copied into the low-order 16 bits of the register. The high-order 16 bits of the register are cleared for the Pentium 4, Intel Xeon, and P6 family processors. They are undefined for Pentium, Intel486, and Intel386 processors. When the destination operand is a memory location, the segment selector is written to memory as a 16-bit quantity, regardless of the operand size.

In compatibility mode, when the destination operand is a 32-bit register, the 16-bit segment selector is copied into the low-order 16 bits of the register. The high-order 16 bits of the register are cleared. When the destination operand is a memory location, the segment selector is written to memory as a 16-bit quantity, regardless of the operand size.

In 64-bit mode, using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). The behavior of SLDT with a 64-bit register is to zero-extend the 16-bit selector and store it in the register. If the destination is memory and operand size is 64, SLDT will write the 16-bit selector to memory as a 16-bit quantity, regardless of the operand size.

Operation

DEST ← LDTR(SegmentSelector);

Flags Affected

None.

Protected Mode Exceptions

#GP(0) If the destination is located in a non-writable segment.

| | |
|-----------------|--|
| | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| | If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | The SLDT instruction is not recognized in real-address mode. If the LOCK prefix is used. |
|-----|---|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | The SLDT instruction is not recognized in virtual-8086 mode. If the LOCK prefix is used. |
|-----|---|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

SMSW—Store Machine Status Word

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------------|---------------------|-------------|------------------|--|
| OF 01 /4 | SMSW <i>r/m16</i> | Valid | Valid | Store machine status word to <i>r/m16</i> . |
| OF 01 /4 | SMSW <i>r32/m16</i> | Valid | Valid | Store machine status word in low-order 16 bits of <i>r32/m16</i> ; high-order 16 bits of <i>r32</i> are undefined. |
| REX.W + OF 01 /4 | SMSW <i>r64/m16</i> | Valid | Valid | Store machine status word in low-order 16 bits of <i>r64/m16</i> ; high-order 16 bits of <i>r32</i> are undefined. |

Description

Stores the machine status word (bits 0 through 15 of control register CR0) into the destination operand. The destination operand can be a general-purpose register or a memory location.

In non-64-bit modes, when the destination operand is a 32-bit register, the low-order 16 bits of register CR0 are copied into the low-order 16 bits of the register and the high-order 16 bits are undefined. When the destination operand is a memory location, the low-order 16 bits of register CR0 are written to memory as a 16-bit quantity, regardless of the operand size.

In 64-bit mode, the behavior of the SMSW instruction is defined by the following examples:

- SMSW *r16* operand size 16, store CR0[15:0] in *r16*
- SMSW *r32* operand size 32, zero-extend CR0[31:0], and store in *r32*
- SMSW *r64* operand size 64, zero-extend CR0[63:0], and store in *r64*
- SMSW *m16* operand size 16, store CR0[15:0] in *m16*
- SMSW *m16* operand size 32, store CR0[15:0] in *m16* (not *m32*)
- SMSW *m16* operands size 64, store CR0[15:0] in *m16* (not *m64*)

SMSW is only useful in operating-system software. However, it is not a privileged instruction and can be used in application programs. The is provided for compatibility with the Intel 286 processor. Programs and procedures intended to run on the Pentium 4, Intel Xeon, P6 family, Pentium, Intel486, and Intel386 processors should use the MOV (control registers) instruction to load the machine status word.

See “Changes to Instruction Behavior in VMX Non-Root Operation” in Chapter 21 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*, for more information about the behavior of this instruction in VMX non-root operation.

Operation

DEST ← CRO[15:0];

(* Machine status word *)

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|--------|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

SQRTPD—Compute Square Roots of Packed Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--|-------------|-----------------|--|
| 66 0F 51 /r | SQRTPD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Computes square roots of the packed double-precision floating-point values in <i>xmm2/m128</i> and stores the results in <i>xmm1</i> . |

Description

Performs a SIMD computation of the square roots of the two packed double-precision floating-point values in the source operand (second operand) stores the packed double-precision floating-point results in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. See Figure 11-3 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD double-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[63:0] ← SQRT(SRC[63:0]);
DEST[127:64] ← SQRT(SRC[127:64]);
```

Intel C/C++ Compiler Intrinsic Equivalent

```
SQRTPD   __m128d _mm_sqrt_pd (m128d a)
```

SIMD Floating-Point Exceptions

Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |

| | |
|-----|---|
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0.CR4.OSXMMEXCPT(bit 10) is 1. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |

INSTRUCTION SET REFERENCE, N-Z

| | |
|-----|---|
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

SQRTPS—Compute Square Roots of Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|--|-------------|-----------------|--|
| OF 51 /r | SQRTPS <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Computes square roots of the packed single-precision floating-point values in <i>xmm2/m128</i> and stores the results in <i>xmm1</i> . |

Description

Performs a SIMD computation of the square roots of the four packed single-precision floating-point values in the source operand (second operand) stores the packed single-precision floating-point results in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. See Figure 10-5 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD single-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[31:0] ← SQRT(SRC[31:0]);
DEST[63:32] ← SQRT(SRC[63:32]);
DEST[95:64] ← SQRT(SRC[95:64]);
DEST[127:96] ← SQRT(SRC[127:96]);
```

Intel C/C++ Compiler Intrinsic Equivalent

```
SQRTPS __m128 _mm_sqrt_ps(__m128 a)
```

SIMD Floating-Point Exceptions

Invalid, Precision, Denormal.

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.
- #PF(fault-code) For a page fault.

| | |
|-----|--|
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |

| | |
|-----|--|
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

SQRTSD—Compute Square Root of Scalar Double-Precision Floating-Point Value

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|---|-------------|-----------------|--|
| F2 0F 51 /r | SQRTSD <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Computes square root of the low double-precision floating-point value in <i>xmm2/m64</i> and stores the results in <i>xmm1</i> . |

Description

Computes the square root of the low double-precision floating-point value in the source operand (second operand) and stores the double-precision floating-point result in the destination operand. The source operand can be an XMM register or a 64-bit memory location. The destination operand is an XMM register. The high quadword of the destination operand remains unchanged. See Figure 11-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a scalar double-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[63:0] ← SQRT(SRC[63:0]);
(* DEST[127:64] unchanged *)

Intel C/C++ Compiler Intrinsic Equivalent

SQRTSD `__m128d _mm_sqrt_sd(m128d a, m128d b)`

SIMD Floating-Point Exceptions

Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|--------|--|
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

Real-Address Mode Exceptions

| | |
|-----|--|
| GP | <p>If any part of the operand lies outside the effective address space from 0 to FFFFH.</p> |
| #NM | <p>If CR0.TS[bit 3] = 1.</p> |
| #XM | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1.</p> |
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|--|
| #PF(fault-code) | <p>For a page fault.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made.</p> |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | <p>If a memory address referencing the SS segment is in a non-canonical form.</p> |
| #GP(0) | <p>If the memory address is in a non-canonical form.</p> |
| #PF(fault-code) | <p>For a page fault.</p> |
| #NM | <p>If CR0.TS[bit 3] = 1.</p> |
| #XM | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1.</p> |

| | |
|--------|--|
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

SQRTSS—Compute Square Root of Scalar Single-Precision Floating-Point Value

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|---|-------------|-----------------|--|
| F3 0F 51 /r | SQRTSS <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Computes square root of the low single-precision floating-point value in <i>xmm2/m32</i> and stores the results in <i>xmm1</i> . |

Description

Computes the square root of the low single-precision floating-point value in the source operand (second operand) and stores the single-precision floating-point result in the destination operand. The source operand can be an XMM register or a 32-bit memory location. The destination operand is an XMM register. The three high-order doublewords of the destination operand remain unchanged. See Figure 10-6 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a scalar single-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[31:0] ← SQRT (SRC[31:0]);
(* DEST[127:64] unchanged *)

Intel C/C++ Compiler Intrinsic Equivalent

SQRTSS `__m128_mm_sqrt_ss(__m128 a)`

SIMD Floating-Point Exceptions

Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|--------|--|
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|--|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|--------|---|
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE[bit 25] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

STC—Set Carry Flag

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|--------------|
| F9 | STC | Valid | Valid | Set CF flag. |

Description

Sets the CF flag in the EFLAGS register.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

$CF \leftarrow 1$;

Flags Affected

The CF flag is set. The OF, ZF, SF, AF, and PF flags are unaffected.

Exceptions (All Operating Modes)

#UD If the LOCK prefix is used.

STD—Set Direction Flag

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|--------------|
| FD | STD | Valid | Valid | Set DF flag. |

Description

Sets the DF flag in the EFLAGS register. When the DF flag is set to 1, string operations decrement the index registers (ESI and/or EDI).

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

$DF \leftarrow 1$;

Flags Affected

The DF flag is set. The CF, OF, ZF, SF, AF, and PF flags are unaffected.

Exceptions (All Operating Modes)

#UD If the LOCK prefix is used.

STI—Set Interrupt Flag

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|---------------------|---|
| FB | STI | Valid | Valid | Set interrupt flag; external, maskable interrupts enabled at the end of the next instruction. |

Description

If protected-mode virtual interrupts are not enabled, STI sets the interrupt flag (IF) in the EFLAGS register. After the IF flag is set, the processor begins responding to external, maskable interrupts after the next instruction is executed. The delayed effect of this instruction is provided to allow interrupts to be enabled just before returning from a procedure (or subroutine). For instance, if an STI instruction is followed by an RET instruction, the RET instruction is allowed to execute before external interrupts are recognized¹. If the STI instruction is followed by a CLI instruction (which clears the IF flag), the effect of the STI instruction is negated.

The IF flag and the STI and CLI instructions do not prohibit the generation of exceptions and NMI interrupts. NMI interrupts (and SMIs) may be blocked for one macro-instruction following an STI.

When protected-mode virtual interrupts are enabled, CPL is 3, and IOPL is less than 3; STI sets the VIF flag in the EFLAGS register, leaving IF unaffected.

Table 4-5 indicates the action of the STI instruction depending on the processor's mode of operation and the CPL/IOPL settings of the running program or procedure.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Table 4-5. Decision Table for STI Results

| PE | VM | IOPL | CPL | PVI | VIP | VME | STI Result |
|----|----|-------|-----|-----|-----|-----|-----------------|
| 0 | X | X | X | X | X | X | IF = 1 |
| 1 | 0 | ≥ CPL | X | X | X | X | IF = 1 |
| 1 | 0 | < CPL | 3 | 1 | 0 | X | VIF = 1 |
| 1 | 0 | < CPL | < 3 | X | X | X | GP Fault |

1. The STI instruction delays recognition of interrupts only if it is executed with EFLAGS.IF = 0. In a sequence of STI instructions, only the first instruction in the sequence is guaranteed to delay interrupts.

In the following instruction sequence, interrupts may be recognized before RET executes:

```
STI
STI
RET
```


Table 4-5. Decision Table for STI Results

| PE | VM | IOPL | CPL | PVI | VIP | VME | STI Result |
|----|----|-------|-----|-----|-----|-----|------------|
| 1 | 0 | < CPL | X | 0 | X | X | GP Fault |
| 1 | 0 | < CPL | X | X | 1 | X | GP Fault |
| 1 | 1 | 3 | X | X | X | X | IF = 1 |
| 1 | 1 | < 3 | X | X | 0 | 1 | VIF = 1 |
| 1 | 1 | < 3 | X | X | 1 | X | GP Fault |
| 1 | 1 | < 3 | X | X | X | 0 | GP Fault |

NOTES:

X = This setting has no impact.

Operation

IF PE = 0 (* Executing in real-address mode *)

THEN

$\underline{IF} \leftarrow 1$; (* Set Interrupt Flag *)

ELSE (* Executing in protected mode or virtual-8086 mode *)

IF VM = 0 (* Executing in protected mode*)

THEN

IF IOPL \geq CPL

THEN

$\underline{IF} \leftarrow 1$; (* Set Interrupt Flag *)

ELSE

IF (IOPL < CPL) and (CPL = 3) and (VIP = 0)

THEN

$\underline{VIF} \leftarrow 1$; (* Set Virtual Interrupt Flag *)

ELSE

#GP(0);

FI;

FI;

ELSE (* Executing in Virtual-8086 mode *)

IF IOPL = 3

THEN

$\underline{IF} \leftarrow 1$; (* Set Interrupt Flag *)

ELSE

IF ((IOPL < 3) and (VIP = 0) and (VME = 1))

THEN

$\underline{VIF} \leftarrow 1$; (* Set Virtual Interrupt Flag *)

ELSE

#GP(0); (* Trap to virtual-8086 monitor *)

FI;)

FI;

FI;
FI;

Flags Affected

The IF flag is set to 1; or the VIF flag is set to 1.

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | If the CPL is greater (has less privilege) than the IOPL of the current program or procedure. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|-----------------------------|
| #UD | If the LOCK prefix is used. |
|-----|-----------------------------|

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

STMXCSR—Store MXCSR Register State

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|--------------------|-------------|-----------------|--|
| 0F AE /3 | STMXCSR <i>m32</i> | Valid | Valid | Store contents of MXCSR register to <i>m32</i> . |

Description

Stores the contents of the MXCSR control and status register to the destination operand. The destination operand is a 32-bit memory location. The reserved bits in the MXCSR register are stored as 0s.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

$m32 \leftarrow \text{MXCSR}$;

Intel C/C++ Compiler Intrinsic Equivalent

`_mm_getcsr(void)`

Exceptions

None.

Numeric Exceptions

None.

Protected Mode Exceptions

| | |
|------------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS, or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #UD | If CR0.EM[bit 2] = 1. |
| #NM | If CR0.TS[bit 3] = 1. |
| #AC | For unaligned memory reference. To enable #AC exceptions, three conditions must be true: CR0.AM[bit 18] = 1, EFLAGS.AC[bit 18] = 1, current CPL = 3. |
| #UD | If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real Address Mode Exceptions

| | |
|-------|---|
| GP(0) | If any part of the operand would lie outside of the effective address space from 0 to 0FFFFH. |
| #UD | If CR0.EM[bit 2] = 1. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual 8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---------------------------------|
| #PF(fault-code) | For a page fault. |
| #AC | For unaligned memory reference. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #AC | For unaligned memory reference. To enable #AC exceptions, three conditions must be true: CR0.AM[bit 18] = 1, EFLAGS.AC[bit 18] = 1, current CPL = 3 |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

STOS/STOSB/STOSW/STOSD/STOSQ—Store String

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------|-----------------|-------------|------------------|--|
| AA | STOS <i>m8</i> | Valid | Valid | For legacy mode, store AL at address ES:(E)DI; For 64-bit mode store AL at address RDI or EDI. |
| AB | STOS <i>m16</i> | Valid | Valid | For legacy mode, store AX at address ES:(E)DI; For 64-bit mode store AX at address RDI or EDI. |
| AB | STOS <i>m32</i> | Valid | Valid | For legacy mode, store EAX at address ES:(E)DI; For 64-bit mode store EAX at address RDI or EDI. |
| REX.W + AB | STOS <i>m64</i> | Valid | N.E. | Store RAX at address RDI or EDI. |
| AA | STOSB | Valid | Valid | For legacy mode, store AL at address ES:(E)DI; For 64-bit mode store AL at address RDI or EDI. |
| AB | STOSW | Valid | Valid | For legacy mode, store AX at address ES:(E)DI; For 64-bit mode store AX at address RDI or EDI. |
| AB | STOSD | Valid | Valid | For legacy mode, store EAX at address ES:(E)DI; For 64-bit mode store EAX at address RDI or EDI. |
| REX.W + AB | STOSQ | Valid | N.E. | Store RAX at address RDI or EDI. |

Description

In non-64-bit and default 64-bit mode; stores a byte, word, or doubleword from the AL, AX, or EAX register (respectively) into the destination operand. The destination operand is a memory location, the address of which is read from either the ES:EDI or ES:DI register (depending on the address-size attribute of the instruction and the mode of operation). The ES segment cannot be overridden with a segment override prefix.

At the assembly-code level, two forms of the instruction are allowed: the “explicit-operands” form and the “no-operands” form. The explicit-operands form (specified with the STOS mnemonic) allows the destination operand to be specified explicitly. Here, the destination operand should be a symbol that indicates the size and location of the destination value. The source operand is then automatically selected to match the size of the destination operand (the AL register for byte operands, AX for word operands, EAX for doubleword operands). The explicit-operands form is provided to allow documentation; however, note that the documentation provided by this form can be misleading. That is, the destination operand symbol must specify the correct **type** (size) of the operand (byte, word, or doubleword), but it does not have to specify the correct **location**. The location is always specified by the ES: (E)DI

register. These must be loaded correctly before the store string instruction is executed.

The no-operands form provides “short forms” of the byte, word, doubleword, and quadword versions of the STOS instructions. Here also ES: (E)DI is assumed to be the destination operand and AL, AX, or EAX is assumed to be the source operand. The size of the destination and source operands is selected by the mnemonic: STOSB (byte read from register AL), STOSW (word from AX), STOSD (doubleword from EAX).

After the byte, word, or doubleword is transferred from the register to the memory location, the (E)DI register is incremented or decremented according to the setting of the DF flag in the EFLAGS register. If the DF flag is 0, the register is incremented; if the DF flag is 1, the register is decremented (the register is incremented or decremented by 1 for byte operations, by 2 for word operations, by 4 for doubleword operations).

In 64-bit mode, the default address size is 64 bits, 32-bit address size is supported using the prefix 67H. Using a REX prefix in the form of REX.W promotes operation on doubleword operand to 64 bits. The promoted no-operand mnemonic is STOSQ. STOSQ (and its explicit operands variant) store a quadword from the RAX register into the destination addressed by RDI or EDI. See the summary chart at the beginning of this section for encoding data and limits.

The STOS, STOSB, STOSW, STOSD, STOSQ instructions can be preceded by the REP prefix for block loads of ECX bytes, words, or doublewords. More often, however, these instructions are used within a LOOP construct because data needs to be moved into the AL, AX, or EAX register before it can be stored. See “REP/REPE/REPZ/REPNE/REPZ—Repeat String Operation Prefix” in this chapter for a description of the REP prefix.

Operation

Non-64-bit Mode:

```

IF (Byte store)
  THEN
    DEST ← AL;
    THEN IF DF = 0
      THEN (E)DI ← (E)DI + 1;
      ELSE (E)DI ← (E)DI - 1;
    FI;
ELSE IF (Word store)
  THEN
    DEST ← AX;
    THEN IF DF = 0
      THEN (E)DI ← (E)DI + 2;
      ELSE (E)DI ← (E)DI - 2;

```

```

        FI;
    FI;
ELSE IF (Doubleword store)
    THEN
        DEST ← EAX;
        THEN IF DF = 0
            THEN (E)DI ← (E)DI + 4;
            ELSE (E)DI ← (E)DI - 4;
        FI;
    FI;
FI;

64-bit Mode:

IF (Byte store)
    THEN
        DEST ← AL;
        THEN IF DF = 0
            THEN (R)E)DI ← (R)E)DI + 1;
            ELSE (R)E)DI ← (R)E)DI - 1;
        FI;
ELSE IF (Word store)
    THEN
        DEST ← AX;
        THEN IF DF = 0
            THEN (R)E)DI ← (R)E)DI + 2;
            ELSE (R)E)DI ← (R)E)DI - 2;
        FI;
    FI;
ELSE IF (Doubleword store)
    THEN
        DEST ← EAX;
        THEN IF DF = 0
            THEN (R)E)DI ← (R)E)DI + 4;
            ELSE (R)E)DI ← (R)E)DI - 4;
        FI;
    FI;
ELSE IF (Quadword store using REX.W )
    THEN
        DEST ← RAX;
        THEN IF DF = 0
            THEN (R)E)DI ← (R)E)DI + 8;
            ELSE (R)E)DI ← (R)E)DI - 8;
        FI;

```

FI;
FI;

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the limit of the ES segment. If the ES register contains a NULL segment selector. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand effective address is outside the ES segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the ES segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

STR—Store Task Register

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|------------------|-------------|------------------|---|
| 0F 00 /1 | STR <i>r/m16</i> | Valid | Valid | Stores segment selector from TR in <i>r/m16</i> . |

Description

Stores the segment selector from the task register (TR) in the destination operand. The destination operand can be a general-purpose register or a memory location. The segment selector stored with this instruction points to the task state segment (TSS) for the currently running task.

When the destination operand is a 32-bit register, the 16-bit segment selector is copied into the lower 16 bits of the register and the upper 16 bits of the register are cleared. When the destination operand is a memory location, the segment selector is written to memory as a 16-bit quantity, regardless of operand size.

In 64-bit mode, operation is the same. The size of the memory operand is fixed at 16 bits. In register stores, the 2-byte TR is zero extended if stored to a 64-bit register.

The STR instruction is useful only in operating-system software. It can only be executed in protected mode.

Operation

DEST ← TR(SegmentSelector);

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the destination is a memory operand that is located in a non-writable segment or if the effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

#UD The STR instruction is not recognized in real-address mode.

Virtual-8086 Mode Exceptions

#UD The STR instruction is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#GP(0) If the memory address is in a non-canonical form.
#SS(U) If the stack address is in a non-canonical form.
#PF(fault-code) If a page fault occurs.
#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.
#UD If the LOCK prefix is used.

SUB—Subtract

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|---------------------------------|-------------|---------------------|--|
| 2C <i>ib</i> | SUB AL, <i>imm8</i> | Valid | Valid | Subtract <i>imm8</i> from AL. |
| 2D <i>iw</i> | SUB AX, <i>imm16</i> | Valid | Valid | Subtract <i>imm16</i> from AX. |
| 2D <i>id</i> | SUB EAX, <i>imm32</i> | Valid | Valid | Subtract <i>imm32</i> from EAX. |
| REX.W + 2D <i>id</i> | SUB RAX, <i>imm32</i> | Valid | N.E. | Subtract <i>imm32</i> sign-extended to 64-bits from RAX. |
| 80 /5 <i>ib</i> | SUB <i>r/m8</i> , <i>imm8</i> | Valid | Valid | Subtract <i>imm8</i> from <i>r/m8</i> . |
| REX + 80 /5 <i>ib</i> | SUB <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | Subtract <i>imm8</i> from <i>r/m8</i> . |
| 81 /5 <i>iw</i> | SUB <i>r/m16</i> , <i>imm16</i> | Valid | Valid | Subtract <i>imm16</i> from <i>r/m16</i> . |
| 81 /5 <i>id</i> | SUB <i>r/m32</i> , <i>imm32</i> | Valid | Valid | Subtract <i>imm32</i> from <i>r/m32</i> . |
| REX.W + 81 /5 <i>id</i> | SUB <i>r/m64</i> , <i>imm32</i> | Valid | N.E. | Subtract <i>imm32</i> sign-extended to 64-bits from <i>r/m64</i> . |
| 83 /5 <i>ib</i> | SUB <i>r/m16</i> , <i>imm8</i> | Valid | Valid | Subtract sign-extended <i>imm8</i> from <i>r/m16</i> . |
| 83 /5 <i>ib</i> | SUB <i>r/m32</i> , <i>imm8</i> | Valid | Valid | Subtract sign-extended <i>imm8</i> from <i>r/m32</i> . |
| REX.W + 83 /5 <i>ib</i> | SUB <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | Subtract sign-extended <i>imm8</i> from <i>r/m64</i> . |
| 28 / <i>r</i> | SUB <i>r/m8</i> , <i>r8</i> | Valid | Valid | Subtract <i>r8</i> from <i>r/m8</i> . |
| REX + 28 / <i>r</i> | SUB <i>r/m8*</i> , <i>r8*</i> | Valid | N.E. | Subtract <i>r8</i> from <i>r/m8</i> . |
| 29 / <i>r</i> | SUB <i>r/m16</i> , <i>r16</i> | Valid | Valid | Subtract <i>r16</i> from <i>r/m16</i> . |
| 29 / <i>r</i> | SUB <i>r/m32</i> , <i>r32</i> | Valid | Valid | Subtract <i>r32</i> from <i>r/m32</i> . |
| REX.W + 29 / <i>r</i> | SUB <i>r/m64</i> , <i>r32</i> | Valid | N.E. | Subtract <i>r64</i> from <i>r/m64</i> . |
| 2A / <i>r</i> | SUB <i>r8</i> , <i>r/m8</i> | Valid | Valid | Subtract <i>r/m8</i> from <i>r8</i> . |
| REX + 2A / <i>r</i> | SUB <i>r8*</i> , <i>r/m8*</i> | Valid | N.E. | Subtract <i>r/m8</i> from <i>r8</i> . |
| 2B / <i>r</i> | SUB <i>r16</i> , <i>r/m16</i> | Valid | Valid | Subtract <i>r/m16</i> from <i>r16</i> . |
| 2B / <i>r</i> | SUB <i>r32</i> , <i>r/m32</i> | Valid | Valid | Subtract <i>r/m32</i> from <i>r32</i> . |
| REX.W + 2B / <i>r</i> | SUB <i>r64</i> , <i>r/m64</i> | Valid | N.E. | Subtract <i>r/m64</i> from <i>r64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Subtracts the second operand (source operand) from the first operand (destination operand) and stores the result in the destination operand. The destination operand can be a register or a memory location; the source operand can be an immediate, register, or memory location. (However, two memory operands cannot be used in one instruction.) When an immediate value is used as an operand, it is sign-extended to the length of the destination operand format.

The SUB instruction performs integer subtraction. It evaluates the result for both signed and unsigned integer operands and sets the OF and CF flags to indicate an overflow in the signed or unsigned result, respectively. The SF flag indicates the sign of the signed result.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

Operation

DEST ← (DEST - SRC);

Flags Affected

The OF, SF, ZF, AF, PF, and CF flags are set according to the result.

Protected Mode Exceptions

| | |
|------------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
|-----|---|

| | |
|-----|---|
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

SUBPD—Subtract Packed Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|---|-------------|------------------|---|
| 66 0F 5C /r | SUBPD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Subtract packed double-precision floating-point values in <i>xmm2/m128</i> from <i>xmm1</i> . |

Description

Performs a SIMD subtract of the two packed double-precision floating-point values in the source operand (second operand) from the two packed double-precision floating-point values in the destination operand (first operand), and stores the packed double-precision floating-point results in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. See Figure 11-3 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD double-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[63:0] ← DEST[63:0] – SRC[63:0];
DEST[127:64] ← DEST[127:64] – SRC[127:64];
```

Intel C/C++ Compiler Intrinsic Equivalent

```
SUBPD    __m128d _mm_sub_pd (m128d a, m128d b)
```

SIMD Floating-Point Exceptions

Overflow, Underflow, Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|-----|--|
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 1.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |
|-----|--|

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | <p>If a memory operand is not aligned on a 16-byte boundary, regardless of segment.</p> <p>If any part of the operand lies outside the effective address space from 0 to FFFFH.</p> |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1.</p> |
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | <p>If the memory address is in a non-canonical form.</p> <p>If memory operand is not aligned on a 16-byte boundary, regardless of segment.</p> |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

#UD

- If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.
- If CR0.EM[bit 2] = 1.
- If CR4.OSFXSR[bit 9] = 0.
- If CPUID.01H: EDX.SSE2[bit 26] = 0.
- If the LOCK prefix is used.

SUBPS—Subtract Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|---------------------------------------|-------------|------------------|--|
| OF 5C /r | SUBPS <i>xmm1</i> <i>xmm2/m128</i> | Valid | Valid | Subtract packed single-precision floating-point values in <i>xmm2/mem</i> from <i>xmm1</i> . |

Description

Performs a SIMD subtract of the four packed single-precision floating-point values in the source operand (second operand) from the four packed single-precision floating-point values in the destination operand (first operand), and stores the packed single-precision floating-point results in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register. See Figure 10-5 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a SIMD double-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[31:0] ← DEST[31:0] – SRC[31:0];
DEST[63:32] ← DEST[63:32] – SRC[63:32];
DEST[95:64] ← DEST[95:64] – SRC[95:64];
DEST[127:96] ← DEST[127:96] – SRC[127:96];
```

Intel C/C++ Compiler Intrinsic Equivalent

```
SUBPS    __m128 __mm_sub_ps(__m128 a, __m128 b)
```

SIMD Floating-Point Exceptions

Overflow, Underflow, Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |

| | |
|-----|--|
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |

| | |
|-----|--|
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

SUBSD—Subtract Scalar Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| F2 0F 5C /r | SUBSD <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Subtracts the low double-precision floating-point values in <i>xmm2/mem64</i> from <i>xmm1</i> . |

Description

Subtracts the low double-precision floating-point value in the source operand (second operand) from the low double-precision floating-point value in the destination operand (first operand), and stores the double-precision floating-point result in the destination operand. The source operand can be an XMM register or a 64-bit memory location. The destination operand is an XMM register. The high quadword of the destination operand remains unchanged. See Figure 11-4 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a scalar double-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[63:0] ← DEST[63:0] – SRC[63:0];
(* DEST[127:64] unchanged *)

Intel C/C++ Compiler Intrinsic Equivalent

SUBSD __m128d _mm_sub_sd (m128d a, m128d b)

SIMD Floating-Point Exceptions

Overflow, Underflow, Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. |

| | |
|--------|--|
| | If CR0.EM[bit 2] = 1. |
| | If CR4.OSFXSR[bit 9] = 0. |
| | If CPUID.01H:EDX.SSE2[bit 26] = 0. |
| | If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|---|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|--------|--|
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE2[bit 26] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

SUBSS—Subtract Scalar Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|---|
| F3 0F 5C /r | SUBSS <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Subtract the lower single-precision floating-point values in <i>xmm2/m32</i> from <i>xmm1</i> . |

Description

Subtracts the low single-precision floating-point value in the source operand (second operand) from the low single-precision floating-point value in the destination operand (first operand), and stores the single-precision floating-point result in the destination operand. The source operand can be an XMM register or a 32-bit memory location. The destination operand is an XMM register. The three high-order double-words of the destination operand remain unchanged. See Figure 10-6 in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for an illustration of a scalar single-precision floating-point operation.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[31:0] ← DEST[31:0] – SRC[31:0];
(* DEST[127:96] unchanged *)

Intel C/C++ Compiler Intrinsic Equivalent

SUBSS __m128 _mm_sub_ss(__m128 a, __m128 b)

SIMD Floating-Point Exceptions

Overflow, Underflow, Invalid, Precision, Denormal.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|--------|--|
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|--|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|---|
| #PF(fault-code) | For a page fault. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |

| | |
|--------|---|
| #UD | <p>If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.</p> <p>If CR0.EM[bit 2] = 1.</p> <p>If CR4.OSFXSR[bit 9] = 0.</p> <p>If CPUID.01H:EDX.SSE[bit 25] = 0.</p> <p>If the LOCK prefix is used.</p> |
| #AC(0) | <p>If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.</p> |

SWAPGS—Swap GS Base Register

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|-------------|-------------|------------------|---|
| OF 01 /7 | SWAPGS | Valid | Invalid | Exchanges the current GS base register value with the value contained in MSR address C0000102H. |

Description

SWAPGS exchanges the current GS base register value with the value contained in MSR address C0000102H (MSR_KERNELGSbase). KernelGSbase is guaranteed to be canonical; so SWAPGS does not perform a canonical check. The SWAPGS instruction is a privileged instruction intended for use by system software.

When using SYSCALL to implement system calls, there is no kernel stack at the OS entry point. Neither is there a straightforward method to obtain a pointer to kernel structures from which the kernel stack pointer could be read. Thus, the kernel can't save general purpose registers or reference memory.

By design, SWAPGS does not require any general purpose registers or memory operands. No registers need to be saved before using the instruction. SWAPGS exchanges the CPL 0 data pointer from the KernelGSbase MSR with the GS base register. The kernel can then use the GS prefix on normal memory references to access kernel data structures. Similarly, when the OS kernel is entered using an interrupt or exception (where the kernel stack is already set up), SWAPGS can be used to quickly get a pointer to the kernel data structures.

The KernelGSbase MSR itself is only accessible using RDMSR/WRMSR instructions. Those instructions are only accessible at privilege level 0. WRMSR will cause a #GP(0) if the value to be written to KernelGSbase MSR is non-canonical.

See Table 4-6.

Table 4-6. SWAPGS Operation Parameters

| Opcode | ModR/M Byte | | | Instruction | |
|--------|-------------|-----|-------|-----------------|-------------|
| | MOD | REG | R/M | Not 64-bit Mode | 64-bit Mode |
| OF 01 | MOD ≠ 11 | 111 | xxx | INVLPG | INVLPG |
| | 11 | 111 | 000 | #UD | SWPGS |
| | 11 | 111 | ≠ 000 | #UD | #UD |

Operation

IF CS.L \neq 1 (* Not in 64-Bit Mode *)

THEN

#UD; FI;

IF CPL \neq 0

THEN #GP(0); FI;

tmp \leftarrow GS(BASE);

GS(BASE) \leftarrow KERNELGSbase;

KERNELGSbase \leftarrow tmp;

Flags Affected

None

Protected Mode Exceptions

#UD If Mode \neq 64-Bit.

Real-Address Mode Exceptions

#UD If Mode \neq 64-Bit.

Virtual-8086 Mode Exceptions

#UD If Mode \neq 64-Bit.

Compatibility Mode Exceptions

#UD If Mode \neq 64-Bit.

64-Bit Mode Exceptions

#GP(0) If CPL \neq 0.

If the LOCK prefix is used.

SYSCALL—Fast System Call

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|--------|-------------|-------------|-----------------|---|
| OF 05 | SYSCALL | Valid | Invalid | Fast call to privilege level 0 system procedures. |

Description

SYSCALL saves the RIP of the instruction following SYSCALL to RCX and loads a new RIP from the IA32_LSTAR (64-bit mode). Upon return, SYSRET copies the value saved in RCX to the RIP.

SYSCALL saves RFLAGS (lower 32 bit only) in R11. It then masks RFLAGS with an OS-defined value using the IA32_FMASK (MSR C000_0084). The actual mask value used by the OS is the complement of the value written to the IA32_FMASK MSR. None of the bits in RFLAGS are automatically cleared (except for RF). SYSRET restores RFLAGS from R11 (the lower 32 bits only).

Software should not alter the CS or SS descriptors in a manner that violates the following assumptions made by SYSCALL/SYSRET:

- The CS and SS base and limit remain the same for all processes, including the operating system (the base is 0H and the limit is 0FFFFFFFH).
- The CS of the SYSCALL target has a privilege level of 0.
- The CS of the SYSRET target has a privilege level of 3.

SYSCALL/SYSRET do not check for violations of these assumptions.

Operation

IF (CS.L \neq 1) or (IA32_EFER.LMA \neq 1) or (IA32_EFER.SCE \neq 1)
 (* Not in 64-Bit Mode or SYSCALL/SYSRET not enabled in IA32_EFER *)

THEN #UD; FI;

RCX \leftarrow RIP;

RIP \leftarrow LSTAR_MSR;

R11 \leftarrow EFLAGS;

EFLAGS \leftarrow (EFLAGS MASKED BY IA32_FMASK);

CPL \leftarrow 0;

CS(SEL) \leftarrow IA32_STAR_MSR[47:32];

CS(DPL) \leftarrow 0;

CS(BASE) \leftarrow 0;

CS(LIMIT) \leftarrow 0xFFFFF;

CS(GRANULAR) \leftarrow 1;

SS(SEL) \leftarrow IA32_STAR_MSR[47:32] + 8;

SS(DPL) \leftarrow 0;

SS(BASE) ← 0;
SS(LIMIT) ← 0xFFFFF;
SS(GRANULAR) ← 1;

Flags Affected

All.

Protected Mode Exceptions

#UD If Mode ≠ 64-bit.

Real-Address Mode Exceptions

#UD If Mode ≠ 64-bit.

Virtual-8086 Mode Exceptions

#UD If Mode ≠ 64-bit.

Compatibility Mode Exceptions

#UD If Mode ≠ 64-bit.

64-Bit Mode Exceptions

#UD If IA32_EFER.SCE = 0.
 If the LOCK prefix is used.

SYSENTER—Fast System Call

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|---|
| 0F 34 | SYSENTER | Valid | Valid | Fast call to privilege level 0 system procedures. |

Description

Executes a fast call to a level 0 system procedure or routine. SYSENTER is a companion instruction to SYSEXIT. The instruction is optimized to provide the maximum performance for system calls from user code running at privilege level 3 to operating system or executive procedures running at privilege level 0.

Prior to executing the SYSENTER instruction, software must specify the privilege level 0 code segment and code entry point, and the privilege level 0 stack segment and stack pointer by writing values to the following MSRs:

- IA32_SYSENTER_CS — Contains a 32-bit value, of which the lower 16 bits are the segment selector for the privilege level 0 code segment. This value is also used to compute the segment selector of the privilege level 0 stack segment.
- IA32_SYSENTER_EIP — Contains the 32-bit offset into the privilege level 0 code segment to the first instruction of the selected operating procedure or routine.
- IA32_SYSENTER_ESP — Contains the 32-bit stack pointer for the privilege level 0 stack.

These MSRs can be read from and written to using RDMSR/WRMSR. Register addresses are listed in Table 4-7. The addresses are defined to remain fixed for future Intel 64 and IA-32 processors.

Table 4-7. MSRs Used By the SYSENTER and SYSEXIT Instructions

| MSR | Address |
|-------------------|---------|
| IA32_SYSENTER_CS | 174H |
| IA32_SYSENTER_ESP | 175H |
| IA32_SYSENTER_EIP | 176H |

When SYSENTER is executed, the processor:

1. Loads the segment selector from the IA32_SYSENTER_CS into the CS register.
2. Loads the instruction pointer from the IA32_SYSENTER_EIP into the EIP register.
3. Adds 8 to the value in IA32_SYSENTER_CS and loads it into the SS register.
4. Loads the stack pointer from the IA32_SYSENTER_ESP into the ESP register.
5. Switches to privilege level 0.
6. Clears the VM flag in the EFLAGS register, if the flag is set.

7. Begins executing the selected system procedure.

The processor does not save a return IP or other state information for the calling procedure.

The SYSENTER instruction always transfers program control to a protected-mode code segment with a DPL of 0. The instruction requires that the following conditions are met by the operating system:

- The segment descriptor for the selected system code segment selects a flat, 32-bit code segment of up to 4 GBytes, with execute, read, accessed, and non-conforming permissions.
- The segment descriptor for selected system stack segment selects a flat 32-bit stack segment of up to 4 GBytes, with read, write, accessed, and expand-up permissions.

The SYSENTER can be invoked from all operating modes except real-address mode.

The SYSENTER and SYSEXIT instructions are companion instructions, but they do not constitute a call/return pair. When executing a SYSENTER instruction, the processor does not save state information for the user code, and neither the SYSENTER nor the SYSEXIT instruction supports passing parameters on the stack.

To use the SYSENTER and SYSEXIT instructions as companion instructions for transitions between privilege level 3 code and privilege level 0 operating system procedures, the following conventions must be followed:

- The segment descriptors for the privilege level 0 code and stack segments and for the privilege level 3 code and stack segments must be contiguous in the global descriptor table. This convention allows the processor to compute the segment selectors from the value entered in the SYSENTER_CS_MSR MSR.
- The fast system call “stub” routines executed by user code (typically in shared libraries or DLLs) must save the required return IP and processor state information if a return to the calling procedure is required. Likewise, the operating system or executive procedures called with SYSENTER instructions must have access to and use this saved return and state information when returning to the user code.

The SYSENTER and SYSEXIT instructions were introduced into the IA-32 architecture in the Pentium II processor. The availability of these instructions on a processor is indicated with the SYSENTER/SYSEXIT present (SEP) feature flag returned to the EDX register by the CPUID instruction. An operating system that qualifies the SEP flag must also qualify the processor family and model to ensure that the SYSENTER/SYSEXIT instructions are actually present. For example:

```
IF CPUID SEP bit is set
  THEN IF (Family = 6) and (Model < 3) and (Stepping < 3)
    THEN
      SYSENTER/SYSEXIT_Not_Supported; FI;
    ELSE
      SYSENTER/SYSEXIT_Supported; FI;
```

FI;

When the CPUID instruction is executed on the Pentium Pro processor (model 1), the processor returns a the SEP flag as set, but does not support the SYSENTER/SYSEXIT instructions.

Operation

IF CRO.PE = 0 THEN #GP(0); FI;

IF SYSENTER_CS_MSR[15:2] = 0 THEN #GP(0); FI;

EFLAGS.VM ← 0; (* Insures protected mode execution *)

EFLAGS.IF ← 0; (* Mask interrupts *)

EFLAGS.RF ← 0;

CS.SEL ← SYSENTER_CS_MSR (* Operating system provides CS *)

(* Set rest of CS to a fixed value *)

CS.BASE ← 0; (* Flat segment *)

CS.LIMIT ← FFFFFFFH; (* 4-GByte limit *)

CS.ARbyte.G ← 1; (* 4-KByte granularity *)

CS.ARbyte.S ← 1;

CS.ARbyte.TYPE ← 1011B; (* Execute + Read, Accessed *)

(* 32-bit code segment*)

CS.ARbyte.D ← 1;

CS.SEL.RPL ← 0;

CS.ARbyte.P ← 1;

CPL ← 0;

SS.SEL ← CS.SEL + 8;

(* Set rest of SS to a fixed value *)

SS.BASE ← 0; (* Flat segment *)

SS.LIMIT ← FFFFFFFH; (* 4-GByte limit *)

SS.ARbyte.G ← 1; (* 4-KByte granularity *)

SS.ARbyte.S ← 0;

SS.ARbyte.TYPE ← 0011B; (* Read/Write, Accessed *)

(* 32-bit stack segment*)

SS.ARbyte.D ← 1;

SS.ARbyte.DPL ← 0;

SS.SEL.RPL ← 0;

SS.ARbyte.P ← 1;

ESP ← SYSENTER_ESP_MSR;

EIP ← SYSENTER_EIP_MSR;

IA-32e Mode Operation

In IA-32e mode, SYSENTER executes a fast system calls from user code running at privilege level 3 (in compatibility mode or 64-bit mode) to 64-bit executive proce-

dures running at privilege level 0. This instruction is a companion instruction to the SYSEXIT instruction.

In IA-32e mode, the IA32_SYSENTER_EIP and IA32_SYSENTER_ESP MSRs hold 64-bit addresses and must be in canonical form; IA32_SYSENTER_CS must not contain a NULL selector.

When SYSENTER transfers control, the following fields are generated and bits set:

- **Target code segment** — Reads non-NULL selector from IA32_SYSENTER_CS.
- **New CS attributes** — L-bit = 1 (go to 64-bit mode); CS base = 0, CS limit = FFFFFFFFH.
- **Target instruction** — Reads 64-bit canonical address from IA32_SYSENTER_EIP.
- **Stack segment** — Computed by adding 8 to the value from IA32_SYSENTER_CS.
- **Stack pointer** — Reads 64-bit canonical address from IA32_SYSENTER_ESP.
- **New SS attributes** — SS base = 0, SS limit = FFFFFFFFH.

Flags Affected

VM, IF, RF (see Operation above)

Protected Mode Exceptions

#GP(0) If IA32_SYSENTER_CS[15:2] = 0.
 #UD If the LOCK prefix is used.

Real-Address Mode Exceptions

#GP If protected mode is not enabled.
 #UD If the LOCK prefix is used.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

SYSEXIT—Fast Return from Fast System Call

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|---------------|-------------|-------------|-----------------|---|
| OF 35 | SYSEXIT | Valid | Valid | Fast return to privilege level 3 user code. |
| REX.W + OF 35 | SYSEXIT | Valid | Valid | Fast return to 64-bit mode privilege level 3 user code. |

Description

Executes a fast return to privilege level 3 user code. SYSEXIT is a companion instruction to the SYSENTER instruction. The instruction is optimized to provide the maximum performance for returns from system procedures executing at protection levels 0 to user procedures executing at protection level 3. It must be executed from code executing at privilege level 0.

Prior to executing SYSEXIT, software must specify the privilege level 3 code segment and code entry point, and the privilege level 3 stack segment and stack pointer by writing values into the following MSR and general-purpose registers:

- **IA32_SYSENTER_CS** — Contains a 32-bit value, of which the lower 16 bits are the segment selector for the privilege level 0 code segment in which the processor is currently executing. This value is used to compute the segment selectors for the privilege level 3 code and stack segments.
- **EDX** — Contains the 32-bit offset into the privilege level 3 code segment to the first instruction to be executed in the user code.
- **ECX** — Contains the 32-bit stack pointer for the privilege level 3 stack.

The IA32_SYSENTER_CS MSR can be read from and written to using RDMSR/WRMSR. The register address is listed in Table 4-7. This address is defined to remain fixed for future Intel 64 and IA-32 processors.

When SYSEXIT is executed, the processor:

1. Adds 16 to the value in IA32_SYSENTER_CS and loads the sum into the CS selector register.
2. Loads the instruction pointer from the EDX register into the EIP register.
3. Adds 24 to the value in IA32_SYSENTER_CS and loads the sum into the SS selector register.
4. Loads the stack pointer from the ECX register into the ESP register.
5. Switches to privilege level 3.
6. Begins executing the user code at the EIP address.

See “SWAPGS—Swap GS Base Register” in this chapter for information about using the SYSENTER and SYSEXIT instructions as companion call and return instructions.

The SYSEXIT instruction always transfers program control to a protected-mode code segment with a DPL of 3. The instruction requires that the following conditions are met by the operating system:

- The segment descriptor for the selected user code segment selects a flat, 32-bit code segment of up to 4 GBytes, with execute, read, accessed, and non-conforming permissions.
- The segment descriptor for selected user stack segment selects a flat, 32-bit stack segment of up to 4 GBytes, with expand-up, read, write, and accessed permissions.

The SYSENTER can be invoked from all operating modes except real-address mode and virtual 8086 mode.

The SYSENTER and SYSEXIT instructions were introduced into the IA-32 architecture in the Pentium II processor. The availability of these instructions on a processor is indicated with the SYSENTER/SYSEXIT present (SEP) feature flag returned to the EDX register by the CPUID instruction. An operating system that qualifies the SEP flag must also qualify the processor family and model to ensure that the SYSENTER/SYSEXIT instructions are actually present. For example:

```
IF CPUID SEP bit is set
  THEN IF (Family = 6) and (Model < 3) and (Stepping < 3)
    THEN
      SYSENTER/SYSEXIT_Not_Supported; FI;
    ELSE
      SYSENTER/SYSEXIT_Supported; FI;
  FI;
```

When the CPUID instruction is executed on the Pentium Pro processor (model 1), the processor returns a the SEP flag as set, but does not support the SYSENTER/SYSEXIT instructions.

Operation

```
IF SYSENTER_CS_MSR[15:2] = 0 THEN #GP(0); FI;
IF CRO.PE = 0 THEN #GP(0); FI;
IF CPL ≠ 0 THEN #GP(0); FI;
```

```
CS.SEL ← (SYSENTER_CS_MSR + 16);      (* Segment selector for return CS *)
(* Set rest of CS to a fixed value *)
CS.BASE ← 0;                          (* Flat segment *)
CS.LIMIT ← FFFFFFFH;                  (* 4-GByte limit *)
CS.ARbyte.G ← 1;                      (* 4-KByte granularity *)
CS.ARbyte.S ← 1;
CS.ARbyte.TYPE ← 1011B;               (* Execute, Read, Non-Conforming Code *)
CS.ARbyte.D ← 1;                      (* 32-bit code segment *)
CS.ARbyte.DPL ← 3;
```

CS.SEL.RPL \leftarrow 3;
 CS.ARbyte.P \leftarrow 1;
 CPL \leftarrow 3;

SS.SEL \leftarrow (SYSENTER_CS_MSR + 24); (* Segment selector for return SS *)
 (* Set rest of SS to a fixed value *);
 SS.BASE \leftarrow 0; (* Flat segment *)
 SS.LIMIT \leftarrow FFFFFFFH; (* 4-GByte limit *)
 SS.ARbyte.G \leftarrow 1; (* 4-KByte granularity *)
 SS.ARbyte.S \leftarrow ;
 SS.ARbyte.TYPE \leftarrow 0011B; (* Expand Up, Read/Write, Data *)
 SS.ARbyte.D \leftarrow 1; (* 32-bit stack segment*)
 SS.ARbyte.DPL \leftarrow 3;
 SS.SEL.RPL \leftarrow 3;
 SS.ARbyte.P \leftarrow 1;

ESP \leftarrow ECX;
 EIP \leftarrow EDX;

IA-32e Mode Operation

In IA-32e mode, SYSEXIT executes a fast system calls from a 64-bit executive procedures running at privilege level 0 to user code running at privilege level 3 (in compatibility mode or 64-bit mode). This instruction is a companion instruction to the SYSENTER instruction.

In IA-32e mode, the IA32_SYSENTER_EIP and IA32_SYSENTER_ESP MSRs hold 64-bit addresses and must be in canonical form; IA32_SYSENTER_CS must not contain a NULL selector.

When the SYSEXIT instruction transfers control to 64-bit mode user code using REX.W, the following fields are generated and bits set:

- **Target code segment** — Computed by adding 32 to the value in the IA32_SYSENTER_CS.
- **New CS attributes** — L-bit = 1 (go to 64-bit mode).
- **Target instruction** — Reads 64-bit canonical address in RDX.
- **Stack segment** — Computed by adding 8 to the value of CS selector.
- **Stack pointer** — Update RSP using 64-bit canonical address in RCX.

When SYSEXIT transfers control to compatibility mode user code when the operand size attribute is 32 bits, the following fields are generated and bits set:

- **Target code segment** — Computed by adding 16 to the value in IA32_SYSENTER_CS.
- **New CS attributes** — L-bit = 0 (go to compatibility mode).
- **Target instruction** — Fetch the target instruction from 32-bit address in EDX.

- **Stack segment** — Computed by adding 24 to the value in IA32_SYSENTER_CS.
- **Stack pointer** — Update ESP from 32-bit address in ECX.

Flags Affected

None.

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | If IA32_SYSENTER_CS[15:2] = 0. If CPL ≠ 0. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|-----------------------------------|
| #GP | If protected mode is not enabled. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|--------|---------|
| #GP(0) | Always. |
|--------|---------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|--------|--|
| #GP(0) | If IA32_SYSENTER_CS = 0. If CPL ≠ 0. If ECX or EDX contains a non-canonical address. |
| #UD | If the LOCK prefix is used. |

SYSRET—Return From Fast System Call

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|--------|-------------|-------------|-----------------|------------------------------|
| 0F 07 | SYSRET | Valid | Invalid | Return from fast system call |

Description

SYSCALL saves the RIP of the instruction following the SYSCALL into RCX and loads the new RIP from the LSTAR (64-bit mode only). Upon return, SYSRET copies the value saved in RCX to the RIP.

In a return to 64-bit mode using Osize 64, SYSRET sets the CS selector value to MSR IA32_STAR[63:48] + 16. The SS is set to IA32_STAR[63:48] + 8.

SYSRET transfer control to compatibility mode using Osize 32. The CS selector value is set to MSR IA32_STAR[63:48]. The SS is set to IA32_STAR[63:48] + 8.

It is the responsibility of the OS to keep descriptors in the GDT/LDT that correspond to selectors loaded by SYSCALL/SYSRET consistent with the base, limit and attribute values forced by the these instructions.

Software should not alter the CS or SS descriptors in a manner that violates the following assumptions made by SYSCALL/SYSRET:

- CS and SS base and limit remain the same for all processes, including the operating system.
- CS of the SYSCALL target has a privilege level of 0.
- CS of the SYSRET target has a privilege level of 3.

SYSCALL/SYSRET do not check for violations of these assumptions.

Operation

IF (CS.L \neq 1) or (IA32_EFER.LMA \neq 1) or (IA32_EFER.SCE \neq 1)
 (* Not in 64-Bit Mode or SYSCALL/SYSRET not enabled in IA32_EFER *)

THEN #UD; FI;

IF (CPL \neq 0)

THEN #GP(0); FI;

IF (RCX \neq CANONICAL_ADDRESS)

THEN #GP(0); FI;

IF (OPERAND_SIZE = 64)

THEN (* Return to 64-Bit Mode *)

EFLAGS \leftarrow R11;

CPL \leftarrow 0x3;

CS(SEL) \leftarrow IA32_STAR[63:48] + 16;

CS(PL) \leftarrow 0x3;

SS(SEL) \leftarrow IA32_STAR[63:48] + 8;

```

SS(PL) ← 0x3;
RIP ← RCX;
ELSE (* Return to Compatibility Mode *)
  EFLAGS ← R11;
  CPL ← 0x3;
  CS(SEL) ← IA32_STAR[63:48];
  CS(PL) ← 0x3;
  SS(SEL) ← IA32_STAR[63:48] + 8;
  SS(PL) ← 0x3;
  EIP ← ECX;

```

FI;

Flags Affected

VM, IF, RF.

Protected Mode Exceptions

#UD If Mode ≠ 64-Bit.

Real-Address Mode Exceptions

#UD If Mode ≠ 64-Bit.

Virtual-8086 Mode Exceptions

#UD If Mode ≠ 64-Bit.

Compatibility Mode Exceptions

#UD If Mode ≠ 64-Bit.

64-Bit Mode Exceptions

#UD If IA32_EFER.SCE bit = 0.
 If the LOCK prefix is used.

#GP(0) If CPL ≠ 0.
 If ECX contains a non-canonical address.

TEST—Logical Compare

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|----------------------------------|-------------|------------------|---|
| A8 <i>ib</i> | TEST AL, <i>imm8</i> | Valid | Valid | AND <i>imm8</i> with AL; set SF, ZF, PF according to result. |
| A9 <i>iw</i> | TEST AX, <i>imm16</i> | Valid | Valid | AND <i>imm16</i> with AX; set SF, ZF, PF according to result. |
| A9 <i>id</i> | TEST EAX, <i>imm32</i> | Valid | Valid | AND <i>imm32</i> with EAX; set SF, ZF, PF according to result. |
| REX.W + A9 <i>id</i> | TEST RAX, <i>imm32</i> | Valid | N.E. | AND <i>imm32</i> sign-extended to 64-bits with RAX; set SF, ZF, PF according to result. |
| F6 /0 <i>ib</i> | TEST <i>r/m8</i> , <i>imm8</i> | Valid | Valid | AND <i>imm8</i> with <i>r/m8</i> ; set SF, ZF, PF according to result. |
| REX + F6 /0 <i>ib</i> | TEST <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | AND <i>imm8</i> with <i>r/m8</i> ; set SF, ZF, PF according to result. |
| F7 /0 <i>iw</i> | TEST <i>r/m16</i> , <i>imm16</i> | Valid | Valid | AND <i>imm16</i> with <i>r/m16</i> ; set SF, ZF, PF according to result. |
| F7 /0 <i>id</i> | TEST <i>r/m32</i> , <i>imm32</i> | Valid | Valid | AND <i>imm32</i> with <i>r/m32</i> ; set SF, ZF, PF according to result. |
| REX.W + F7 /0 <i>id</i> | TEST <i>r/m64</i> , <i>imm32</i> | Valid | N.E. | AND <i>imm32</i> sign-extended to 64-bits with <i>r/m64</i> ; set SF, ZF, PF according to result. |
| 84 / <i>r</i> | TEST <i>r/m8</i> , <i>r8</i> | Valid | Valid | AND <i>r8</i> with <i>r/m8</i> ; set SF, ZF, PF according to result. |
| REX + 84 / <i>r</i> | TEST <i>r/m8*</i> , <i>r8*</i> | Valid | N.E. | AND <i>r8</i> with <i>r/m8</i> ; set SF, ZF, PF according to result. |
| 85 / <i>r</i> | TEST <i>r/m16</i> , <i>r16</i> | Valid | Valid | AND <i>r16</i> with <i>r/m16</i> ; set SF, ZF, PF according to result. |
| 85 / <i>r</i> | TEST <i>r/m32</i> , <i>r32</i> | Valid | Valid | AND <i>r32</i> with <i>r/m32</i> ; set SF, ZF, PF according to result. |
| REX.W + 85 / <i>r</i> | TEST <i>r/m64</i> , <i>r64</i> | Valid | N.E. | AND <i>r64</i> with <i>r/m64</i> ; set SF, ZF, PF according to result. |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Computes the bit-wise logical AND of first operand (source 1 operand) and the second operand (source 2 operand) and sets the SF, ZF, and PF status flags according to the result. The result is then discarded.

In 64-bit mode, using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

```
TEMP ← SRC1 AND SRC2;
SF ← MSB(TEMP);
```

```
IF TEMP = 0
    THEN ZF ← 1;
    ELSE ZF ← 0;
```

FI:

```
PF ← BitwiseXNOR(TEMP[0:7]);
CF ← 0;
OF ← 0;
(* AF is undefined *)
```

Flags Affected

The OF and CF flags are set to 0. The SF, ZF, and PF flags are set according to the result (see the “Operation” section above). The state of the AF flag is undefined.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

UCOMISD—Unordered Compare Scalar Double-Precision Floating-Point Values and Set EFLAGS

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--|-------------|-----------------|--|
| 66 0F 2E /r | UCOMISD <i>xmm1</i> , <i>xmm2/m64</i> | Valid | Valid | Compares (unordered) the low double-precision floating-point values in <i>xmm1</i> and <i>xmm2/m64</i> and set the EFLAGS accordingly. |

Description

Performs an unordered compare of the double-precision floating-point values in the low quadwords of source operand 1 (first operand) and source operand 2 (second operand), and sets the ZF, PF, and CF flags in the EFLAGS register according to the result (unordered, greater than, less than, or equal). The OF, SF and AF flags in the EFLAGS register are set to 0. The unordered result is returned if either source operand is a NaN (QNaN or SNaN).

Source operand 1 is an XMM register; source operand 2 can be an XMM register or a 64 bit memory location.

The UCOMISD instruction differs from the COMISD instruction in that it signals a SIMD floating-point invalid operation exception (#1) only when a source operand is an SNaN. The COMISD instruction signals an invalid operation exception if a source operand is either a QNaN or an SNaN.

The EFLAGS register is not updated if an unmasked SIMD floating-point exception is generated.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

RESULT ← UnorderedCompare(SRC1[63:0] <> SRC2[63:0]) {
(* Set EFLAGS *)

CASE (RESULT) OF

UNORDERED: ZF, PF, CF ← 111;
GREATER_THAN: ZF, PF, CF ← 000;
LESS_THAN: ZF, PF, CF ← 001;
EQUAL: ZF, PF, CF ← 100;

ESAC;

OF, AF, SF ← 0;

Intel C/C++ Compiler Intrinsic Equivalent

```
int __mm_ucomieq_sd(__m128d a, __m128d b)
int __mm_ucomilt_sd(__m128d a, __m128d b)
int __mm_ucomile_sd(__m128d a, __m128d b)
int __mm_ucomigt_sd(__m128d a, __m128d b)
int __mm_ucomige_sd(__m128d a, __m128d b)
int __mm_ucomineq_sd(__m128d a, __m128d b)
```

SIMD Floating-Point Exceptions

Invalid (if SNaN operands), Denormal.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|--|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. |

If CPUID.01H:EDX.SSE2[bit 26] = 0.
 If the LOCK prefix is used.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.
 #AC(0) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.
 #GP(0) If the memory address is in a non-canonical form.
 #PF(fault-code) For a page fault.
 #NM If CR0.TS[bit 3] = 1.
 #XM If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1.
 #UD If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.
 If CR0.EM[bit 2] = 1.
 If CR4.OSFXSR[bit 9] = 0.
 If CPUID.01H:EDX.SSE2[bit 26] = 0.
 If the LOCK prefix is used.
 #AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

UCOMISS—Unordered Compare Scalar Single-Precision Floating-Point Values and Set EFLAGS

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|--|-------------|------------------|---|
| OF 2E /r | UCOMISS <i>xmm1</i> , <i>xmm2/m32</i> | Valid | Valid | Compare lower single-precision floating-point value in <i>xmm1</i> register with lower single-precision floating-point value in <i>xmm2/mem</i> and set the status flags accordingly. |

Description

Performs an unordered compare of the single-precision floating-point values in the low doublewords of the source operand 1 (first operand) and the source operand 2 (second operand), and sets the ZF, PF, and CF flags in the EFLAGS register according to the result (unordered, greater than, less than, or equal). In The OF, SF and AF flags in the EFLAGS register are set to 0. The unordered result is returned if either source operand is a NaN (QNaN or SNaN).

Source operand 1 is an XMM register; source operand 2 can be an XMM register or a 32 bit memory location.

The UCOMISS instruction differs from the COMISS instruction in that it signals a SIMD floating-point invalid operation exception (#1) only when a source operand is an SNaN. The COMISS instruction signals an invalid operation exception if a source operand is either a QNaN or an SNaN.

The EFLAGS register is not updated if an unmasked SIMD floating-point exception is generated.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

RESULT ← UnorderedCompare(SRC1[31:0] <> SRC2[31:0]) {

(* Set EFLAGS *)

CASE (RESULT) OF

UNORDERED: ZF,PF,CF ← 111;

GREATER_THAN: ZF,PF,CF ← 000;

LESS_THAN: ZF,PF,CF ← 001;

EQUAL: ZF,PF,CF ← 100;

ESAC;

OF,AF,SF ← 0;

Intel C/C++ Compiler Intrinsic Equivalent

`int_mm_ucomieq_ss(__m128 a, __m128 b)`

`int_mm_ucomilt_ss(__m128 a, __m128 b)`

`int_mm_ucomile_ss(__m128 a, __m128 b)`

`int_mm_ucomigt_ss(__m128 a, __m128 b)`

`int_mm_ucomige_ss(__m128 a, __m128 b)`

`int_mm_ucomineq_ss(__m128 a, __m128 b)`

SIMD Floating-Point Exceptions

Invalid (if SNaN operands), Denormal.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |

Real-Address Mode Exceptions

| | |
|-----|--|
| GP | If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #XM | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1. |
| #UD | If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0. If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. |

If CPUID.01H: EDX.SSE[bit 25] = 0.
 If the LOCK prefix is used.

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.
 #AC(0) If alignment checking is enabled and an unaligned memory reference is made.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.
 #GP(0) If the memory address is in a non-canonical form.
 #PF(fault-code) For a page fault.
 #NM If CR0.TS[bit 3] = 1.
 #XM If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 1.
 #UD If an unmasked SIMD floating-point exception and CR4.OSXMMEXCPT[bit 10] = 0.
 If CR0.EM[bit 2] = 1.
 If CR4.OSFXSR[bit 9] = 0.
 If CPUID.01H: EDX.SSE[bit 25] = 0.
 If the LOCK prefix is used.
 #AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

UD2—Undefined Instruction

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|---------------------|---------------------------------|
| 0F 0B | UD2 | Valid | Valid | Raise invalid opcode exception. |

Description

Generates an invalid opcode. This instruction is provided for software testing to explicitly generate an invalid opcode. The opcode for this instruction is reserved for this purpose.

Other than raising the invalid opcode exception, this instruction is the same as the NOP instruction.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

#UD (* Generates invalid opcode exception *);

Flags Affected

None.

Exceptions (All Operating Modes)

#UD Raises an invalid opcode exception in all operating modes.

UNPCKHPD—Unpack and Interleave High Packed Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--|-------------|------------------|--|
| 66 OF 15 /r | UNPCKHPD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpacks and interleaves double-precision floating-point values from high quadwords of <i>xmm1</i> and <i>xmm2/m128</i> . |

Description

Performs an interleaved unpack of the high double-precision floating-point values from the source operand (second operand) and the destination operand (first operand). See Figure 4-16. The source operand can be an XMM register or a 128-bit memory location; the destination operand is an XMM register.

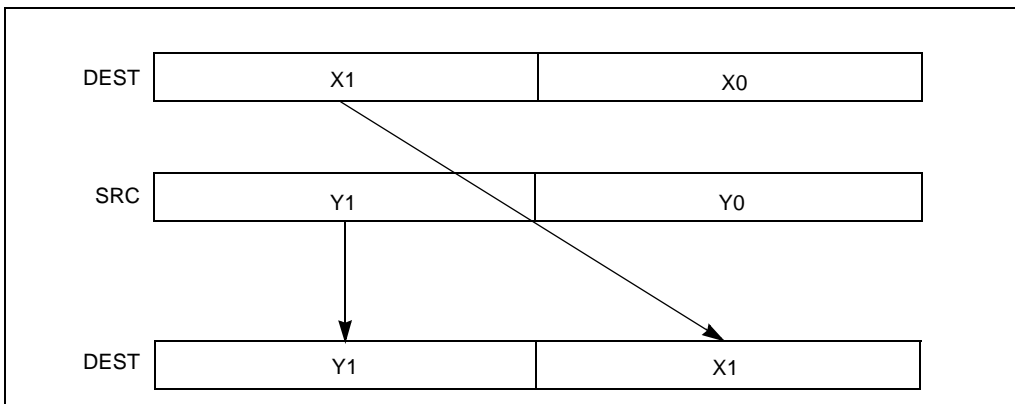


Figure 4-16. UNPCKHPD Instruction High Unpack and Interleave Operation

When unpacking from a memory operand, an implementation may fetch only the appropriate 64 bits; however, alignment to 16-byte boundary and normal segment checking will still be enforced.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[63:0] ← DEST[127:64];
DEST[127:64] ← SRC[127:64];
```

Intel C/C++ Compiler Intrinsic Equivalent

UNPCKHPD__m128d __mm_unpackhi_pd(__m128d a, __m128d b)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

UNPCKHPS—Unpack and Interleave High Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|--|-------------|-----------------|--|
| OF 15 /r | UNPCKHPS <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpacks and interleaves single-precision floating-point values from high quadwords of <i>xmm1</i> and <i>xmm2/mem</i> into <i>xmm1</i> . |

Description

Performs an interleaved unpack of the high-order single-precision floating-point values from the source operand (second operand) and the destination operand (first operand). See Figure 4-17. The source operand can be an XMM register or a 128-bit memory location; the destination operand is an XMM register.

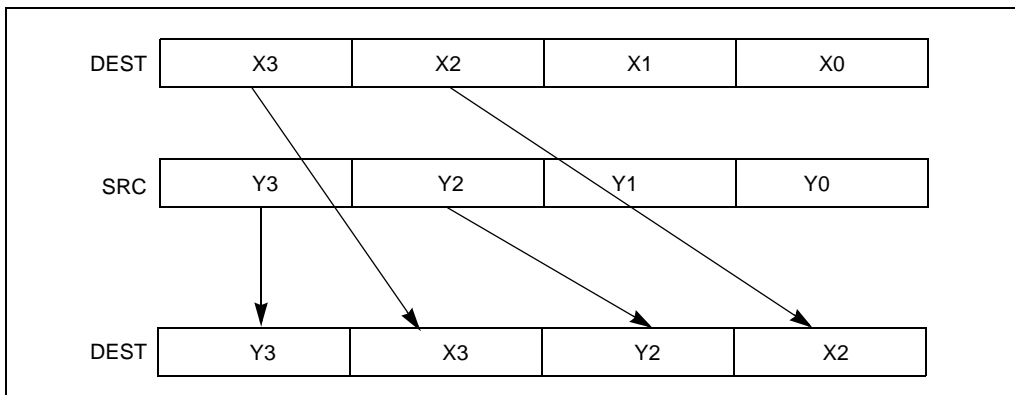


Figure 4-17. UNPCKHPS Instruction High Unpack and Interleave Operation

When unpacking from a memory operand, an implementation may fetch only the appropriate 64 bits; however, alignment to 16-byte boundary and normal segment checking will still be enforced.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```

DEST[31:0] ← DEST[95:64];
DEST[63:32] ← SRC[95:64];
DEST[95:64] ← DEST[127:96];
DEST[127:96] ← SRC[127:96];

```

Intel C/C++ Compiler Intrinsic Equivalent

UNPCKHPS __m128 __mm_unpackhi_ps(__m128 a, __m128 b)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF (fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

UNPCKLPD—Unpack and Interleave Low Packed Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|-------------|--|-------------|-----------------|---|
| 66 OF 14 /r | UNPCKLPD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Unpacks and interleaves double-precision floating-point values from low quadwords of <i>xmm1</i> and <i>xmm2/m128</i> . |

Description

Performs an interleaved unpack of the low double-precision floating-point values from the source operand (second operand) and the destination operand (first operand). See Figure 4-18. The source operand can be an XMM register or a 128-bit memory location; the destination operand is an XMM register.

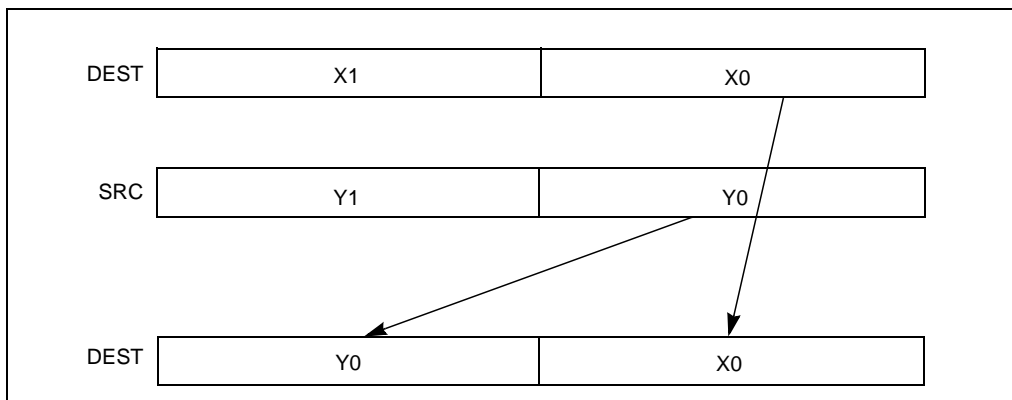


Figure 4-18. UNPCKLPD Instruction Low Unpack and Interleave Operation

When unpacking from a memory operand, an implementation may fetch only the appropriate 64 bits; however, alignment to 16-byte boundary and normal segment checking will still be enforced.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[63:0] ← DEST[63:0];
DEST[127:64] ← SRC[63:0];
```


Intel C/C++ Compiler Intrinsic Equivalent

UNPCKHPD __m128d __mm_unpacklo_pd(__m128d a, __m128d b)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

UNPCKLPS—Unpack and Interleave Low Packed Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|---|-------------|-----------------|---|
| OF 14 /r | UNPCKLPS <i>xmm1</i> , <i>xmm2/mem</i> | Valid | Valid | Unpacks and interleaves single-precision floating-point values from low quadwords of <i>xmm1</i> and <i>xmm2/mem</i> into <i>xmm1</i> . |

Description

Performs an interleaved unpack of the low-order single-precision floating-point values from the source operand (second operand) and the destination operand (first operand). See Figure 4-19. The source operand can be an XMM register or a 128-bit memory location; the destination operand is an XMM register.

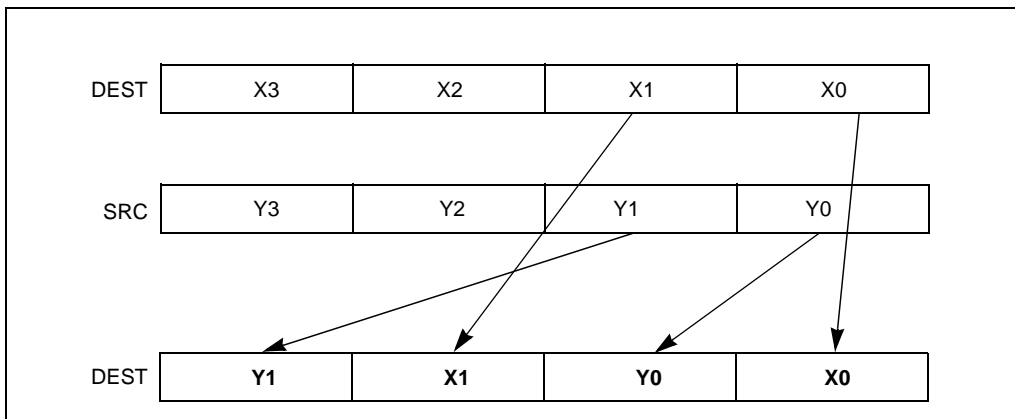


Figure 4-19. UNPCKLPS Instruction Low Unpack and Interleave Operation

When unpacking from a memory operand, an implementation may fetch only the appropriate 64 bits; however, alignment to 16-byte boundary and normal segment checking will still be enforced.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

```
DEST[31:0] ← DEST[31:0];
DEST[63:32] ← SRC[31:0];
DEST[95:64] ← DEST[63:32];
```

DEST[127:96] ← SRC[63:32];

Intel C/C++ Compiler Intrinsic Equivalent

UNPCKLPS __m128_mm_unpacklo_ps(__m128 a, __m128 b)

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H: EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

#PF(fault-code) For a page fault.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

VERR/VERW—Verify a Segment for Reading or Writing

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|-------------------|-------------|-----------------|---|
| 0F 00 /4 | VERR <i>r/m16</i> | Valid | Valid | Set ZF=1 if segment specified with <i>r/m16</i> can be read. |
| 0F 00 /5 | VERW <i>r/m16</i> | Valid | Valid | Set ZF=1 if segment specified with <i>r/m16</i> can be written. |

Description

Verifies whether the code or data segment specified with the source operand is readable (VERR) or writable (VERW) from the current privilege level (CPL). The source operand is a 16-bit register or a memory location that contains the segment selector for the segment to be verified. If the segment is accessible and readable (VERR) or writable (VERW), the ZF flag is set; otherwise, the ZF flag is cleared. Code segments are never verified as writable. This check cannot be performed on system segments.

To set the ZF flag, the following conditions must be met:

- The segment selector is not NULL.
- The selector must denote a descriptor within the bounds of the descriptor table (GDT or LDT).
- The selector must denote the descriptor of a code or data segment (not that of a system segment or gate).
- For the VERR instruction, the segment must be readable.
- For the VERW instruction, the segment must be a writable data segment.
- If the segment is not a conforming code segment, the segment's DPL must be greater than or equal to (have less or the same privilege as) both the CPL and the segment selector's RPL.

The validation performed is the same as is performed when a segment selector is loaded into the DS, ES, FS, or GS register, and the indicated access (read or write) is performed. The segment selector's value cannot result in a protection exception, enabling the software to anticipate possible segment access problems.

This instruction's operation is the same in non-64-bit modes and 64-bit mode. The operand size is fixed at 16 bits.

Operation

```
IF SRC(Offset) > (GDTR(Limit) or (LDTR(Limit)))
  THEN ZF ← 0; FI;
```

Read segment descriptor;

```
IF SegmentDescriptor(DescriptorType) = 0 (* System segment *)
```

or (SegmentDescriptor(Type) ≠ conforming code segment)
and (CPL > DPL) or (RPL > DPL)

THEN

ZF ← 0;

ELSE

IF ((Instruction = VERR) and (Segment readable))
or ((Instruction = VERW) and (Segment writable))

THEN

ZF ← 1;

FI;

FI;

Flags Affected

The ZF flag is set to 1 if the segment is accessible and readable (VERR) or writable (VERW); otherwise, it is set to 0.

Protected Mode Exceptions

The only exceptions generated for these instructions are those related to illegal addressing of the source operand.

| | |
|-----------------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register is used to access memory and it contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | The VERR and VERW instructions are not recognized in real-address mode. If the LOCK prefix is used. |
|-----|--|

Virtual-8086 Mode Exceptions

| | |
|-----|--|
| #UD | The VERR and VERW instructions are not recognized in virtual-8086 mode. If the LOCK prefix is used. |
|-----|--|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used. |

WAIT/FWAIT—Wait

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|---------------------|---|
| 9B | WAIT | Valid | Valid | Check pending unmasked floating-point exceptions. |
| 9B | FWAIT | Valid | Valid | Check pending unmasked floating-point exceptions. |

Description

Causes the processor to check for and handle pending, unmasked, floating-point exceptions before proceeding. (FWAIT is an alternate mnemonic for WAIT.)

This instruction is useful for synchronizing exceptions in critical sections of code. Coding a WAIT instruction after a floating-point instruction insures that any unmasked floating-point exceptions the instruction may raise are handled before the processor can modify the instruction's results. See the section titled "Floating-Point Exception Synchronization" in Chapter 8 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1*, for more information on using the WAIT/FWAIT instruction.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

Operation

CheckForPendingUnmaskedFloatingPointExceptions;

FPU Flags Affected

The C0, C1, C2, and C3 flags are undefined.

Floating-Point Exceptions

None.

Protected Mode Exceptions

#NM If CR0.MP[bit 1] = 1 and CR0.TS[bit 3] = 1.

#UD If the LOCK prefix is used.

Real-Address Mode Exceptions

Same exceptions as in protected mode.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

WBINVD—Write Back and Invalidate Cache

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|--|
| 0F 09 | WBINVD | Valid | Valid | Write back and flush Internal caches; initiate writing-back and flushing of external caches. |

Description

Writes back all modified cache lines in the processor's internal cache to main memory and invalidates (flushes) the internal caches. The instruction then issues a special-function bus cycle that directs external caches to also write back modified data and another bus cycle to indicate that the external caches should be invalidated.

After executing this instruction, the processor does not wait for the external caches to complete their write-back and flushing operations before proceeding with instruction execution. It is the responsibility of hardware to respond to the cache write-back and flush signals.

The WBINVD instruction is a privileged instruction. When the processor is running in protected mode, the CPL of a program or procedure must be 0 to execute this instruction. This instruction is also a serializing instruction (see "Serializing Instructions" in Chapter 9 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A*).

In situations where cache coherency with main memory is not a concern, software can use the INVD instruction.

This instruction's operation is the same in non-64-bit modes and 64-bit mode.

IA-32 Architecture Compatibility

The WBINVD instruction is implementation dependent, and its function may be implemented differently on future Intel 64 and IA-32 processors. The instruction is not supported on IA-32 processors earlier than the Intel486 processor.

Operation

```
WriteBack(InternalCaches);
Flush(InternalCaches);
SignalWriteBack(ExternalCaches);
SignalFlush(ExternalCaches);
Continue; (* Continue execution *)
```

Flags Affected

None.

Protected Mode Exceptions

- #GP(0) If the current privilege level is not 0.
- #UD If the LOCK prefix is used.

Real-Address Mode Exceptions

- #UD If the LOCK prefix is used.

Virtual-8086 Mode Exceptions

- #GP(0) WBINVD cannot be executed at the virtual-8086 mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

WRMSR—Write to Model Specific Register

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|--------|-------------|-------------|------------------|---|
| 0F 30 | WRMSR | Valid | Valid | Write the value in EDX:EAX to MSR specified by ECX. |

Description

Writes the contents of registers EDX:EAX into the 64-bit model specific register (MSR) specified in the ECX register. (On processors that support the Intel 64 architecture, the high-order 32 bits of RCX are ignored.) The contents of the EDX register are copied to high-order 32 bits of the selected MSR and the contents of the EAX register are copied to low-order 32 bits of the MSR. (On processors that support the Intel 64 architecture, the high-order 32 bits of each of RAX and RDX are ignored.) Undefined or reserved bits in an MSR should be set to values previously read.

This instruction must be executed at privilege level 0 or in real-address mode; otherwise, a general protection exception #GP(0) is generated. Specifying a reserved or unimplemented MSR address in ECX will also cause a general protection exception. The processor will also generate a general protection exception if software attempts to write to bits in a reserved MSR.

When the WRMSR instruction is used to write to an MTRR, the TLBs are invalidated. This includes global entries (see “Translation Lookaside Buffers (TLBs)” in Chapter 3 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A*).

MSRs control functions for testability, execution tracing, performance-monitoring and machine check errors. Appendix B, “Model-Specific Registers (MSRs)”, in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*, lists all MSRs that can be read with this instruction and their addresses. Note that each processor family has its own set of MSRs.

The WRMSR instruction is a serializing instruction (see “Serializing Instructions” in Chapter 7 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A*).

The CPUID instruction should be used to determine whether MSRs are supported (CPUID.01H:EDX[5] = 1) before using this instruction.

IA-32 Architecture Compatibility

The MSRs and the ability to read them with the WRMSR instruction were introduced into the IA-32 architecture with the Pentium processor. Execution of this instruction by an IA-32 processor earlier than the Pentium processor results in an invalid opcode exception #UD.

Operation

MSR[ECX] ← EDX:EAX;

Flags Affected

None.

Protected Mode Exceptions

- | | |
|--------|--|
| #GP(0) | If the current privilege level is not 0. If the value in ECX specifies a reserved or unimplemented MSR address. If the value in EDX:EAX sets bits that are reserved in the MSR specified by ECX. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

- | | |
|-----|--|
| #GP | If the value in ECX specifies a reserved or unimplemented MSR address. If the value in EDX:EAX sets bits that are reserved in the MSR specified by ECX. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

- | | |
|--------|---|
| #GP(0) | The WRMSR instruction is not recognized in virtual-8086 mode. |
|--------|---|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

XADD—Exchange and Add

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------------|-----------------|-------------|---------------------|--|
| OF C0 /r | XADD r/m8, r8 | Valid | Valid | Exchange r8 and r/m8; load sum into r/m8. |
| REX + OF C0 /r | XADD r/m8*, r8* | Valid | N.E. | Exchange r8 and r/m8; load sum into r/m8. |
| OF C1 /r | XADD r/m16, r16 | Valid | Valid | Exchange r16 and r/m16; load sum into r/m16. |
| OF C1 /r | XADD r/m32, r32 | Valid | Valid | Exchange r32 and r/m32; load sum into r/m32. |
| REX.W + OF C1 /r | XADD r/m64, r64 | Valid | N.E. | Exchange r64 and r/m64; load sum into r/m64. |

NOTES:

* In 64-bit mode, r/m8 can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Exchanges the first operand (destination operand) with the second operand (source operand), then loads the sum of the two values into the destination operand. The destination operand can be a register or a memory location; the source operand is a register.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

IA-32 Architecture Compatibility

IA-32 processors earlier than the Intel486 processor do not recognize this instruction. If this instruction is used, you should provide an equivalent code sequence that runs on earlier processors.

Operation

```
TEMP ← SRC + DEST;
SRC ← DEST;
DEST ← TEMP;
```

Flags Affected

The CF, PF, AF, SF, ZF, and OF flags are set according to the result of the addition, which is stored in the destination operand.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination is located in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

XCHG—Exchange Register/Memory with Register

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-----------------------|--------------------------------|-------------|------------------|---|
| 90+ <i>rw</i> | XCHG AX, <i>r16</i> | Valid | Valid | Exchange <i>r16</i> with AX. |
| 90+ <i>rw</i> | XCHG <i>r16</i> , AX | Valid | Valid | Exchange AX with <i>r16</i> . |
| 90+ <i>rd</i> | XCHG EAX, <i>r32</i> | Valid | Valid | Exchange <i>r32</i> with EAX. |
| REX.W + 90+ <i>rd</i> | XCHG RAX, <i>r64</i> | Valid | N.E. | Exchange <i>r64</i> with RAX. |
| 90+ <i>rd</i> | XCHG <i>r32</i> , EAX | Valid | Valid | Exchange EAX with <i>r32</i> . |
| REX.W + 90+ <i>rd</i> | XCHG <i>r64</i> , RAX | Valid | N.E. | Exchange RAX with <i>r64</i> . |
| 86 <i>lr</i> | XCHG <i>r/m8</i> , <i>r8</i> | Valid | Valid | Exchange <i>r8</i> (byte register) with byte from <i>r/m8</i> . |
| REX + 86 <i>lr</i> | XCHG <i>r/m8*</i> , <i>r8*</i> | Valid | N.E. | Exchange <i>r8</i> (byte register) with byte from <i>r/m8</i> . |
| 86 <i>lr</i> | XCHG <i>r8</i> , <i>r/m8</i> | Valid | Valid | Exchange byte from <i>r/m8</i> with <i>r8</i> (byte register). |
| REX + 86 <i>lr</i> | XCHG <i>r8*</i> , <i>r/m8*</i> | Valid | N.E. | Exchange byte from <i>r/m8</i> with <i>r8</i> (byte register). |
| 87 <i>lr</i> | XCHG <i>r/m16</i> , <i>r16</i> | Valid | Valid | Exchange <i>r16</i> with word from <i>r/m16</i> . |
| 87 <i>lr</i> | XCHG <i>r16</i> , <i>r/m16</i> | Valid | Valid | Exchange word from <i>r/m16</i> with <i>r16</i> . |
| 87 <i>lr</i> | XCHG <i>r/m32</i> , <i>r32</i> | Valid | Valid | Exchange <i>r32</i> with doubleword from <i>r/m32</i> . |
| REX.W + 87 <i>lr</i> | XCHG <i>r/m64</i> , <i>r64</i> | Valid | N.E. | Exchange <i>r64</i> with quadword from <i>r/m64</i> . |
| 87 <i>lr</i> | XCHG <i>r32</i> , <i>r/m32</i> | Valid | Valid | Exchange doubleword from <i>r/m32</i> with <i>r32</i> . |
| REX.W + 87 <i>lr</i> | XCHG <i>r64</i> , <i>r/m64</i> | Valid | N.E. | Exchange quadword from <i>r/m64</i> with <i>r64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Exchanges the contents of the destination (first) and source (second) operands. The operands can be two general-purpose registers or a register and a memory location. If a memory operand is referenced, the processor's locking protocol is automatically implemented for the duration of the exchange operation, regardless of the presence

or absence of the LOCK prefix or of the value of the IOPL. (See the LOCK prefix description in this chapter for more information on the locking protocol.)

This instruction is useful for implementing semaphores or similar data structures for process synchronization. (See "Bus Locking" in Chapter 7 of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A*, for more information on bus locking.)

The XCHG instruction can also be used instead of the BSWAP instruction for 16-bit operands.

In 64-bit mode, the instruction's default operation size is 32 bits. Using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

TEMP ← DEST;
 DEST ← SRC;
 SRC ← TEMP;

Flags Affected

None.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | If either operand is in a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF (fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |

#UD If the LOCK prefix is used but the destination is not a memory operand.

Virtual-8086 Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF (fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made.

#UD If the LOCK prefix is used but the destination is not a memory operand.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

#PF (fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

#UD If the LOCK prefix is used but the destination is not a memory operand.

XGETBV—Get Value of Extended Control Register

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|-------------|-------------|-----------------|---|
| OF 01 D0 | XGETBV | Valid | Valid | Reads an XCR specified by ECX into EDX:EAX. |

Description

Reads the contents of the extended control register (XCR) specified in the ECX register into registers EDX:EAX. (On processors that support the Intel 64 architecture, the high-order 32 bits of RCX are ignored.) The EDX register is loaded with the high-order 32 bits of the XCR and the EAX register is loaded with the low-order 32 bits. (On processors that support the Intel 64 architecture, the high-order 32 bits of each of RAX and RDX are cleared.) If fewer than 64 bits are implemented in the XCR being read, the values returned to EDX:EAX in unimplemented bit locations are undefined.

Specifying a reserved or unimplemented XCR in ECX causes a general protection exception.

Currently, only XCR0 (the XFEATURE_ENABLED_MASK register) is supported. Thus, all other values of ECX are reserved and will cause a #GP(0).

Operation

EDX:EAX ← XCR[ECX];

Flags Affected

None.

Protected Mode Exceptions

- #GP(0) If an invalid XCR is specified in ECX.
- #UD If CPUID.01H:ECX.XSAVE[bit 26] = 0.
If CR4.OSXSAVE[bit 18] = 0.
If the LOCK prefix is used.
If 66H, F3H or F2H prefix is used.

Real-Address Mode Exceptions

- #GP If an invalid XCR is specified in ECX.
- #UD If CPUID.01H:ECX.XSAVE[bit 26] = 0.
If CR4.OSXSAVE[bit 18] = 0.
If the LOCK prefix is used.

If 66H, F3H or F2H prefix is used.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

XLAT/XLATB—Table Look-up Translation

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|------------|----------------|-------------|------------------|---|
| D7 | XLAT <i>m8</i> | Valid | Valid | Set AL to memory byte DS:[(E)BX + unsigned AL]. |
| D7 | XLATB | Valid | Valid | Set AL to memory byte DS:[(E)BX + unsigned AL]. |
| REX.W + D7 | XLATB | Valid | N.E. | Set AL to memory byte [RBX + unsigned AL]. |

Description

Locates a byte entry in a table in memory, using the contents of the AL register as a table index, then copies the contents of the table entry back into the AL register. The index in the AL register is treated as an unsigned integer. The XLAT and XLATB instructions get the base address of the table in memory from either the DS:EBX or the DS:BX registers (depending on the address-size attribute of the instruction, 32 or 16, respectively). (The DS segment may be overridden with a segment override prefix.)

At the assembly-code level, two forms of this instruction are allowed: the “explicit-operand” form and the “no-operand” form. The explicit-operand form (specified with the XLAT mnemonic) allows the base address of the table to be specified explicitly with a symbol. This explicit-operands form is provided to allow documentation; however, note that the documentation provided by this form can be misleading. That is, the symbol does not have to specify the correct base address. The base address is always specified by the DS: (E)BX registers, which must be loaded correctly before the XLAT instruction is executed.

The no-operands form (XLATB) provides a “short form” of the XLAT instructions. Here also the processor assumes that the DS: (E)BX registers contain the base address of the table.

In 64-bit mode, operation is similar to that in legacy or compatibility mode. AL is used to specify the table index (the operand size is fixed at 8 bits). RBX, however, is used to specify the table’s base address. See the summary chart at the beginning of this section for encoding data and limits.

Operation

```
IF AddressSize = 16
  THEN
    AL ← (DS:BX + ZeroExtend(AL));
  ELSE IF (AddressSize = 32)
    AL ← (DS:EBX + ZeroExtend(AL)); FI;
  ELSE (AddressSize = 64)
```

AL ← (RBX + ZeroExtend(AL));
 FI;

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |
| #UD | If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs. |
| #UD | If the LOCK prefix is used. |

XOR—Logical Exclusive OR

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------------------|---------------------------------|-------------|------------------|---|
| 34 <i>ib</i> | XOR AL, <i>imm8</i> | Valid | Valid | AL XOR <i>imm8</i> . |
| 35 <i>iw</i> | XOR AX, <i>imm16</i> | Valid | Valid | AX XOR <i>imm16</i> . |
| 35 <i>id</i> | XOR EAX, <i>imm32</i> | Valid | Valid | EAX XOR <i>imm32</i> . |
| REX.W + 35 <i>id</i> | XOR RAX, <i>imm32</i> | Valid | N.E. | RAX XOR <i>imm32</i> (<i>sign-extended</i>). |
| 80 /6 <i>ib</i> | XOR <i>r/m8</i> , <i>imm8</i> | Valid | Valid | <i>r/m8</i> XOR <i>imm8</i> . |
| REX + 80 /6 <i>ib</i> | XOR <i>r/m8*</i> , <i>imm8</i> | Valid | N.E. | <i>r/m8</i> XOR <i>imm8</i> . |
| 81 /6 <i>iw</i> | XOR <i>r/m16</i> , <i>imm16</i> | Valid | Valid | <i>r/m16</i> XOR <i>imm16</i> . |
| 81 /6 <i>id</i> | XOR <i>r/m32</i> , <i>imm32</i> | Valid | Valid | <i>r/m32</i> XOR <i>imm32</i> . |
| REX.W + 81 /6 <i>id</i> | XOR <i>r/m64</i> , <i>imm32</i> | Valid | N.E. | <i>r/m64</i> XOR <i>imm32</i> (<i>sign-extended</i>). |
| 83 /6 <i>ib</i> | XOR <i>r/m16</i> , <i>imm8</i> | Valid | Valid | <i>r/m16</i> XOR <i>imm8</i> (<i>sign-extended</i>). |
| 83 /6 <i>ib</i> | XOR <i>r/m32</i> , <i>imm8</i> | Valid | Valid | <i>r/m32</i> XOR <i>imm8</i> (<i>sign-extended</i>). |
| REX.W + 83 /6 <i>ib</i> | XOR <i>r/m64</i> , <i>imm8</i> | Valid | N.E. | <i>r/m64</i> XOR <i>imm8</i> (<i>sign-extended</i>). |
| 30 / <i>r</i> | XOR <i>r/m8</i> , <i>r8</i> | Valid | Valid | <i>r/m8</i> XOR <i>r8</i> . |
| REX + 30 / <i>r</i> | XOR <i>r/m8*</i> , <i>r8*</i> | Valid | N.E. | <i>r/m8</i> XOR <i>r8</i> . |
| 31 / <i>r</i> | XOR <i>r/m16</i> , <i>r16</i> | Valid | Valid | <i>r/m16</i> XOR <i>r16</i> . |
| 31 / <i>r</i> | XOR <i>r/m32</i> , <i>r32</i> | Valid | Valid | <i>r/m32</i> XOR <i>r32</i> . |
| REX.W + 31 / <i>r</i> | XOR <i>r/m64</i> , <i>r64</i> | Valid | N.E. | <i>r/m64</i> XOR <i>r64</i> . |
| 32 / <i>r</i> | XOR <i>r8</i> , <i>r/m8</i> | Valid | Valid | <i>r8</i> XOR <i>r/m8</i> . |
| REX + 32 / <i>r</i> | XOR <i>r8*</i> , <i>r/m8*</i> | Valid | N.E. | <i>r8</i> XOR <i>r/m8</i> . |
| 33 / <i>r</i> | XOR <i>r16</i> , <i>r/m16</i> | Valid | Valid | <i>r16</i> XOR <i>r/m16</i> . |
| 33 / <i>r</i> | XOR <i>r32</i> , <i>r/m32</i> | Valid | Valid | <i>r32</i> XOR <i>r/m32</i> . |
| REX.W + 33 / <i>r</i> | XOR <i>r64</i> , <i>r/m64</i> | Valid | N.E. | <i>r64</i> XOR <i>r/m64</i> . |

NOTES:

* In 64-bit mode, *r/m8* can not be encoded to access the following byte registers if a REX prefix is used: AH, BH, CH, DH.

Description

Performs a bitwise exclusive OR (XOR) operation on the destination (first) and source (second) operands and stores the result in the destination operand location. The source operand can be an immediate, a register, or a memory location; the destination operand can be a register or a memory location. (However, two memory operands cannot be used in one instruction.) Each bit of the result is 1 if the corresponding bits of the operands are different; each bit is 0 if the corresponding bits are the same.

This instruction can be used with a LOCK prefix to allow the instruction to be executed atomically.

In 64-bit mode, using a REX prefix in the form of REX.R permits access to additional registers (R8-R15). Using a REX prefix in the form of REX.W promotes operation to 64 bits. See the summary chart at the beginning of this section for encoding data and limits.

Operation

DEST ← DEST XOR SRC;

Flags Affected

The OF and CF flags are cleared; the SF, ZF, and PF flags are set according to the result. The state of the AF flag is undefined.

Protected Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the destination operand points to a non-writable segment. If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. If the DS, ES, FS, or GS register contains a NULL segment selector. |
| #SS(0) | If a memory operand effective address is outside the SS segment limit. |
| #PF(fault-code) | If a page fault occurs. |
| #AC(0) | If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3. |
| #UD | If the LOCK prefix is used but the destination is not a memory operand. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #GP | If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| #SS | If a memory operand effective address is outside the SS segment limit. |

#UD If the LOCK prefix is used but the destination is not a memory operand.

Virtual-8086 Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF (fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made.

#UD If the LOCK prefix is used but the destination is not a memory operand.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

#SS(0) If a memory address referencing the SS segment is in a non-canonical form.

#GP(0) If the memory address is in a non-canonical form.

#PF (fault-code) If a page fault occurs.

#AC(0) If alignment checking is enabled and an unaligned memory reference is made while the current privilege level is 3.

#UD If the LOCK prefix is used but the destination is not a memory operand.

XORPD—Bitwise Logical XOR for Double-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|-------------|--------------------------------------|-------------|------------------|--|
| 66 0F 57 /r | XORPD <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Bitwise exclusive-OR of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical exclusive-OR of the two packed double-precision floating-point values from the source operand (second operand) and the destination operand (first operand), and stores the result in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[127:0] ← DEST[127:0] BitwiseXOR SRC[127:0];

Intel C/C++ Compiler Intrinsic Equivalent

XORPD `__m128d _mm_xor_pd(__m128d a, __m128d b)`

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

- #GP(0) For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments.
If a memory operand is not aligned on a 16-byte boundary, regardless of segment.
- #SS(0) For an illegal address in the SS segment.
- #PF (fault-code) For a page fault.
- #NM If CR0.TS[bit 3] = 1.
- #UD If CR0.EM[bit 2] = 1.
If CR4.OSFXSR[bit 9] = 0.
If CPUID.01H:EDX.SSE2[bit 26] = 0.
If the LOCK prefix is used.

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE2[bit 26] = 0. If the LOCK prefix is used. |

XORPS—Bitwise Logical XOR for Single-Precision Floating-Point Values

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|--------------------------------------|-------------|------------------|--|
| OF 57 /r | XORPS <i>xmm1</i> , <i>xmm2/m128</i> | Valid | Valid | Bitwise exclusive-OR of <i>xmm2/m128</i> and <i>xmm1</i> . |

Description

Performs a bitwise logical exclusive-OR of the four packed single-precision floating-point values from the source operand (second operand) and the destination operand (first operand), and stores the result in the destination operand. The source operand can be an XMM register or a 128-bit memory location. The destination operand is an XMM register.

In 64-bit mode, using a REX prefix in the form of REX.R permits this instruction to access additional registers (XMM8-XMM15).

Operation

DEST[127:0] ← DEST[127:0] BitwiseXOR SRC[127:0];

Intel C/C++ Compiler Intrinsic Equivalent

XORPS `__m128_mm_xor_ps(__m128 a, __m128 b)`

SIMD Floating-Point Exceptions

None.

Protected Mode Exceptions

| | |
|------------------|---|
| #GP(0) | For an illegal memory operand effective address in the CS, DS, ES, FS or GS segments. If a memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #SS(0) | For an illegal address in the SS segment. |
| #PF (fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | If a memory operand is not aligned on a 16-byte boundary, regardless of segment. If any part of the operand lies outside the effective address space from 0 to FFFFH. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

Virtual-8086 Mode Exceptions

Same exceptions as in real address mode.

| | |
|-----------------|-------------------|
| #PF(fault-code) | For a page fault. |
|-----------------|-------------------|

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If memory operand is not aligned on a 16-byte boundary, regardless of segment. |
| #PF(fault-code) | For a page fault. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CR0.EM[bit 2] = 1. If CR4.OSFXSR[bit 9] = 0. If CPUID.01H:EDX.SSE[bit 25] = 0. If the LOCK prefix is used. |

XRSTOR—Restore Processor Extended States

| Opcode | Instruction | 64-Bit Mode | Compat/ Leg Mode | Description |
|----------|-------------------|-------------|------------------|--|
| OF AE /5 | XRSTOR <i>mem</i> | Valid | Valid | Restore processor extended states from <i>memory</i> . The states are specified by EDX:EAX |

Description

Performs a full or partial restore of the enabled processor states using the state information stored in the memory address specified by the source operand. The implicit EDX:EAX register pair specifies a 64-bit restore mask.

The format of the XSAVE/XRSTOR area is shown in Table 4-8. The memory layout of the XSAVE/XRSTOR area may have holes between save areas written by the processor as a result of the processor not supporting certain processor extended states or system software not supporting certain processor extended states.

Table 4-8. General Layout of XSAVE/XRSTOR Save Area

| Save Areas | Offset (Byte) | Size (Bytes) |
|----------------------------|----------------------------|----------------------------|
| FPU/SSE SaveArea | 0 | 512 |
| Header | 512 | 64 |
| Reserved (Ext_Save_Area_2) | CPUID.(EAX=0DH, ECX=2):EBX | CPUID.(EAX=0DH, ECX=2):EAX |
| Reserved(Ext_Save_Area_3) | CPUID.(EAX=0DH, ECX=3):EBX | CPUID.(EAX=0DH, ECX=3):EAX |
| Reserved(Ext_Save_Area_4) | CPUID.(EAX=0DH, ECX=4):EBX | CPUID.(EAX=0DH, ECX=4):EAX |
| Reserved(...) | ... | ... |

XRSTOR operates on each subset of the processor state or a processor extended state in one of three ways (depending on the corresponding bit in the XFEATURE_ENABLED_MASK register (XCRO), the restore mask EDX:EAX, and the save mask XSAVE.HEADER.XSTATE_BV in memory):

- Updates the processor state component using the state information stored in the respective save area (see Table 4-8) of the source operand, if the corresponding bit in XCRO, EDX:EAX, and XSAVE.HEADER.XSTATE_BV are all 1.
- Writes certain registers in the processor state component using processor-supplied values (see Table 4-10) without using state information stored in respective save area of the memory region, if the corresponding bit in XCRO and

EDX:EAX are both 1, but the corresponding bit in XSAVE.HEADER.XSTATE_BV is 0.

- The processor state component is unchanged, if the corresponding bit in XCRO or EDX:EAX is 0.

The format of the header section (XSAVE.HEADER) of the XSAVE/XRSTOR area is shown in Table 4-9.

Table 4-9. XSAVE.HEADER Layout

| 15 | 8 | 7 | 0 | Byte Offset from Header | Byte Offset from XSAVE/XRSTOR Area |
|----|-------------------|---|-------------------|-------------------------|------------------------------------|
| | Rsrvd (Must be 0) | | XSTATE_BV | 0 | 512 |
| | Reserved | | Rsrvd (Must be 0) | 16 | 528 |
| | Reserved | | Reserved | 32 | 544 |
| | Reserved | | Reserved | 48 | 560 |

If a processor state component is not enabled in XCRO but the corresponding save mask bit in XSAVE.HEADER.XSTATE_BV is 1, an attempt to execute XRSTOR will cause a #GP(0) exception. Software may specify all 1's in the implicit restore mask EDX:EAX, so that all the enabled processors states in XCRO are restored from state information stored in memory or from processor supplied values.

An attempt to restore processor states with writing 1s to reserved bits in certain registers (see Table 4-11) will cause a #GP(0) exception.

Because bit 63 of the XFEATURE_ENABLED_MASK register is reserved for future bit vector expansion, it will not be used for any future processor state feature, and XRSTOR will ignore bit 63 of EDX:EAX (EDX[31]).

Table 4-10. Processor Supplied Init Values XRSTOR May Use

| Processor State Component | Processor Supplied Register Values |
|---------------------------|---|
| x87 FPU State | FCW ← 037FH; FTW ← 0FFFFH; FSW ← 0H; FPU CS ← 0H; FPU DS ← 0H; FPU IP ← 0H; FPU DP ← 0; ST0-ST7 ← 0; |
| SSE State ¹ | If 64-bit Mode: XMM0-XMM15 ← 0H; Else XMM0-XMM7 ← 0H |

NOTES:

1. MXCSR state is not updated by processor supplied values. MXCSR state can only be updated by XRSTOR from state information stored in XSAVE/XRSTOR area.

Table 4-11. Reserved Bit Checking and XRSTOR

| Processor State Component | Reserved Bit Checking |
|---------------------------|------------------------|
| X87 FPU State | None |
| SSE State | Reserved bits of MXCSR |

A source operand not aligned to 64-byte boundary (for 64-bit and 32-bit modes) will result in a general-protection (#GP) exception. In 64-bit mode, the upper 32 bits of RDX and RAX are ignored.

Operation

/ The alignment of the x87 and SSE fields in the XSAVE area is the same as in FXSAVE area*/*

```
RS_TMP_MASK[62:0] ← (EDX[30:0] << 32 ) OR EAX[31:0];
ST_TMP_MASK[62:0] ← SRCMEM.HEADER.XSTATE_BV[62:0];
IF ( ( (XCRO[62:0] XOR 7FFFFFFF_FFFFFFFFH ) AND ST_TMP_MASK[62:0] ) )
    THEN
        #GP(0)
    ELSE
        FOR i = 0, 62 STEP 1
            IF ( RS_TMP_MASK[i] and XCRO[i] )
                THEN
                    IF ( ST_TMP_MASK[i] )
                        CASE ( i ) OF
                            0: Processor state[x87 FPU] ← SRCMEM.FPUSSESave_Area[FPU];
                            1: Processor state[SSE] ← SRCMEM.FPUSSESave_Area[SSE];
                               // MXCSR is loaded as part of the SSE state
                        DEFAULT: // i corresponds to a valid sub-leaf index of CPUID leaf 0DH
                               Processor state[i] ← SRCMEM.Ext_Save_Area[ i ];
                        ESAC;
                    ELSE
                        Processor extended state[i] ← Processor supplied values; (see Table 4-10)
                        CASE ( i ) OF
                            1: MXCSR ← SRCMEM.FPUSSESave_Area[SSE];
                        ESAC;
                    FI;
                FI;
            NEXT;
        FI;
```

Flags Affected

None.

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | <p>If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If a memory operand is not aligned on a 64-byte boundary, regardless of segment.</p> <p>If a bit in XCRO is 0 and the corresponding bit in HEADER.XSTATE_BV field of the source operand is 1.</p> <p>If bytes 23:8 of HEADER is not zero.</p> <p>If attempting to write any reserved bits of the MXCSR register with 1.</p> |
| #SS(0) | <p>If a memory operand effective address is outside the SS segment limit.</p> |
| #PF(fault-code) | <p>If a page fault occurs.</p> |
| #NM | <p>If CR0.TS[bit 3] = 1.</p> |
| #UD | <p>If CPUID.01H:ECX.XSAVE[bit 26] = 0.</p> <p>If CR4.OSXSAVE[bit 18] = 0.</p> <p>If the LOCK prefix is used.</p> <p>If 66H, F3H or F2H prefix is used.</p> |

Real-Address Mode Exceptions

| | |
|-----|--|
| #GP | <p>If a memory operand is not aligned on a 64-byte boundary, regardless of segment.</p> <p>If any part of the operand lies outside the effective address space from 0 to FFFFH.</p> <p>If a bit in XCRO is 0 and the corresponding bit in HEADER.XSTATE_BV field of the source operand is 1.</p> <p>If bytes 23:8 of HEADER is not zero.</p> <p>If attempting to write any reserved bits of the MXCSR register with 1.</p> |
| #NM | <p>If CR0.TS[bit 3] = 1.</p> |
| #UD | <p>If CPUID.01H:ECX.XSAVE[bit 26] = 0.</p> <p>If CR4.OSXSAVE[bit 18] = 0.</p> <p>If the LOCK prefix is used.</p> <p>If 66H, F3H or F2H prefix is used.</p> |

Virtual-8086 Mode Exceptions

Same exceptions as in Protected Mode

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | <p>If the memory address is in a non-canonical form.</p> <p>If a memory operand is not aligned on a 64-byte boundary, regardless of segment.</p> <p>If a bit in XCRO is 0 and the corresponding bit in XSAVE.HEADER.XSTATE_BV is 1.</p> <p>If bytes 23: 8 of HEADER is not zero.</p> <p>If attempting to write any reserved bits of the MXCSR register with 1.</p> |
| #SS(0) | <p>If a memory address referencing the SS segment is in a non-canonical form.</p> |
| #PF(fault-code) | <p>If a page fault occurs.</p> |
| #NM | <p>If CR0.TS[bit 3] = 1.</p> |
| #UD | <p>If CPUID.01H: ECX.XSAVE[bit 26] = 0.</p> <p>If CR4.OSXSAVE[bit 18] = 0.</p> <p>If the LOCK prefix is used.</p> <p>If 66H, F3H or F2H prefix is used.</p> |

XSAVE—Save Processor Extended States

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|------------------|-------------|-----------------|---|
| OF AE /4 | XSAVE <i>mem</i> | Valid | Valid | Save processor extended states to <i>memory</i> . The states are specified by EDX:EAX |

Description

Performs a full or partial save of the enabled processor state components to a memory address specified in the destination operand. A full or partial save of the processor states is specified by an implicit mask operand via the register pair, EDX:EAX. The destination operand is a memory location that must be 64-byte aligned.

The implicit 64-bit mask operand in EDX:EAX specifies the subset of enabled processor state components to save into the XSAVE/XRSTOR save area. The XSAVE/XRSTOR save area comprises of individual save area for each processor state components and a header section, see Table 4-8. Each component save area is written if both the corresponding bits in the save mask operand and in the XFEATURE_ENABLED_MASK (XCRO) register are 1. A processor state component save area is not updated if either one of the corresponding bits in the mask operand or the XFEATURE_ENABLED_MASK register is 0. If the mask operand (EDX:EAX) contains all 1's, all enabled processor state components in XFEATURE_ENABLED_MASK is written to the respective component save area.

The bit assignment used for the EDX:EAX register pair matches the XFEATURE_ENABLED_MASK register (see chapter 2 of Vol. 3B). For the XSAVE instruction, software can specify "1" in any bit position of EDX:EAX, irrespective of whether the corresponding bit position in XFEATURE_ENABLED_MASK is valid for the processor. The bit vector in EDX:EAX is "anded" with the XFEATURE_ENABLED_MASK to determine which save area will be written.

The content layout of the XSAVE/XRSTOR save area is architecturally defined to be extendable and enumerated via the sub-leaves of CPUID.0DH leaf. The extendable framework of the XSAVE/XRSTOR layout is depicted by Table 4-8. The layout of the XSAVE/XRSTOR save area is fixed and may contain non-contiguous individual save areas. The XSAVE/XRSTOR save area is not compacted if some features are not saved or are not supported by the processor and/or by system software.

The layout of the register fields of first 512 bytes of the XSAVE/XRSTOR is the same as the FXSAVE/FXRSTOR area. But XSAVE/XRSTOR organizes the 512 byte area as x87 FPU states (including FPU operation states, x87/MMX data registers), MXCSR (including MXCSR_MASK), and XMM registers (see Table 4-12). For details of individual FPU register layout, refer to the FXSAVE instruction.

Table 4-12. XSAVE Save Area Layout for x87 FPU and SSE State

| 31 | 28 | 27 | 24 | 23 | 20 | 19 | 16 | 15 | 12 | 11 | 8 | 7 | 4 | 3 | 0 | |
|---|----|----|----|---|----|----|----|----------|----|----|---|---|---|---|---|-----|
| MXCSR and MASK | | | | x87 FPU operation states (see FXSAVE instruction) | | | | | | | | | | | 0 | |
| x87/MMX data registers (see FXSAVE instruction) | | | | | | | | | | | | | | | | 32 |
| x87/MMX data registers (see FXSAVE instruction) | | | | | | | | | | | | | | | | 64 |
| x87/MMX data registers (see FXSAVE instruction) | | | | | | | | | | | | | | | | 96 |
| x87/MMX data registers (see FXSAVE instruction) | | | | | | | | | | | | | | | | 128 |
| XMM1 | | | | | | | | XMM0 | | | | | | | | 160 |
| XMM3 | | | | | | | | XMM2 | | | | | | | | 192 |
| XMM5 | | | | | | | | XMM4 | | | | | | | | 224 |
| XMM7 | | | | | | | | XMM6 | | | | | | | | 256 |
| XMM9 | | | | | | | | XMM8 | | | | | | | | 288 |
| XMM11 | | | | | | | | XMM10 | | | | | | | | 320 |
| XMM13 | | | | | | | | XMM12 | | | | | | | | 352 |
| XMM15 | | | | | | | | XMM14 | | | | | | | | 384 |
| Reserved | | | | | | | | Reserved | | | | | | | | 416 |
| Reserved | | | | | | | | Reserved | | | | | | | | 448 |
| Reserved | | | | | | | | Reserved | | | | | | | | 480 |

The processor writes 1 or 0 to each HEADER.XSTATE_BV[i] bit field of an enabled processor state component in a manner that is consistent to XRSTOR's interaction with HEADER.XSTATE_BV (see the operation section of XRSTOR instruction). If a processor implementation discerns that a processor state component is in its initial-ized state (according to Table 4-10) it may modify the corresponding bit in the HEADER.XSTATE_BV as '0'.

A destination operand not aligned to 64-byte boundary (in either 64-bit or 32-bit modes) will result in a general-protection (#GP) exception being generated. In 64-bit mode, the upper 32 bits of RDX and RAX are ignored.

Operation

$TMP_MASK[62:0] \leftarrow ((EDX[30:0] \ll 32) \text{ OR } EAX[31:0]) \text{ AND } XFEATURE_ENABLE_MASK[62:0];$

FOR $i = 0, 62$ STEP 1

 IF ($TMP_MASK[i] = 1$) THEN

 THEN

 CASE (i) of

 0: $DEST.FPUSSESAVE_Area[x87 \text{ FPU}] \leftarrow processor\ state[x87 \text{ FPU}];$

```

1: DEST.FPUSSESAVE_Area[SSE] ← processor state[SSE];
   // SSE state include MXCSR
DEFAULT: // i corresponds to a valid sub-leaf index of CPUID leaf 0DH
   DEST.Ext_Save_Area[ i ] ← processor state[ i ] ;
ESAC:
DEST.HEADER.XSTATE_BV[ i ] ← INIT_FUNCTION[ i ];

FI;
NEXT;

```

Flags Affected

None.

Protected Mode Exceptions

#GP(0) If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
If a memory operand is not aligned on a 64-byte boundary, regardless of segment.

#SS(0) If a memory operand effective address is outside the SS segment limit.

#PF(fault-code) If a page fault occurs.

#NM If CR0.TS[bit 3] = 1.

#UD If CPUID.01H: ECX.XSAVE[bit 26] = 0.
If CR4.OSXSAVE[bit 18] = 0.
If the LOCK prefix is used.
If 66H, F3H or F2H prefix is used.

Real-Address Mode Exceptions

#GP If a memory operand is not aligned on a 64-byte boundary, regardless of segment.
If any part of the operand lies outside the effective address space from 0 to FFFFH.

#NM If CR0.TS[bit 3] = 1.

#UD If CPUID.01H: ECX.XSAVE[bit 26] = 0.
If CR4.OSXSAVE[bit 18] = 0.
If the LOCK prefix is used.
If 66H, F3H or F2H prefix is used.

Virtual-8086 Mode Exceptions

Same exceptions as in protected mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

| | |
|------------------|--|
| #SS(0) | If a memory address referencing the SS segment is in a non-canonical form. |
| #GP(0) | If the memory address is in a non-canonical form. If a memory operand is not aligned on a 64-byte boundary, regardless of segment. |
| #PF (fault-code) | If a page fault occurs. |
| #NM | If CR0.TS[bit 3] = 1. |
| #UD | If CPUID.01H: ECX.XSAVE[bit 26] = 0. If CR4.OSXSAVE[bit 18] = 0. If the LOCK prefix is used. If 66H, F3H or F2H prefix is used. |

XSETBV—Set Extended Control Register

| Opcode | Instruction | 64-Bit Mode | Compat/Leg Mode | Description |
|----------|-------------|-------------|-----------------|---|
| OF 01 D1 | XSETBV | Valid | Valid | Write the value in EDX:EAX to the XCR specified by ECX. |

Description

Writes the contents of registers EDX:EAX into the 64-bit extended control register (XCR) specified in the ECX register. (On processors that support the Intel 64 architecture, the high-order 32 bits of RCX are ignored.) The contents of the EDX register are copied to high-order 32 bits of the selected XCR and the contents of the EAX register are copied to low-order 32 bits of the XCR. (On processors that support the Intel 64 architecture, the high-order 32 bits of each of RAX and RDX are ignored.) Undefined or reserved bits in an XCR should be set to values previously read.

This instruction must be executed at privilege level 0 or in real-address mode; otherwise, a general protection exception #GP(0) is generated. Specifying a reserved or unimplemented XCR in ECX will also cause a general protection exception. The processor will also generate a general protection exception if software attempts to write to reserved bits in an XCR.

Currently, only XCRO (the XFEATURE_ENABLED_MASK register) is supported. Thus, all other values of ECX are reserved and will cause a #GP(0). Note that bit 0 of XFEATURE_ENABLED_MASK (corresponding to x87 state) must be set to 1; the instruction will cause a #GP(0) if an attempt is made to clear this bit.

Operation

XCR[ECX] ← EDX:EAX;

Flags Affected

None.

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | <p>If the current privilege level is not 0.</p> <p>If an invalid XCR is specified in ECX.</p> <p>If the value in EDX:EAX sets bits that are reserved in the XCR specified by ECX.</p> <p>If an attempt is made to clear bit 0 of XFEATURE_ENABLED_MASK.</p> |
| #UD | <p>If CPUID.01H:ECX.XSAVE[bit 26] = 0.</p> <p>If CR4.OSXSAVE[bit 18] = 0.</p> |

If the LOCK prefix is used.
If 66H, F3H or F2H prefix is used.

Real-Address Mode Exceptions

#GP If an invalid XCR is specified in ECX.
 If the value in EDX: EAX sets bits that are reserved in the XCR specified by ECX.
 If an attempt is made to clear bit 0 of XFEATURE_ENABLED_MASK.

#UD If CPUID.01H: ECX.XSAVE[bit 26] = 0.
 If CR4.OSXSAVE[bit 18] = 0.
 If the LOCK prefix is used.
 If 66H, F3H or F2H prefix is used.

Virtual-8086 Mode Exceptions

#GP(0) The XSETBV instruction is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

Same exceptions as in protected mode.

64-Bit Mode Exceptions

Same exceptions as in protected mode.

5.1 OVERVIEW

This chapter describes the virtual-machine extensions (VMX) for the Intel 64 and IA-32 architectures. VMX is intended to support virtualization of processor hardware and a system software layer acting as a host to multiple guest software environments. The virtual-machine extensions (VMX) includes five instructions that manage the virtual-machine control structure (VMCS) and five instruction that manage VMX operation. Additional details of VMX are described in *IA-32 Intel Architecture Software Developer's Manual, Volume 3B*.

The behavior of the VMCS-maintenance instructions is summarized below:

- **VMPTRLD** — This instruction takes a single 64-bit source operand that is in memory. It makes the referenced VMCS active and current, loading the current-VMCS pointer with this operand and establishes the current VMCS based on the contents of VMCS-data area in the referenced VMCS region. Because this makes the referenced VMCS active, a logical processor may start maintaining on the processor some of the VMCS data for the VMCS.
- **VMPTRST** — This instruction takes a single 64-bit destination operand that is in memory. The current-VMCS pointer is stored into the destination operand.
- **VMCLEAR** — This instruction takes a single 64-bit operand that is in memory. The instruction sets the launch state of the VMCS referenced by the operand to “clear”, renders that VMCS inactive, and ensures that data for the VMCS have been written to the VMCS-data area in the referenced VMCS region. If the operand is the same as the current-VMCS pointer, that pointer is made invalid.
- **VMREAD** — This instruction reads a component from the VMCS (the encoding of that field is given in a register operand) and stores it into a destination operand that may be a register or in memory.
- **VMWRITE** — This instruction writes a component to the VMCS (the encoding of that field is given in a register operand) from a source operand that may be a register or in memory.

The behavior of the VMX management instructions is summarized below:

- **VMCALL** — This instruction allows a guest in VMX non-root operation to call the VMM for service. A VM exit occurs, transferring control to the VMM.
- **VMLAUNCH** — This instruction launches a virtual machine managed by the VMCS. A VM entry occurs, transferring control to the VM.
- **VMRESUME** — This instruction resumes a virtual machine managed by the VMCS. A VM entry occurs, transferring control to the VM.
- **VMXOFF** — This instruction causes the processor to leave VMX operation.

- **VMXON** — This instruction takes a single 64-bit source operand that is in memory. It causes a logical processor to enter VMX root operation and to use the memory referenced by the operand to support VMX operation.

Only VMCALL can be executed in compatibility mode (causing a VM exit). The other VMX instructions generate invalid-opcode exceptions if executed in compatibility mode.

The behavior of the VMX-specific TLB-management instructions is summarized below:

- **INVEPT** — This instruction invalidates entries in the TLBs and paging-structure caches that were derived from **Extended Page Tables** (EPT).
- **INVVPID** — This instruction invalidates entries in the TLBs and paging-structure caches based on a Virtual-Processor Identifier (VPID).

5.2 CONVENTIONS

The operation sections for the VMX instructions in Section 5.3 use the pseudo-function VMexit, which indicates that the logical processor performs a VM exit.

The operation sections also use the pseudo-functions VMsucceed, VMfail, VMfailInvalid, and VMfailValid. These pseudo-functions signal instruction success or failure by setting or clearing bits in RFLAGS and, in some cases, by writing the VM-instruction error field. The following pseudocode fragments detail these functions:

VMsucceed:

```
CF ← 0;
PF ← 0;
AF ← 0;
ZF ← 0;
SF ← 0;
OF ← 0;
```

VMfail(ErrorNumber):

```
IF VMCS pointer is valid
    THEN VMfailValid(ErrorNumber);
    ELSE VMfailInvalid;
FI;
```

VMfailInvalid:

```
CF ← 1;
PF ← 0;
AF ← 0;
ZF ← 0;
SF ← 0;
```

OF ← 0;

VMfailValid(ErrorNumber);// executed only if there is a current VMCS

CF ← 0;

PF ← 0;

AF ← 0;

ZF ← 1;

SF ← 0;

OF ← 0;

Set the VM-instruction error field to ErrorNumber;

The different VM-instruction error numbers are enumerated in Section 5.4, “VM Instruction Error Numbers”.

5.3 VMX INSTRUCTIONS

This section provides detailed descriptions of the VMX instructions.

INVEPT— Invalidate Translations Derived from EPT

| Opcode | Instruction | Description |
|-------------|------------------|---|
| 66 0F 38 80 | INVEPT r64, m128 | Invalidates EPT-derived entries in the TLBs and paging-structure caches (in 64-bit mode) |
| 66 0F 38 80 | INVEPT r32, m128 | Invalidates EPT-derived entries in the TLBs and paging-structure caches (outside 64-bit mode) |

Description

Invalidates entries in the translation lookaside buffers (TLBs) and paging-structure caches that were derived from **extended page tables** (EPT). (See Chapter “Extended Page Tables” in *IA-32 Intel Architecture Software Developer’s Manual, Volume 3B*.) Invalidation is based on the **INVEPT type** specified in the register operand and the **INVEPT descriptor** specified in the memory operand.

Outside IA-32e mode, the register operand is always 32 bits, regardless of the value of CS.D. In 64-bit mode, the register operand has 64 bits; however, if bits 63:32 of the register operand are not zero, INVEPT will fail due to an attempt to use an unsupported INVEPT type (see below).

The INVEPT types supported by a logical processor are reported in the IA32_VMX_EPT_VPID_CAP MSR (see Appendix “VMX Capability Reporting Facility” in *IA-32 Intel Architecture Software Developer’s Manual, Volume 3B*). There are two INVEPT types currently defined:

- Single-context invalidation. If the INVEPT type is 1, the logical processor invalidates all translations derived from the EPT context specified in the INVEPT descriptor. In some cases, it may invalidate translations from other EPT contexts as well.
- Global invalidation: If the INVEPT type is 2, the logical processor invalidates all translations derived from any EPT context.

If an unsupported INVEPT type is specified, the instruction fails.

The INVEPT descriptor comprises 128 bits and contains a 64-bit EPT pointer value in bits 63:0 (see Figure 5-1). The 64-bit EPT pointer value defines an EPT context.

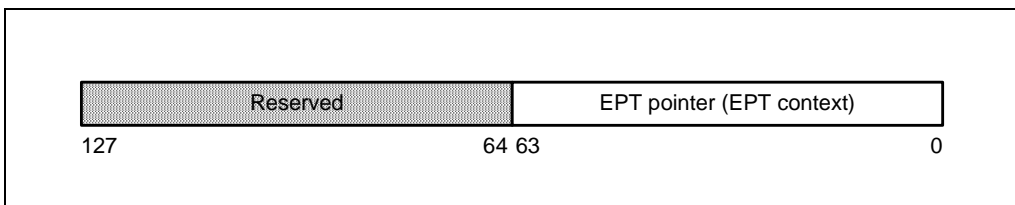


Figure 5-1. INVEPT Descriptor

Operation

```

IF (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELIF in VMX non-root operation
    THEN VM exit;
ELIF CPL > 0
    THEN #GP(0);
ELSE
    INVEPT_TYPE ← value of register operand;
    IF IA32_VMX_EPT_VPID_CAP MSR indicates that processor does not support INVEPT_TYPE
        THEN VMfail(Invalid operand to INVEPT/INVVPID);
    ELSE // INVEPT_TYPE must be 1 or 2
        INVEPT_DESC ← value of memory operand;
        EPTP_CTX ← INVEPT_DESC[63:0];
        CASE INVEPT_TYPE OF
            1: // single-context invalidation
                IF VM entry with the “enable EPT” VM execution control set to 1
                    would fail due to the EPTP field containing the value EPTP_CTX
                    THEN VMfail(Invalid operand to INVEPT/INVVPID);
                ELSE
                    Invalidate translations derived from EPT for EPTP_CTX;
                    VMSucceed;
            FI;
            BREAK;
            2: // global invalidation
                Invalidate translations derived from EPT for all EPT contexts;
                VMSucceed;
                BREAK;
        ESAC;
    FI;
FI;

```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Segment overrides | Treated normally |
| Operand size | Ignored |
| Address size | Treated normally |

REX Register extensions treated normally; operand-size overrides ignored

Protected Mode Exceptions

#GP(0) If the current privilege level is not 0.
If the memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.
If the DS, ES, FS, or GS register contains an unusable segment.
If the source operand is located in an execute-only code segment.

#PF(fault-code) If a page fault occurs in accessing the memory operand.

#SS(0) If the memory operand effective address is outside the SS segment limit.
If the SS register contains an unusable segment.

#UD If not in VMX operation.
If the logical processor does not support EPT (IA32_VMX_PROCBASED_CTL2[33]=0).
If the logical processor supports EPT (IA32_VMX_PROCBASED_CTL2[33]=1) but does not support the INVEPT instruction (IA32_VMX_EPT_VPID_CAP[20]=0).

Real-Address Mode Exceptions

#UD A logical processor cannot be in real-address mode while in VMX operation and the INVEPT instruction is not recognized outside VMX operation.

Virtual-8086 Mode Exceptions

#UD The INVEPT instruction is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

#UD The INVEPT instruction is not recognized in compatibility mode.

64-Bit Mode Exceptions

#GP(0) If the current privilege level is not 0.
If the memory operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form.

#PF(fault-code) If a page fault occurs in accessing the memory operand.

#SS(0) If the memory operand is in the SS segment and the memory address is in a non-canonical form.

#UD If not in VMX operation.

If the logical processor does not support EPT
(IA32_VMX_PROCBASED_CTL2[33]=0).

If the logical processor supports EPT
(IA32_VMX_PROCBASED_CTL2[33]=1) but does not support
the INVEPT instruction (IA32_VMX_EPT_VPID_CAP[20]=0).

INVPID— Invalidate Translations Based on VPID

| Opcode | Instruction | Description |
|-------------|------------------|---|
| 66 0F 38 81 | INVPID r64, m128 | Invalidates entries in the TLBs and paging-structure caches based on VPID (in 64-bit mode) |
| 66 0F 38 81 | INVPID r32, m128 | Invalidates entries in the TLBs and paging-structure caches based on VPID (outside 64-bit mode) |

Description

Invalidates entries in the translation lookaside buffers (TLBs) and paging-structure caches based on **virtual-processor identifier** (VPID). (See Chapter “Virtual-Processor Identifiers” in *IA-32 Intel Architecture Software Developer’s Manual, Volume 3B*.) Invalidation is based on the **INVPID type** specified in the register operand and the **INVPID descriptor** specified in the memory operand.

Outside IA-32e mode, the register operand is always 32 bits, regardless of the value of CS.D. In 64-bit mode, the register operand has 64 bits; however, if bits 63:32 of the register operand are not zero, INVPID will fail due to an attempt to use an unsupported INVPID type (see below).

The INVPID types supported by a logical processors are reported in the IA32_VMX_EPT_VPID_CAP MSR (see Appendix “VMX Capability Reporting Facility” in *IA-32 Intel Architecture Software Developer’s Manual, Volume 3B*). There are four INVPID types currently defined:

- Individual-address invalidation: If the INVPID type is 0, the logical processor invalidates translations associated with a single linear address and with the VPID specified in the INVPID descriptor. In some cases, it may invalidate translations for other linear addresses (or with other VPIDs) as well.
- Single-context invalidation: If the INVPID type is 1, the logical processor invalidates all translations associated with the VPID specified in the INVPID descriptor. In some cases, it may invalidate translations with other VPIDs as well.
- All-contexts invalidation: If the INVPID type is 2, the logical processor invalidates all translations with all VPIDs except VPID 0. In some cases, it may invalidate translations with VPID 0 as well.
- Single-context invalidation, retaining global mappings: If the INVPID type is 3, the logical processor invalidates all non-global translations associated with the VPID specified in the INVPID descriptor. In some cases, it may invalidate global translations (and those with other VPIDs) as well.

If an unsupported INVPID type is specified, the instruction fails.

The INVPID descriptor comprises 128 bits and consists of a VPID and a linear address as shown in Figure 5-2.

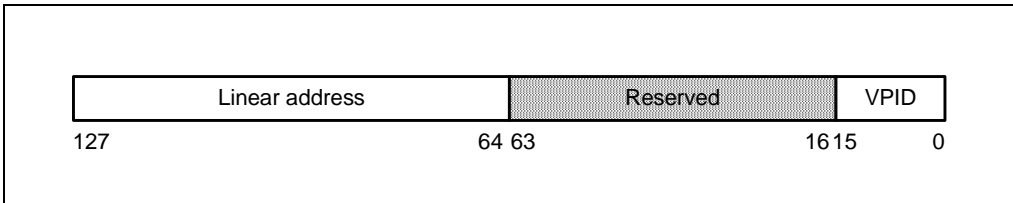


Figure 5-2. INVVPID Descriptor

Operation

```

IF (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELSIF in VMX non-root operation
    THEN VM exit;
ELSIF CPL > 0
    THEN #GP(0);
ELSE
    INVVPID_TYPE ← value of register operand;
    IF IA32_VMX_EPT_VPID_CAP MSR indicates that processor does not support
        INVVPID_TYPE
        THEN VMfail(Invalid operand to INVEPT/INVVPID);
    ELSE // INVVPID_TYPE must be in the range 0-3
        INVVPID_DESC ← value of memory operand;
        IF INVVPID_DESC[63:16] ≠ 0
            THEN VMfail(Invalid operand to INVEPT/INVVPID);
        ELSE
            CASE INVVPID_TYPE OF
                0: // individual-address invalidation
                    VPID_CTX ← INVVPID_DESC[15:0];
                    IF VPID_CTX = 0
                        THEN VMfail(Invalid operand to INVEPT/INVVPID);
                    ELSE
                        GL_ADDR ← INVVPID_DESC[127:64];
                        IF (GL_ADDR is not in a canonical form)
                            THEN
                                VMfail(Invalid operand to INVEPT/INVVPID);
                            ELSE
                                Invalidate translations for GL_ADDR
                                in VPID_CTX;
                                VMsucceed;
            FI;
        FI;
    FI;

```

```

        BREAK;
1:          // single-context invalidation
        VPID_CTX ← INVVPID_DESC[15:0];
        IF VPID_CTX = 0
            THEN VMfail(Invalid operand to INVEPT/INVVPID);
            ELSE
                Invalidate all translations in VPID_CTX;
                VMSucceed;
        FI;
        BREAK;
2:          // all-context invalidation
        Invalidate all translations of all non-zero VPID contexts;
        VMSucceed;
        BREAK;
3:          // single-context invalidation retaining globals
        VPID_CTX ← INVVPID_DESC[15:0];
        IF VPID_CTX = 0
            THEN VMfail(Invalid operand to INVEPT/INVVPID);
            ELSE
                Invalidate all non-global translations in VPID_CTX;
                VMSucceed;
        FI;
        BREAK;
        ESAC;
    FI;
FI;
```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Segment overrides | Treated normally |
| Operand size | Ignored |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

#GP(0) If the current privilege level is not 0.

| | |
|-----------------|---|
| | If the memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
| | If the DS, ES, FS, or GS register contains an unusable segment. |
| | If the source operand is located in an execute-only code segment. |
| #PF(fault-code) | If a page fault occurs in accessing the memory operand. |
| #SS(0) | If the memory operand effective address is outside the SS segment limit. |
| | If the SS register contains an unusable segment. |
| #UD | If not in VMX operation. |
| | If the logical processor does not support VPIDs (IA32_VMX_PROCBASED_CTL2[37]=0). |
| | If the logical processor supports VPIDs (IA32_VMX_PROCBASED_CTL2[37]=1) but does not support the INVVPID instruction (IA32_VMX_EPT_VPID_CAP[32]=0). |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the INVVPID instruction is not recognized outside VMX operation. |
|-----|--|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | The INVVPID instruction is not recognized in virtual-8086 mode. |
|-----|---|

Compatibility Mode Exceptions

| | |
|-----|--|
| #UD | The INVVPID instruction is not recognized in compatibility mode. |
|-----|--|

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If the current privilege level is not 0. |
| | If the memory operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs in accessing the memory operand. |
| #SS(0) | If the memory destination operand is in the SS segment and the memory address is in a non-canonical form. |
| #UD | If not in VMX operation. |
| | If the logical processor does not support VPIDs (IA32_VMX_PROCBASED_CTL2[37]=0). |
| | If the logical processor supports VPIDs (IA32_VMX_PROCBASED_CTL2[37]=1) but does not support the INVVPID instruction (IA32_VMX_EPT_VPID_CAP[32]=0). |

VMCALL—Call to VM Monitor

| Opcode | Instruction | Description |
|----------|-------------|--|
| 0F 01 C1 | VMCALL | Call to VM monitor by causing VM exit. |

Description

This instruction allows guest software can make a call for service into an underlying VM monitor. The details of the programming interface for such calls are VMM-specific; this instruction does nothing more than cause a VM exit, registering the appropriate exit reason.

Use of this instruction in VMX root operation invokes an SMM monitor (see Section 24.16.2 in *IA-32 Intel Architecture Software Developer's Manual, Volume 3B*). This invocation will activate the dual-monitor treatment of system-management interrupts (SMIs) and system-management mode (SMM) if it is not already active (see Section 24.16.6 in *IA-32 Intel Architecture Software Developer's Manual, Volume 3B*).

Operation

```

IF not in VMX operation
    THEN #UD;
ELSIF in VMX non-root operation
    THEN VM exit;
ELSIF (RFLAGS.VM = 1) OR (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELSIF CPL > 0
    THEN #GP(0);
ELSIF in SMM or the logical processor does not support the dual-monitor treatment of SMIs and SMM or the valid bit in the IA32_SMM_MONITOR_CTL MSR is clear
    THEN VMfail (VMCALL executed in VMX root operation);
ELSIF dual-monitor treatment of SMIs and SMM is active
    THEN perform an SMM VM exit (see Section 24.16.2
        of the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B);
ELSIF current-VMCS pointer is not valid
    THEN VMfailInvalid;
ELSIF launch state of current VMCS is not clear
    THEN VMfailValid (VMCALL with non-clear VMCS);
ELSIF VM-exit control fields are not valid (see Section 24.16.6.1 of the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B)
    THEN VMfailValid (VMCALL with invalid VM-exit control fields);
ELSE
    enter SMM;
    read revision identifier in MSEG;
  
```

```

IF revision identifier does not match that supported by processor
  THEN
    leave SMM;
    VMfailValid(VMCALL with incorrect MSEG revision identifier);
  ELSE
    read SMM-monitor features field in MSEG (see Section 24.16.6.2,
    in the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B);
    IF features field is invalid
      THEN
        leave SMM;
        VMfailValid(VMCALL with invalid SMM-monitor features);
      ELSE activate dual-monitor treatment of SMIs and SMM (see Section 24.16.6
      in the Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume
      3B);
    FI;
  FI;
FI;

```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|---|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPZ and REP/REPE/REPZ) |
| Segment overrides | Ignored |
| Operand size | Causes #UD |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | If the current privilege level is not 0 and the logical processor is in VMX root operation. |
| #UD | If executed outside VMX operation. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMCALL instruction is not recognized outside VMX operation. |
|-----|---|

Virtual-8086 Mode Exceptions

#UD If executed outside VMX non-root operation.

Compatibility Mode Exceptions

#UD If executed outside VMX non-root operation.

64-Bit Mode Exceptions

#UD If executed outside VMX non-root operation.

VMCLEAR—Clear Virtual-Machine Control Structure

| Opcode | Instruction | Description |
|-------------|-------------|--|
| 66 0F C7 /6 | VMCLEAR m64 | Copy VMCS data to VMCS region in memory. |

Description

This instruction applies to the VMCS whose VMCS region resides at the physical address contained in the instruction operand. The instruction ensures that VMCS data for that VMCS (some of these data may be currently maintained on the processor) are copied to the VMCS region in memory. It also initializes parts of the VMCS region (for example, it sets the launch state of that VMCS to clear). See Chapter 20, “Virtual-Machine Control Structures,” in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*.

The operand of this instruction is always 64 bits and is always in memory. If the operand is the current-VMCS pointer, then that pointer is made invalid (set to FFFFFFFF_FFFFFFFFH).

Note that the VMCLEAR instruction might not explicitly write any VMCS data to memory; the data may be already resident in memory before the VMCLEAR is executed.

Operation

IF (register operand) or (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)

THEN #UD;

ELSIF in VMX non-root operation

THEN VM exit;

ELSIF CPL > 0

THEN #GP(0);

ELSE

addr ← contents of 64-bit in-memory operand;

IF addr is not 4KB-aligned OR

(processor supports Intel 64 architecture and

addr sets any bits beyond the physical-address width) OR

(processor does not support Intel 64 architecture, addr sets any bits in the range 63:32)

THEN VMfail(VMCLEAR with invalid physical address);

ELSIF addr = VMXON pointer

THEN VMfail(VMCLEAR with VMXON pointer);

ELSE

ensure that data for VMCS referenced by the operand is in memory;

initialize implementation-specific data in VMCS region;

launch state of VMCS referenced by the operand ← “clear”

```

IF operand addr = current-VMCS pointer
    THEN current-VMCS pointer ← FFFFFFFF_FFFFFFFFH;
FI;
VMsucceed;

FI;
FI;

```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|---|
| LOCK | Causes #UD. |
| REP* | Reserved and may cause unpredictable behavior (applies to both REPNE/REPZ and REP/REPE/REPZ). |
| Segment overrides | Treated normally |
| Operand size | Ignored |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | <p>If the current privilege level is not 0.</p> <p>If the memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register contains an unusable segment.</p> <p>If the operand is located in an execute-only code segment.</p> |
| #PF(fault-code) | If a page fault occurs in accessing the memory operand. |
| #SS(0) | <p>If the memory operand effective address is outside the SS segment limit.</p> <p>If the SS register contains an unusable segment.</p> |
| #UD | <p>If operand is a register.</p> <p>If not in VMX operation.</p> |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMCLEAR instruction is not recognized outside VMX operation. |
|-----|--|

Virtual-8086 Mode Exceptions

#UD The VMCLEAR instruction is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

#UD The VMCLEAR instruction is not recognized in compatibility mode.

64-Bit Mode Exceptions

#GP(0) If the current privilege level is not 0.
 If the source operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form.

#PF (fault-code) If a page fault occurs in accessing the memory operand.

#SS(0) If the source operand is in the SS segment and the memory address is in a non-canonical form.

#UD If operand is a register.
 If not in VMX operation.

VMLAUNCH/VMRESUME—Launch/Resume Virtual Machine

| Opcode | Instruction | Description |
|----------|-------------|---|
| OF 01 C2 | VMLAUNCH | Launch virtual machine managed by current VMCS. |
| OF 01 C3 | VMRESUME | Resume virtual machine managed by current VMCS. |

Description

Effects a VM entry managed by the current VMCS.

- VMLAUNCH fails if the launch state of current VMCS is not “clear”. If the instruction is successful, it sets the launch state to “launched.”
- VMRESUME fails if the launch state of the current VMCS is not “launched.”

If VM entry is attempted, the logical processor performs a series of consistency checks as detailed in Chapter 22, “VM Entries,” in the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*. Failure to pass checks on the VMX controls or on the host-state area passes control to the instruction following the VMLAUNCH or VMRESUME instruction. If these pass but checks on the guest-state area fail, the logical processor loads state from the host-state area of the VMCS, passing control to the instruction referenced by the RIP field in the host-state area.

VM entry is not allowed when events are blocked by MOV SS or POP SS. Neither VMLAUNCH nor VMRESUME should be used immediately after either MOV to SS or POP to SS.

Operation

```

IF (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELSIF in VMX non-root operation
    THEN VMexit;
ELSIF CPL > 0
    THEN #GP(0);
ELSIF current-VMCS pointer is not valid
    THEN VMfailInvalid;
ELSIF events are being blocked by MOV SS
    THEN VMfailValid(VM entry with events blocked by MOV SS);
ELSIF (VMLAUNCH and launch state of current VMCS is not “clear”)
    THEN VMfailValid(VMLAUNCH with non-clear VMCS);
ELSIF (VMRESUME and launch state of current VMCS is not “launched”)
    THEN VMfailValid(VMRESUME with non-launched VMCS);
ELSE
    Check settings of VMX controls and host-state area;
    IF invalid settings
  
```

```

THEN VmfailValid(VM entry with invalid VMX-control field(s)) or
    VmfailValid(VM entry with invalid host-state field(s)) or
    VmfailValid(VM entry with invalid executive-VMCS pointer)) or
    VmfailValid(VM entry with non-launched executive VMCS) or
    VmfailValid(VM entry with executive-VMCS pointer not VMXON pointer) or
    VmfailValid(VM entry with invalid VM-execution control fields in executive
    VMCS)
    as appropriate;
ELSE
    Attempt to load guest state and PDPTRs as appropriate;
    clear address-range monitoring;
    IF failure in checking guest state or PDPTRs
        THEN VM entry fails (see Section 22.7, in the
        Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B);
        ELSE
            Attempt to load MSRs from VM-entry MSR-load area;
            IF failure
                THEN VM entry fails (see Section 22.7, in the Intel® 64 and IA-32
                Architectures Software Developer's Manual, Volume 3B);
                ELSE
                    IF VMLAUNCH
                        THEN launch state of VMCS ← "launched";
                    FI;
                    IF in SMM and "entry to SMM" VM-entry control is 0
                        THEN
                            IF "deactivate dual-monitor treatment" VM-entry
                            control is 0
                                THEN SMM-transfer VMCS pointer ←
                                current-VMCS pointer;
                            FI;
                            IF executive-VMCS pointer is VMX pointer
                                THEN current-VMCS pointer ←
                                VMCS-link pointer;
                                ELSE current-VMCS pointer ←
                                executive-VMCS pointer;
                            FI;
                            leave SMM;
                        FI;
                    VM entry succeeds;
                FI;
            FI;
        FI;
    FI;
FI;

```

Further details of the operation of the VM-entry appear in Chapter 22 of *IA-32 Intel Architecture Software Developer's Manual, Volume 3B*.

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|---|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPZ and REP/REPE/REPZ) |
| Segment overrides | Ignored |
| Operand size | Causes #UD |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

| | |
|--------|--|
| #GP(0) | If the current privilege level is not 0. |
| #UD | If executed outside VMX operation. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMLAUNCH and VMRESUME instructions are not recognized outside VMX operation. |
|-----|--|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | The VMLAUNCH and VMRESUME instructions are not recognized in virtual-8086 mode. |
|-----|---|

Compatibility Mode Exceptions

| | |
|-----|--|
| #UD | The VMLAUNCH and VMRESUME instructions are not recognized in compatibility mode. |
|-----|--|

64-Bit Mode Exceptions

| | |
|--------|--|
| #GP(0) | If the current privilege level is not 0. |
| #UD | If executed outside VMX operation. |

VMPTRLD—Load Pointer to Virtual-Machine Control Structure

| Opcode | Instruction | Description |
|----------|-------------|---|
| OF C7 /6 | VMPTRLD m64 | Loads the current VMCS pointer from memory. |

Description

Marks the current-VMCS pointer valid and loads it with the physical address in the instruction operand. The instruction fails if its operand is not properly aligned, sets unsupported physical-address bits, or is equal to the VMXON pointer. In addition, the instruction fails if the 32 bits in memory referenced by the operand do not match the VMCS revision identifier supported by this processor.¹

The operand of this instruction is always 64 bits and is always in memory.

Operation

IF (register operand) or (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)

THEN #UD;

ELSIF in VMX non-root operation

THEN VMexit;

ELSIF CPL > 0

THEN #GP(0);

ELSE

addr ← contents of 64-bit in-memory source operand;

IF addr is not 4KB-aligned OR

(processor supports Intel 64 architecture and

addr sets any bits beyond the processor's physical-address width) OR

processor does not support Intel 64 architecture and addr sets any bits in the range 63:32

THEN VMfail(VMPTRLD with invalid physical address);

ELSIF addr = VMXON pointer

THEN VMfail(VMPTRLD with VMXON pointer);

ELSE

rev ← 32 bits located at physical address addr;

IF rev ≠ VMCS revision identifier supported by processor

THEN VMfail(VMPTRLD with incorrect VMCS revision identifier);

ELSE

current-VMCS pointer ← addr;

VMsucceed;

1. Software should consult the VMX capability MSR VMX_BASIC to discover the VMCS revision identifier supported by this processor (see Appendix G, "VMX Capability Reporting Facility," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B*).

FI;
FI;
FI;

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REPNE/REPZ | Causes #UD |
| REP/REPE/REPZ | Changes encoding to that of VMXON; see “VMXON—Enter VMX Operation” for operation and interactions with other prefixes. |
| Segment overrides | Treated normally |
| Operand size | Changes encoding to that of VMCLEAR; see “VMCLEAR—Clear Virtual-Machine Control Structure” for operation and interactions with other prefixes. |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | <p>If the current privilege level is not 0.</p> <p>If the memory source operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register contains an unusable segment.</p> <p>If the source operand is located in an execute-only code segment.</p> |
| #PF(fault-code) | If a page fault occurs in accessing the memory source operand. |
| #SS(0) | <p>If the memory source operand effective address is outside the SS segment limit.</p> <p>If the SS register contains an unusable segment.</p> |
| #UD | <p>If operand is a register.</p> <p>If not in VMX operation.</p> |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMPTRLD instruction is not recognized outside VMX operation. |
|-----|--|

Virtual-8086 Mode Exceptions

#UD The VMPTRLD instruction is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

#UD The VMPTRLD instruction is not recognized in compatibility mode.

64-Bit Mode Exceptions

#GP(0) If the current privilege level is not 0.
 If the source operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form.

#PF (fault-code) If a page fault occurs in accessing the memory source operand.

#SS(0) If the source operand is in the SS segment and the memory address is in a non-canonical form.

#UD If operand is a register.
 If not in VMX operation.

VMPTRST—Store Pointer to Virtual-Machine Control Structure

| Opcode | Instruction | Description |
|----------|-------------|--|
| 0F C7 /7 | VMPTRST m64 | Stores the current VMCS pointer into memory. |

Description

Stores the current-VMCS pointer into a specified memory address. The operand of this instruction is always 64 bits and is always in memory.

Operation

IF (register operand) or (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)

THEN #UD;

ELSIF in VMX non-root operation

THEN VMexit;

ELSIF CPL > 0

THEN #GP(0);

ELSE

64-bit in-memory destination operand ← current-VMCS pointer;
VMsucceed;

FI;

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPZ and REP/REPE/REPZ) |
| Segment overrides | Treated normally |
| Operand size | Causes #UD |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | If the current privilege level is not 0. If the memory destination operand effective address is outside the CS, DS, ES, FS, or GS segment limit. |
|--------|---|

| | |
|-----------------|--|
| | If the DS, ES, FS, or GS register contains an unusable segment. |
| | If the destination operand is located in a read-only data segment or any code segment. |
| #PF(fault-code) | If a page fault occurs in accessing the memory destination operand. |
| #SS(0) | If the memory destination operand effective address is outside the SS segment limit. |
| | If the SS register contains an unusable segment. |
| #UD | If operand is a register. |
| | If not in VMX operation. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMPTRST instruction is not recognized outside VMX operation. |
|-----|--|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | The VMPTRST instruction is not recognized in virtual-8086 mode. |
|-----|---|

Compatibility Mode Exceptions

| | |
|-----|--|
| #UD | The VMPTRST instruction is not recognized in compatibility mode. |
|-----|--|

64-Bit Mode Exceptions

| | |
|-----------------|--|
| #GP(0) | If the current privilege level is not 0. |
| | If the destination operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs in accessing the memory destination operand. |
| #SS(0) | If the destination operand is in the SS segment and the memory address is in a non-canonical form. |
| #UD | If operand is a register. |
| | If not in VMX operation. |

VMREAD—Read Field from Virtual-Machine Control Structure

| Opcode | Instruction | Description |
|--------|-------------------|---|
| OF 78 | VMREAD r/m64, r64 | Reads a specified VMCS field (in 64-bit mode). |
| OF 78 | VMREAD r/m32, r32 | Reads a specified VMCS field (outside 64-bit mode). |

Description

Reads a specified field from the VMCS and stores it into a specified destination operand (register or memory).

The specific VMCS field is identified by the VMCS-field encoding contained in the register source operand. Outside IA-32e mode, the source operand has 32 bits, regardless of the value of CS.D. In 64-bit mode, the source operand has 64 bits; however, if bits 63:32 of the source operand are not zero, VMREAD will fail due to an attempt to access an unsupported VMCS component (see operation section).

The effective size of the destination operand, which may be a register or in memory, is always 32 bits outside IA-32e mode (the setting of CS.D is ignored with respect to operand size) and 64 bits in 64-bit mode. If the VMCS field specified by the source operand is shorter than this effective operand size, the high bits of the destination operand are cleared to 0. If the VMCS field is longer, then the high bits of the field are not read.

Note that any faults resulting from accessing a memory destination operand can occur only after determining, in the operation section below, that the VMCS pointer is valid and that the specified VMCS field is supported.

Operation

```

IF (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELSIF in VMX non-root operation
    THEN VMexit;
ELSIF CPL > 0
    THEN #GP(0);
ELSIF current-VMCS pointer is not valid
    THEN VMfailInvalid;
    ELSIF register source operand does not correspond to any VMCS field
        THEN VMfailValid(VMREAD/VMWRITE from/to unsupported VMCS component);
    ELSE
        DEST ← contents of VMCS field indexed by register source operand;
        VMsucceed;
FI;
```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Segment overrides | Treated normally |
| Operand size | Causes #UD |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | <p>If the current privilege level is not 0.</p> <p>If a memory destination operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register contains an unusable segment.</p> <p>If the destination operand is located in a read-only data segment or any code segment.</p> |
| #PF(fault-code) | If a page fault occurs in accessing a memory destination operand. |
| #SS(0) | <p>If a memory destination operand effective address is outside the SS segment limit.</p> <p>If the SS register contains an unusable segment.</p> |
| #UD | If not in VMX operation. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMREAD instruction is not recognized outside VMX operation. |
|-----|---|

Virtual-8086 Mode Exceptions

| | |
|-----|--|
| #UD | The VMREAD instruction is not recognized in virtual-8086 mode. |
|-----|--|

Compatibility Mode Exceptions

| | |
|-----|---|
| #UD | The VMREAD instruction is not recognized in compatibility mode. |
|-----|---|

64-Bit Mode Exceptions

| | |
|--------|--|
| #GP(0) | If the current privilege level is not 0. |
|--------|--|

VMX INSTRUCTION REFERENCE

| | |
|------------------|---|
| | If the memory destination operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form. |
| #PF (fault-code) | If a page fault occurs in accessing a memory destination operand. |
| #SS(0) | If the memory destination operand is in the SS segment and the memory address is in a non-canonical form. |
| #UD | If not in VMX operation. |

VMRESUME—Resume Virtual Machine

See VMLAUNCH/VMRESUME—Launch/Resume Virtual Machine.

VMWRITE—Write Field to Virtual-Machine Control Structure

| Opcode | Instruction | Description |
|--------|--------------------|---|
| 0F 79 | VMWRITE r64, r/m64 | Writes a specified VMCS field (in 64-bit mode) |
| 0F 79 | VMWRITE r32, r/m32 | Writes a specified VMCS field (outside 64-bit mode) |

Description

Writes to a specified field in the VMCS specified by a secondary source operand (register only) using the contents of a primary source operand (register or memory).

The VMCS field is identified by the VMCS-field encoding contained in the register secondary source operand. Outside IA-32e mode, the secondary source operand is always 32 bits, regardless of the value of CS.D. In 64-bit mode, the secondary source operand has 64 bits; however, if bits 63:32 of the secondary source operand are not zero, VMWRITE will fail due to an attempt to access an unsupported VMCS component (see operation section).

The effective size of the primary source operand, which may be a register or in memory, is always 32 bits outside IA-32e mode (the setting of CS.D is ignored with respect to operand size) and 64 bits in 64-bit mode. If the VMCS field specified by the secondary source operand is shorter than this effective operand size, the high bits of the primary source operand are ignored. If the VMCS field is longer, then the high bits of the field are cleared to 0.

Note that any faults resulting from accessing a memory source operand occur after determining, in the operation section below, that the VMCS pointer is valid but before determining if the destination VMCS field is supported.

Operation

```

IF (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELIF in VMX non-root operation
    THEN VMexit;
ELIF CPL > 0
    THEN #GP(0);
ELIF current-VMCS pointer is not valid
    THEN VMfailInvalid;
ELIF register destination operand does not correspond to any VMCS field
    THEN VMfailValid(VMREAD/VMWRITE from/to unsupported VMCS component);
ELIF VMCS field indexed by register destination operand is read-only
    THEN VMfailValid(VMWRITE to read-only VMCS component);
ELSE
    VMCS field indexed by register destination operand ← SRC;
    VMsucceed;

```


FI;

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Segment overrides | Treated normally |
| Operand size | Causes #UD |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | <p>If the current privilege level is not 0.</p> <p>If a memory source operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register contains an unusable segment.</p> <p>If the source operand is located in an execute-only code segment.</p> |
| #PF(fault-code) | If a page fault occurs in accessing a memory source operand. |
| #SS(0) | <p>If a memory source operand effective address is outside the SS segment limit.</p> <p>If the SS register contains an unusable segment.</p> |
| #UD | If not in VMX operation. |

Real-Address Mode Exceptions

| | |
|-----|--|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMWRITE instruction is not recognized outside VMX operation. |
|-----|--|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | The VMWRITE instruction is not recognized in virtual-8086 mode. |
|-----|---|

Compatibility Mode Exceptions

| | |
|-----|--|
| #UD | The VMWRITE instruction is not recognized in compatibility mode. |
|-----|--|

64-Bit Mode Exceptions

| | |
|------------------|--|
| #GP(0) | If the current privilege level is not 0. If the memory source operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form. |
| #PF (fault-code) | If a page fault occurs in accessing a memory source operand. |
| #SS(0) | If the memory source operand is in the SS segment and the memory address is in a non-canonical form. |
| #UD | If not in VMX operation. |

VMXOFF—Leave VMX Operation

| Opcode | Instruction | Description |
|----------|-------------|-----------------------|
| 0F 01 C4 | VMXOFF | Leaves VMX operation. |

Description

Takes the logical processor out of VMX operation, unblocks INIT signals, conditionally re-enables A20M, and clears any address-range monitoring.¹

Operation

```

IF (not in VMX operation) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)
    THEN #UD;
ELSIF in VMX non-root operation
    THEN VMexit;
ELSIF CPL > 0
    THEN #GP(0);
ELSIF dual-monitor treatment of SMIs and SMM is active
    THEN VMfail(VMXOFF under dual-monitor treatment of SMIs and SMM);
ELSE
    leave VMX operation;
    unblock INIT;
    IF outside SMX operation2
        THEN unblock and enable A20M;
    clear address-range monitoring;
    VMSucceed;
FI;
FI;
```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |

1. See the information on MONITOR/MWAIT in Chapter 7, “Multiple-Processor Management,” of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A*.
2. A logical processor is outside SMX operation if GETSEC[SENDER] has not been executed or if GETSEC[SEXIT] was executed after the last execution of GETSEC[SENDER]. See Chapter 6, “Safer Mode Extensions Reference.”

| | |
|-------------------|------------|
| Segment overrides | Ignored |
| Operand size | Causes #UD |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | If executed in VMX root operation with CPL > 0. |
| #UD | If executed outside VMX operation. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | A logical processor cannot be in real-address mode while in VMX operation and the VMXOFF instruction is not recognized outside VMX operation. |
|-----|---|

Virtual-8086 Mode Exceptions

| | |
|-----|--|
| #UD | The VMXOFF instruction is not recognized in virtual-8086 mode. |
|-----|--|

Compatibility Mode Exceptions

| | |
|-----|---|
| #UD | The VMXOFF instruction is not recognized in compatibility mode. |
|-----|---|

64-Bit Mode Exceptions

| | |
|--------|---|
| #GP(0) | If executed in VMX root operation with CPL > 0. |
| #UD | If executed outside VMX operation. |

VMXON—Enter VMX Operation

| Opcode | Instruction | Description |
|-------------|-------------|---------------------------|
| F3 0F C7 /6 | VMXON m64 | Enter VMX root operation. |

Description

Puts the logical processor in VMX operation with no current VMCS, blocks INIT signals, disables A20M, and clears any address-range monitoring established by the MONITOR instruction.¹

The operand of this instruction is a 4KB-aligned physical address (the VMXON pointer) that references the VMXON region, which the logical processor may use to support VMX operation. This operand is always 64 bits and is always in memory.

Operation

IF (register operand) or (CR4.VMXE = 0) or (CR0.PE = 0) or (RFLAGS.VM = 1) or (IA32_EFER.LMA = 1 and CS.L = 0)

THEN #UD;

ELSIF not in VMX operation

THEN

IF (CPL > 0) or (in A20M mode) or

(the values of CR0 and CR4 are not supported in VMX operation²) or

(bit 0 (lock bit) of IA32_FEATURE_CONTROL MSR is clear) or

(in SMX operation³ and bit 1 of IA32_FEATURE_CONTROL MSR is clear) or

(outside SMX operation and bit 2 of IA32_FEATURE_CONTROL MSR is clear)

THEN #GP(0);

ELSE

addr ← contents of 64-bit in-memory source operand;

IF addr is not 4KB-aligned or

(processor supports Intel 64 architecture and

addr sets any bits beyond the VMX physical-address width) or

(processor does not support Intel 64 architecture and

addr sets any bits in the range 63:32)

1. See the information on MONITOR/MWAIT in Chapter 7, “Multiple-Processor Management,” of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3A*.
2. See Section 19.8 of the *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*.
3. A logical processor is in SMX operation if GETSEC[SEXIT] has not been executed since the last execution of GETSEC[SENDER]. A logical processor is outside SMX operation if GETSEC[SENDER] has not been executed or if GETSEC[SEXIT] was executed after the last execution of GETSEC[SENDER]. See Chapter 6, “Safer Mode Extensions Reference.”

```

    THEN VMfailInvalid;
    ELSE
        rev ← 32 bits located at physical address addr;
        IF rev ≠ VMCS revision identifier supported by processor
            THEN VMfailInvalid;
            ELSE
                current-VMCS pointer ← FFFFFFFF_FFFFFFFFH;
                enter VMX operation;
                block INIT signals;
                block and disable A20M;
                clear address-range monitoring;
                VMSucceed;
        FI;
    FI;
    FI;
    ELSIF in VMX non-root operation
        THEN VMexit;
    ELSIF CPL > 0
        THEN #GP(0);
        ELSE VMfail("VMXON executed in VMX root operation");
    FI;

```

Flags Affected

See the operation section and Section 5.2.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Ignored (includes REPNE/REPZ and REP/REPE/REPZ) |
| Segment overrides | Treated normally |
| Operand size | Ignored |
| Address size | Treated normally |
| REX | Register extensions treated normally; operand-size overrides ignored |

Protected Mode Exceptions

| | |
|--------|---|
| #GP(0) | <p>If executed outside VMX operation with CPL>0 or with invalid CRO or CR4 fixed bits.</p> <p>If executed in A20M mode.</p> <p>If the memory source operand effective address is outside the CS, DS, ES, FS, or GS segment limit.</p> <p>If the DS, ES, FS, or GS register contains an unusable segment.</p> |
|--------|---|

| | |
|-----------------|---|
| | If the source operand is located in an execute-only code segment. |
| #PF(fault-code) | If a page fault occurs in accessing the memory source operand. |
| #SS(0) | If the memory source operand effective address is outside the SS segment limit. |
| | If the SS register contains an unusable segment. |
| #UD | If operand is a register. |
| | If executed with CR4.VMXE = 0. |

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | The VMXON instruction is not recognized in real-address mode. |
|-----|---|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | The VMXON instruction is not recognized in virtual-8086 mode. |
|-----|---|

Compatibility Mode Exceptions

| | |
|-----|--|
| #UD | The VMXON instruction is not recognized in compatibility mode. |
|-----|--|

64-Bit Mode Exceptions

| | |
|-----------------|---|
| #GP(0) | If executed outside VMX operation with CPL > 0 or with invalid CRO or CR4 fixed bits. |
| | If executed in A20M mode. |
| | If the source operand is in the CS, DS, ES, FS, or GS segments and the memory address is in a non-canonical form. |
| #PF(fault-code) | If a page fault occurs in accessing the memory source operand. |
| #SS(0) | If the source operand is in the SS segment and the memory address is in a non-canonical form. |
| #UD | If operand is a register. |
| | If executed with CR4.VMXE = 0. |

5.4 VM INSTRUCTION ERROR NUMBERS

For certain error conditions, the VM-instruction error field is loaded with an error number to indicate the source of the error.

5.4.1 Error Numbers

Table 5-1 lists VM-instruction error numbers.

Table 5-1. VM-Instruction Error Numbers

| Error Number | Description |
|--------------|--|
| 1 | VMCALL executed in VMX root operation |
| 2 | VMCLEAR with invalid physical address |
| 3 | VMCLEAR with VMXON pointer |
| 4 | VMLAUNCH with non-clear VMCS |
| 5 | VMRESUME with non-launched VMCS |
| 6 | VMRESUME with a corrupted VMCS (indicates corruption of the current VMCS) |
| 7 | VM entry with invalid control field(s) ^{1,2} |
| 8 | VM entry with invalid host-state field(s) ¹ |
| 9 | VMPTRLD with invalid physical address |
| 10 | VMPTRLD with VMXON pointer |
| 11 | VMPTRLD with incorrect VMCS revision identifier |
| 12 | VMREAD/VMWRITE from/to unsupported VMCS component |
| 13 | VMWRITE to read-only VMCS component |
| 15 | VMXON executed in VMX root operation |
| 16 | VM entry with invalid executive-VMCS pointer ¹ |
| 17 | VM entry with non-launched executive VMCS ¹ |
| 18 | VM entry with executive-VMCS pointer not VMXON pointer (when attempting to deactivate the dual-monitor treatment of SMIs and SMM) ¹ |
| 19 | VMCALL with non-clear VMCS (when attempting to activate the dual-monitor treatment of SMIs and SMM) |
| 20 | VMCALL with invalid VM-exit control fields |
| 22 | VMCALL with incorrect MSEG revision identifier (when attempting to activate the dual-monitor treatment of SMIs and SMM) |
| 23 | VMXOFF under dual-monitor treatment of SMIs and SMM |
| 24 | VMCALL with invalid SMM-monitor features (when attempting to activate the dual-monitor treatment of SMIs and SMM) |

Table 5-1. VM-Instruction Error Numbers (Contd.)

| Error Number | Description |
|--------------|---|
| 25 | VM entry with invalid VM-execution control fields in executive VMCS (when attempting to return from SMM) ^{1,2} |
| 26 | VM entry with events blocked by MOV SS. |
| 28 | Invalid operand to INVEPT/INVVPID. |

NOTES:

1. VM-entry checks on control fields and host-state fields may be performed in any order. Thus, an indication by error number of one cause does not imply that there are not also other errors. Different processors may give different error numbers for the same VMCS.
2. Error number 7 is not used for VM entries that return from SMM that fail due to invalid VM-execution control fields in the executive VMCS. Error number 25 is used for these cases.

CHAPTER 6

SAFER MODE EXTENSIONS REFERENCE

6.1 OVERVIEW

This chapter describes the Safer Mode Extensions (SMX) for the Intel 64 and IA-32 architectures. Safer Mode Extensions (SMX) provide a programming interface for system software to establish a measured environment within the platform to support trust decisions by end users. The measured environment includes:

- Measured launch of a system executive, referred to as a Measured Launched Environment (MLE)¹. The system executive may be based on a Virtual Machine Monitor (VMM), a measured VMM is referred to as MVMM².
- Mechanisms to ensure the above measurement is protected and stored in a secure location in the platform.
- Protection mechanisms that allow the VMM to control attempts to modify the VMM

The measurement and protection mechanisms used by a measured environment are supported by the capabilities of an Intel® Trusted Execution Technology (Intel® TXT) platform:

- The SMX are the processor's programming interface in an Intel TXT platform;
- The chipset in an Intel TXT platform provides enforcement of the protection mechanisms;
- Trusted Platform Module (TPM) 1.2 in the platform provides platform configuration registers (PCRs) to store software measurement values.

6.2 SMX FUNCTIONALITY

SMX functionality is provided in an Intel 64 processor through the GETSEC instruction via leaf functions. The GETSEC instruction supports multiple leaf functions. Leaf functions are selected by the value in EAX at the time GETSEC is executed. Each GETSEC leaf function is documented separately in the reference pages with a unique mnemonic (even though these mnemonics share the same opcode, 0F 37).

-
1. See *Intel® Trusted Execution Technology Measured Launched Environment Programming Guide*.
 2. An MVMM is sometimes referred to as a measured launched environment (MLE). See *Intel® Trusted Execution Technology Measured Launched Environment Programming Guide*

6.2.1 Detecting and Enabling SMX

Software can detect support for SMX operation using the CPUID instruction. If software executes CPUID with 1 in EAX, a value of 1 in bit 6 of ECX indicates support for SMX operation (GETSEC is available), see CPUID instruction for the layout of feature flags of reported by CPUID.01H:ECX.

System software enables SMX operation by setting CR4.SMXE[Bit 14] = 1 before attempting to execute GETSEC. Otherwise, execution of GETSEC results in the processor signaling an invalid opcode exception (#UD).

If the CPUID SMX feature flag is clear (CPUID.01H.ECX[Bit 6] = 0), attempting to set CR4.SMXE[Bit 14] results in a general protection exception.

The IA32_FEATURE_CONTROL MSR (at address 03AH) provides feature control bits that configure operation of VMX and SMX. These bits are documented in Table 6-1.

Table 6-1. Layout of IA32_FEATURE_CONTROL

| Bit Position | Description |
|--------------|--|
| 0 | Lock bit (0 = unlocked, 1 = locked). When set to '1' further writes to this MSR are blocked. |
| 1 | Enable VMX in SMX operation |
| 2 | Enable VMX outside SMX operation |
| 7:3 | Reserved |
| 14:8 | SENTER Local Function Enables: When set, each bit in the field represents an enable control for a corresponding SENTER function. |
| 15 | SENTER Global Enable: Must be set to '1' to enable operation of GETSEC[SENTER] |
| 63:16 | Reserved |

- Bit 0 is a lock bit. If the lock bit is clear, an attempt to execute VMXON will cause a general-protection exception. Attempting to execute GETSEC[SENTER] when the lock bit is clear will also cause a general-protection exception. If the lock bit is set, WRMSR to the IA32_FEATURE_CONTROL MSR will cause a general-protection exception. Once the lock bit is set, the MSR cannot be modified until a power-on reset. System BIOS can use this bit to provide a setup option for BIOS to disable support for VMX, SMX or both VMX and SMX.
- Bit 1 enables VMX in SMX operation (between executing the SENTER and SEXIT leaves of GETSEC). If this bit is clear, an attempt to execute VMXON in SMX will cause a general-protection exception if executed in SMX operation. Attempts to set this bit on logical processors that do not support both VMX operation (Chapter 6, "Safer Mode Extensions Reference") and SMX operation cause general-protection exceptions.

- Bit 2 enables VMX outside SMX operation. If this bit is clear, an attempt to execute VMXON will cause a general-protection exception if executed outside SMX operation. Attempts to set this bit on logical processors that do not support VMX operation cause general-protection exceptions.
- Bits 8 through 14 specify enabled functionality of the SENTER leaf function. Each bit in the field represents an enable control for a corresponding SENTER function. Only enabled SENTER leaf functionality can be used when executing SENTER.
- Bits 15 specify global enable of all SENTER functionalities.

6.2.2 SMX Instruction Summary

System software must first query for available GETSEC leaf functions by executing GETSEC[CAPABILITIES]. The CAPABILITIES leaf function returns a bit map of available GETSEC leaves. An attempt to execute an unsupported leaf index results in an undefined opcode (#UD) exception.

6.2.2.1 GETSEC[CAPABILITIES]

The SMX functionality provides an architectural interface for newer processor generations to extend SMX capabilities. Specifically, the GETSEC instruction provides a capability leaf function for system software to discover the available GETSEC leaf functions that are supported in a processor. Table 6-2 lists the currently available GETSEC leaf functions.

Table 6-2. GETSEC Leaf Functions

| Index (EAX) | Leaf function | Description |
|-------------|---------------|--|
| 0 | CAPABILITIES | Returns the available leaf functions of the GETSEC instruction |
| 1 | Undefined | Reserved |
| 2 | ENTERACCS | Enter |
| 3 | EXITAC | Exit |
| 4 | SENER | Launch an MLE |
| 5 | SEXIT | Exit the MLE |
| 6 | PARAMETERS | Return SMX related parameter information |
| 7 | SMCTRL | SMX mode control |
| 8 | WAKEUP | Wake up sleeping processors in safer mode |
| 9 - (4G-1) | Undefined | Reserved |

6.2.2.2 GETSEC[ENTERACCS]

The GETSEC[ENTERACCS] leaf enables authenticated code execution mode. The ENTERACCS leaf function performs an authenticated code module load using the chipset public key as the signature verification. ENTERACCS requires the existence of an Intel® Trusted Execution Technology capable chipset since it unlocks the chipset private configuration register space after successful authentication of the loaded module. The physical base address and size of the authenticated code module are specified as input register values in EBX and ECX, respectively.

While in the authenticated code execution mode, certain processor state properties change. For this reason, the time in which the processor operates in authenticated code execution mode should be limited to minimize impact on external system events.

Upon entry into , the previous paging context is disabled (since the authenticated code module image is specified with physical addresses and can no longer rely upon external memory-based page-table structures).

Prior to executing the GETSEC[ENTERACCS] leaf, system software must ensure the logical processor issuing GETSEC[ENTERACCS] is the boot-strap processor (BSP), as indicated by IA32_APIC_BASE.BSP = 1. System software must ensure other logical processors are in a suitable idle state and not marked as BSP.

The GETSEC[ENTERACCS] leaf may be used by different agents to load different authenticated code modules to perform functions related to different aspects of a measured environment, for example system software and Intel® TXT enabled BIOS may use more than one authenticated code modules.

6.2.2.3 GETSEC[EXITAC]

GETSEC[EXITAC] takes the processor out of . When this instruction leaf is executed, the contents of the authenticated code execution area are scrubbed and control is transferred to the non-authenticated context defined by a near pointer passed with the GETSEC[EXITAC] instruction.

The authenticated code execution area is no longer accessible after completion of GETSEC[EXITAC]. RBX (or EBX) holds the address of the near absolute indirect target to be taken.

6.2.2.4 GETSEC[SENDER]

The GETSEC[SENDER] leaf function is used by the initiating logical processor (ILP) to launch an MLE. GETSEC[SENDER] can be considered a superset of the ENTERACCS leaf, because it enters as part of the measured environment launch.

Measured environment startup consists of the following steps:

- the ILP rendezvous the responding logical processors (RLPs) in the platform into a controlled state (At the completion of this handshake, all the RLPs except for

the ILP initiating the measured environment launch are placed in a newly defined SENTER sleep state).

- Load and authenticate the authenticated code module required by the measured environment, and enter authenticated code execution mode.
- Verify and lock certain system configuration parameters.
- Measure the dynamic root of trust and store into the PCRs in TPM.
- Transfer control to the MLE with interrupts disabled.

Prior to executing the GETSEC[SENDER] leaf, system software must ensure the platform's TPM is ready for access and the ILP is the boot-strap processor (BSP), as indicated by IA32_APIC_BASE.BSP. System software must ensure other logical processors (RLPs) are in a suitable idle state and not marked as BSP.

System software launching a measurement environment is responsible for providing a proper authenticate code module address when executing GETSEC[SENDER]. The AC module responsible for the launch of a measured environment and loaded by GETSEC[SENDER] is referred to as SINIT. See *Intel® Trusted Execution Technology Measured Launched Environment Programming Guide* for additional information on system software requirements prior to executing GETSEC[SENDER].

6.2.2.5 GETSEC[SEXIT]

System software exits the measured environment by executing the instruction GETSEC[SEXIT] on the ILP. This instruction rendezvous the responding logical processors in the platform for exiting from the measured environment. External events (if left masked) are unmasked and Intel® TXT-capable chipset's private configuration space is re-locked.

6.2.2.6 GETSEC[PARAMETERS]

The GETSEC[PARAMETERS] leaf function is used to report attributes, options and limitations of SMX operation. Software uses this leaf to identify operating limits or additional options.

The information reported by GETSEC[PARAMETERS] may require executing the leaf multiple times using EBX as an index. If the GETSEC[PARAMETERS] instruction leaf or if a specific parameter field is not available, then SMX operation should be interpreted to use the default limits of respective GETSEC leaves or parameter fields defined in the GETSEC[PARAMETERS] leaf.

6.2.2.7 GETSEC[SMCTRL]

The GETSEC[SMCTRL] leaf function is used for providing additional control over specific conditions associated with the SMX architecture. An input register is supported for selecting the control operation to be performed. See the specific leaf description for details on the type of control provided.

6.2.2.8 GETSEC[WAKEUP]

Responding logical processors (RLPs) are placed in the SENTER sleep state after the initiating logical processor executes GETSEC[SENDER]. The ILP can wake up RLPs to join the measured environment by using GETSEC[WAKEUP]. When the RLPs in SENTER sleep state wake up, these logical processors begin execution at the entry point defined in a data structure held in system memory (pointed to by a chipset register LT.MLE.JOIN) in TXT configuration space.

6.2.3 Measured Environment and SMX

This section gives a simplified view of a representative life cycle of a measured environment that is launched by a system executive using SMX leaf functions. *Intel® Trusted Execution Technology Measured Launched Environment Programming Guide* provides more detailed examples of using SMX and chipset resources (including chipset registers, Trusted Platform Module) to launch an MVMM.

The life cycle starts with the system executive (an OS, an OS loader, and so forth) loading the MLE and SINIT AC module into available system memory. The system executive must validate and prepare the platform for the measured launch. When the platform is properly configured, the system executive executes GETSEC[SENDER] on the initiating logical processor (ILP) to rendezvous the responding logical processors into an SENTER sleep state, the ILP then enters into using the SINIT AC module. In a multi-threaded or multi-processing environment, the system executive must ensure that other logical processors are already in an idle loop, or asleep (such as after executing HLT) before executing GETSEC[SENDER].

After the GETSEC[SENDER] rendezvous handshake is performed between all logical processors in the platform, the ILP loads the chipset authenticated code module (SINIT) and performs an authentication check. If the check passes, the processor hashes the SINIT AC module and stores the result into TPM PCR 17. It then switches execution context to the SINIT AC module. The SINIT AC module will perform a number of platform operations, including: verifying the system configuration, protecting the system memory used by the MLE from I/O devices capable of DMA, producing a hash of the MLE, storing the hash value in TPM PCR 18, and various other operations. When SINIT completes execution, it executes the GETSEC[EXITAC] instruction and transfers control the MLE at the designated entry point.

Upon receiving control from the SINIT AC module, the MLE must establish its protection and isolation controls before enabling DMA and interrupts and transferring control to other software modules. It must also wakeup the RLPs from their SENTER sleep state using the GETSEC[WAKEUP] instruction and bring them into its protection and isolation environment.

While executing in a measured environment, the MVMM can access the Trusted Platform Module (TPM) in locality 2. The MVMM has complete access to all TPM commands and may use the TPM to report current measurement values or use the measurement values to protect information such that only when the platform config-

uration registers (PCRs) contain the same value is the information released from the TPM. This protection mechanism is known as sealing.

A measured environment shutdown is ultimately completed by executing GETSEC[SEXIT]. Prior to this step system software is responsible for scrubbing sensitive information left in the processor caches, system memory.

6.3 GETSEC LEAF FUNCTIONS

This section provides detailed descriptions of each leaf function of the GETSEC instruction. GETSEC is available only if CPUID.01H:ECX[Bit 6] = 1. This indicates the availability of SMX and the GETSEC instruction. Before GETSEC can be executed, SMX must be enabled by setting CR4.SMXE[Bit 14] = 1.

A GETSEC leaf can only be used if it is shown to be available as reported by the GETSEC[CAPABILITIES] function. Attempts to access a GETSEC leaf index not supported by the processor, or if CR4.SMXE is 0, results in the signaling of an undefined opcode exception.

All GETSEC leaf functions are available in protected mode, including the compatibility sub-mode of IA-32e mode and the 64-bit sub-mode of IA-32e mode. Unless otherwise noted, the behavior of all GETSEC functions and interactions related to the measured environment are independent of IA-32e mode. This also applies to the interpretation of register widths¹ passed as input parameters to GETSEC functions and to register results returned as output parameters.

The GETSEC functions ENTERACCS, SENTER, SEXIT, and WAKEUP require a Intel® TXT capable-chipset to be present in the platform. The GETSEC[CAPABILITIES] returned bit vector in position 0 indicates an Intel® TXT-capable chipset has been sampled present² by the processor.

The processor's operating mode also affects the execution of the following GETSEC leaf functions: SMCTRL, ENTERACCS, EXITAC, SENTER, SEXIT, and WAKEUP. These functions are only allowed in protected mode at CPL = 0. They are not allowed while in SMM in order to prevent potential intra-mode conflicts. Further execution qualifications exist to prevent potential architectural conflicts (for example: nesting of the measured environment or authenticated code execution mode). See the definitions of the GETSEC leaf functions for specific requirements.

-
1. This chapter uses the 64-bit notation RAX, RIP, RSP, RFLAGS, etc. for processor registers because processors that support SMX also support Intel 64 Architecture. The MVMM can be launched in IA-32e mode or outside IA-32e mode. The 64-bit notation of processor registers also refer to its 32-bit forms if SMX is used in 32-bit environment. In some places, notation such as EAX is used to refer specifically to lower 32 bits of the indicated register
 2. Sampled present means that the processor sent a message to the chipset and the chipset responded that it (a) knows about the message and (b) is capable of executing SENTER. This means that the chipset CAN support Intel® TXT, and is configured and WILLING to support it.

SAFER MODE EXTENSIONS REFERENCE

For the purpose of performance monitor counting, the execution of GETSEC functions is counted as a single instruction with respect to retired instructions. The response by a responding logical processor (RLP) to messages associated with GETSEC[SENDER] or GTSEC[SEXIT] is transparent to the retired instruction count on the ILP.

GETSEC[CAPABILITIES] - Report the SMX Capabilities

| Opcode | Instruction | Description |
|--------------------|----------------------|---|
| OF 37 (EAX = 0) | GETSEC[CAPABILITIES] | Report the SMX capabilities. The capabilities index is input in EBX with the result returned in EAX. |

Description

The GETSEC[CAPABILITIES] function returns a bit vector of supported GETSEC leaf functions. The CAPABILITIES leaf of GETSEC is selected with EAX set to 0 at entry. EBX is used as the selector for returning the bit vector field in EAX. GETSEC[CAPABILITIES] may be executed at all privilege levels, but the CR4.SMXE bit must be set or an undefined opcode exception (#UD) is returned.

With EBX = 0 upon execution of GETSEC[CAPABILITIES], EAX returns the a bit vector representing status on the presence of a Intel® TXT-capable chipset and the first 30 available GETSEC leaf functions. The format of the returned bit vector is provided in Table 6-3.

If bit 0 is set to 1, then an Intel® TXT-capable chipset has been sampled present by the processor. If bits in the range of 1-30 are set, then the corresponding GETSEC leaf function is available. If the bit value at a given bit index is 0, then the GETSEC leaf function corresponding to that index is unsupported and attempted execution results in a #UD.

Bit 31 of EAX indicates if further leaf indexes are supported. If the Extended Leafs bit 31 is set, then additional leaf functions are accessed by repeating GETSEC[CAPABILITIES] with EBX incremented by one. When the most significant bit of EAX is not set, then additional GETSEC leaf functions are not supported; indexing EBX to a higher value results in EAX returning zero.

Table 6-3. Getsec Capability Result Encoding (EBX = 0)

| Field | Bit position | Description |
|-----------------|--------------|---------------------------------------|
| Chipset Present | 0 | Intel® TXT-capable chipset is present |
| Undefined | 1 | Reserved |
| ENTERACCS | 2 | GETSEC[ENTERACCS] is available |
| EXITAC | 3 | GETSEC[EXITAC] is available |
| SENER | 4 | GETSEC[SENER] is available |
| SEXIT | 5 | GETSEC[SEXIT] is available |

Table 6-3. Getsec Capability Result Encoding (EBX = 0) (Contd.)

| Field | Bit position | Description |
|----------------|--------------|--|
| PARAMETERS | 6 | GETSEC[PARAMETERS] is available |
| SMCTRL | 7 | GETSEC[SMCTRL] is available |
| WAKEUP | 8 | GETSEC[WAKEUP] is available |
| Undefined | 30:9 | Reserved |
| Extended Leafs | 31 | Reserved for extended information reporting of GETSEC capabilities |

Operation

```

IF (CR4.SMXE=0)
    THEN #UD;
ELSIF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
IF (EBX=0) THEN
    BitVector← 0;
    IF (TXT chipset present)
        BitVector[Chipset present]← 1;
    IF (ENTERACCS Available)
        THEN BitVector[ENTERACCS]← 1;
    IF (EXITAC Available)
        THEN BitVector[EXITAC]← 1;
    IF (SENER Available)
        THEN BitVector[SENER]← 1;
    IF (SEXIT Available)
        THEN BitVector[SEXIT]← 1;
    IF (PARAMETERS Available)
        THEN BitVector[PARAMETERS]← 1;
    IF (SMCTRL Available)
        THEN BitVector[SMCTRL]← 1;
    IF (WAKEUP Available)
        THEN BitVector[WAKEUP]← 1;
    EAX← BitVector;
ELSE
    EAX← 0;
END;;

```

Flags Affected

None

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

#UD IF CR4.SMXE = 0.

Real-Address Mode Exceptions

#UD IF CR4.SMXE = 0.

Virtual-8086 Mode Exceptions

#UD IF CR4.SMXE = 0.

Compatibility Mode Exceptions

#UD IF CR4.SMXE = 0.

64-Bit Mode Exceptions

#UD IF CR4.SMXE = 0.

VM-exit Condition

Reason (GETSEC) IF in VMX non-root operation.

GETSEC[ENTERACCS] - Execute Authenticated Chipset Code

| Opcode | Instruction | Description |
|--------------------|-------------------|--|
| OF 37 (EAX = 2) | GETSEC[ENTERACCS] | Enter authenticated code execution mode. EBX holds the authenticated code module physical base address. ECX holds the authenticated code module size (bytes). |

Description

The GETSEC[ENTERACCS] function loads, authenticates and executes an authenticated code module using an Intel® TXT platform chipset's public key. The ENTERACCS leaf of GETSEC is selected with EAX set to 2 at entry.

There are certain restrictions enforced by the processor for the execution of the GETSEC[ENTERACCS] instruction:

- Execution is not allowed unless the processor is in protected mode or IA-32e mode with CPL = 0 and EFLAGS.VM = 0.
- Processor cache must be available and not disabled, that is, CR0.CD and CR0.NW bits must be 0.
- For processor packages containing more than one logical processor, CR0.CD is checked to ensure consistency between enabled logical processors.
- For enforcing consistency of operation with numeric exception reporting using Interrupt 16, CR0.NE must be set.
- An Intel TXT-capable chipset must be present as communicated to the processor by sampling of the power-on configuration capability field after reset.
- The processor can not already be in authenticated code execution mode as launched by a previous GETSEC[ENTERACCS] or GETSEC[SENDER] instruction without a subsequent exiting using GETSEC[EXITAC]).
- To avoid potential operability conflicts between modes, the processor is not allowed to execute this instruction if it currently is in SMM or VMX operation.
- To insure consistent handling of SIPI messages, the processor executing the GETSEC[ENTERACCS] instruction must also be designated the BSP (boot-strap processor) as defined by A32_APIC_BASE.BSP (Bit 8).

Failure to conform to the above conditions results in the processor signaling a general protection exception.

Prior to execution of the ENTERACCS leaf, other logical processors, i.e. RLPs, in the platform must be:

- idle in a wait-for-SIPI state (as initiated by an INIT assertion or through reset for non-BSP designated processors), or
- in the SENTER sleep state as initiated by a GETSEC[SENDER] from the initiating logical processor (ILP).

If other logical processor(s) in the same package are not idle in one of these states, execution of ENTERACCS signals a general protection exception. The same requirement and action applies if the other logical processor(s) of the same package do not have `CRO.CD = 0`.

A successful execution of ENTERACCS results in the ILP entering an authenticated code execution mode. Prior to reaching this point, the processor performs several checks. These include:

- Establish and check the location and size of the specified authenticated code module to be executed by the processor.
- Inhibit the ILP's response to the external events: INIT, A20M, NMI and SMI.
- Broadcast a message to enable protection of memory and I/O from other processor agents.
- Load the designated code module into an authenticated code execution area.
- Isolate the contents of the authenticated code execution area from further state modification by external agents.
- Authenticate the authenticated code module.
- Initialize the initiating logical processor state based on information contained in the authenticated code module header.
- Unlock the Intel® TXT-capable chipset private configuration space and TPM locality 3 space.
- Begin execution in the authenticated code module at the defined entry point.

The `GETSEC[ENTERACCS]` function requires two additional input parameters in the general purpose registers EBX and ECX. EBX holds the authenticated code (AC) module physical base address (the AC module must reside below 4 GBytes in physical address space) and ECX holds the AC module size (in bytes). The physical base address and size are used to retrieve the code module from system memory and load it into the internal authenticated code execution area. The base physical address is checked to verify it is on a modulo-4096 byte boundary. The size is verified to be a multiple of 64, that it does not exceed the internal authenticated code execution area capacity (as reported by `GETSEC[CAPABILITIES]`), and that the top address of the AC module does not exceed 32 bits. An error condition results in an abort of the authenticated code execution launch and the signaling of a general protection exception.

As an integrity check for proper processor hardware operation, execution of `GETSEC[ENTERACCS]` will also check the contents of all the machine check status registers (as reported by the MSRs `IA32_MCi_STATUS`) for any valid uncorrectable error condition. In addition, the global machine check status register `IA32_MCG_STATUS` MCIP bit must be cleared and the IERR processor package pin (or its equivalent) must not be asserted, indicating that no machine check exception processing is currently in progress. These checks are performed prior to initiating the load of the authenticated code module. Any outstanding valid uncorrectable machine check error condition present in these status registers at this point will result in the processor signaling a general protection violation.

The ILP masks the response to the assertion of the external signals INIT#, A20M, NMI#, and SMI#. This masking remains active until optionally unmasked by GETSEC[EXITAC] (this defined unmasking behavior assumes GETSEC[ENTERACCS] was not executed by a prior GETSEC[ENTER]). The purpose of this masking control is to prevent exposure to existing external event handlers that may not be under the control of the authenticated code module..

The ILP sets an internal flag to indicate it has entered authenticated code execution mode. The state of the A20M pin is likewise masked and forced internally to a de-asserted state so that any external assertion is not recognized during authenticated code execution mode.

To prevent other (logical) processors from interfering with the ILP operating in authenticated code execution mode, memory (excluding implicit write-back transactions) access and I/O originating from other processor agents are blocked. This protection starts when the ILP enters into authenticated code execution mode. Only memory and I/O transactions initiated from the ILP are allowed to proceed. Exiting authenticated code execution mode is done by executing GETSEC[EXITAC]. The protection of memory and I/O activities remains in effect until the ILP executes GETSEC[EXITAC].

Prior to launching the authenticated execution module using GETSEC[ENTERACCS] or GETSEC[ENTER], the processor's MTRRs (Memory Type Range Registers) must first be initialized to map out the authenticated RAM addresses as WB (writeback). Failure to do so may affect the ability for the processor to maintain isolation of the loaded authenticated code module. If the processor detected this requirement is not met, it will signal an Intel® TXT reset condition with an error code during the loading of the authenticated code module.

While physical addresses within the load module must be mapped as WB, the memory type for locations outside of the module boundaries must be mapped to one of the supported memory types as returned by GETSEC[PARAMETERS] (or UC as default).

To conform to the minimum granularity of MTRR MSR for specifying the memory type, authenticated code RAM (ACRAM) is allocated to the processor in 4096 byte granular blocks. If an AC module size as specified in ECX is not a multiple of 4096 then the processor will allocate up to the next 4096 byte boundary for mapping as ACRAM with indeterminate data. This pad area will not be visible to the authenticated code module as external memory nor can it depend on the value of the data used to fill the pad area.

At the successful completion of GETSEC[ENTERACCS], the architectural state of the processor is partially initialized from contents held in the header of the authenticated code module. The processor GDTR, CS, and DS selectors are initialized from fields within the authenticated code module. Since the authenticated code module must be relocatable, all address references must be relative to the authenticated code module base address in EBX. The processor GDTR base value is initialized to the AC module header field GDTBasePtr + module base address held in EBX and the GDTR limit is set to the value in the GDTLimit field. The CS selector is initialized to the AC module header SegSel field, while the DS selector is initialized to CS + 8. The segment

descriptor fields are implicitly initialized to BASE=0, LIMIT=FFFFFFh, G=1, D=1, P=1, S=1, read/write access for DS, and execute/read access for CS. The processor begins the authenticated code module execution with the EIP set to the AC module header EntryPoint field + module base address (EBX). The AC module based fields used for initializing the processor state are checked for consistency and any failure results in a shutdown condition.

A summary of the register state initialization after successful completion of GETSEC[ENTERACCS] is given for the processor in Table 6-4. The paging is disabled upon entry into authenticated code execution mode. The authenticated code module is loaded and initially executed using physical addresses. It is up to the system software after execution of GETSEC[ENTERACCS] to establish a new (or restore its previous) paging environment with an appropriate mapping to meet new protection requirements. EBP is initialized to the authenticated code module base physical address for initial execution in the authenticated environment. As a result, the authenticated code can reference EBP for relative address based references, given that the authenticated code module must be position independent.

Table 6-4. Register State Initialization after GETSEC[ENTERACCS]

| Register State | Initialization Status | Comment |
|----------------|--|---|
| CR0 | PG←0, AM←0, WP←0: Others unchanged | Paging, Alignment Check, Write-protection are disabled |
| CR4 | MCE←0: Others unchanged | Machine Check Exceptions Disabled |
| EFLAGS | 00000002H | |
| IA32_EFER | 0H | IA-32e mode disabled |
| EIP | AC.base + EntryPoint | AC.base is in EBX as input to GETSEC[ENTERACCS] |
| [E R]BX | Pre-ENTERACCS state: Next [E R]IP prior to GETSEC[ENTERACCS] | Carry forward 64-bit processor state across GETSEC[ENTERACCS] |
| ECX | Pre-ENTERACCS state: [31:16]=GDTR.limit; [15:0]=CS.sel | Carry forward processor state across GETSEC[ENTERACCS] |
| [E R]DX | Pre-ENTERACCS state: GDTR base | Carry forward 64-bit processor state across GETSEC[ENTERACCS] |
| EBP | AC.base | |
| CS | Sel=[SegSel], base=0, limit=FFFFFFh, G=1, D=1, AR=9BH | |
| DS | Sel=[SegSel] +8, base=0, limit=FFFFFFh, G=1, D=1, AR=93H | |

Table 6-4. Register State Initialization after GETSEC[ENTERACCS] (Contd.)

| Register State | Initialization Status | Comment |
|-----------------------|---|---|
| GDTR | Base= AC.base (EBX) + [GDTBasePtr], Limit=[GDTLimit] | |
| DR7 | 00000400H | |
| IA32_DEBUGCTL | 0H | |
| IA32_MISC_ENA BLES | see Table 6-5 for example | The number of initialized fields may change due to processor implementation |

The segmentation related processor state that has not been initialized by GETSEC[ENTERACCS] requires appropriate initialization before use. Since a new GDT context has been established, the previous state of the segment selector values held in ES, SS, FS, GS, TR, and LDTR might not be valid.

The MSR IA32_EFER is also unconditionally cleared as part of the processor state initialized by ENTERACCS. Since paging is disabled upon entering authenticated code execution mode, a new paging environment will have to be reestablished in order to establish IA-32e mode while operating in authenticated code execution mode.

Debug exception and trap related signaling is also disabled as part of GETSEC[ENTERACCS]. This is achieved by resetting DR7, TF in EFLAGS, and the MSR IA32_DEBUGCTL. These debug functions are free to be re-enabled once supporting exception handler(s), descriptor tables, and debug registers have been properly initialized following entry into authenticated code execution mode. Also, any pending single-step trap condition will have been cleared upon entry into this mode.

The IA32_MISC_ENABLES MSR is initialized upon entry into authenticated execution mode. Certain bits of this MSR are preserved because preserving these bits may be important to maintain previously established platform settings (See the footnote for Table 6-5.). The remaining bits are cleared for the purpose of establishing a more consistent environment for the execution of authenticated code modules. One of the impacts of initializing this MSR is any previous condition established by the MONITOR instruction will be cleared.

To support the possible return to the processor architectural state prior to execution of GETSEC[ENTERACCS], certain critical processor state is captured and stored in the general- purpose registers at instruction completion. [E|R]BX holds effective address ([E|R]IP) of the instruction that would execute next after GETSEC[ENTERACCS], ECX[15:0] holds the CS selector value, ECX[31:16] holds the GDTR limit field, and [E|R]DX holds the GDTR base field. The subsequent authenticated code can preserve the contents of these registers so that this state can be manually restored if needed, prior to exiting authenticated code execution mode with GETSEC[EXITAC]. For the processor state after exiting authenticated code execution mode, see the description of GETSEC[SEXIT].

Table 6-5. IA32_MISC_ENALBES MSR Initialization¹ by ENTERACCS and SENTER

| Field | Bit position | Description |
|---------------------------------------|--------------|---|
| Fast strings enable | 0 | Clear to 0 |
| FOPCODE compatibility mode enable | 2 | Clear to 0 |
| Thermal monitor enable | 3 | Set to 1 if other thermal monitor capability is not enabled. ² |
| Split-lock disable | 4 | Clear to 0 |
| Bus lock on cache line splits disable | 8 | Clear to 0 |
| Hardware prefetch disable | 9 | Clear to 0 |
| GV1/2 legacy enable | 15 | Clear to 0 |
| MONITOR/MWAIT s/m enable | 18 | Clear to 0 |
| Adjacent sector prefetch disable | 19 | Clear to 0 |

NOTES:

1. The number of IA32_MISC_ENABLES fields that are initialized may vary due to processor implementations.
2. ENTERACCS (and SENTER) initialize the state of processor thermal throttling such that at least a minimum level is enabled. If thermal throttling is already enabled when executing one of these GETSEC leaves, then no change in the thermal throttling control settings will occur. If thermal throttling is disabled, then it will be enabled via setting of the thermal throttle control bit 3 as a result of executing these GETSEC leaves.

The IDTR will also require reloading with a new IDT context after entering authenticated code execution mode, before any exceptions or the external interrupts INTR and NMI can be handled. Since external interrupts are re-enabled at the completion of authenticated code execution mode (as terminated with EXITAC), it is recommended that a new IDT context be established before this point. Until such a new IDT context is established, the programmer must take care in not executing an INT n instruction or any other operation that would result in an exception or trap signaling.

Prior to completion of the GETSEC[ENTERACCS] instruction and after successful authentication of the AC module, the private configuration space of the Intel TXT chipset is unlocked. The authenticated code module alone can gain access to this normally restricted chipset state for the purpose of securing the platform.

Once the authenticated code module is launched at the completion of GETSEC[ENTERACCS], it is free to enable interrupts by setting EFLAGS.IF and enable NMI by execution of IRET. This presumes that it has re-established interrupt handling support through initialization of the IDT, GDT, and corresponding interrupt handling code.

Operation in a Uni-Processor Platform

(* The state of the internal flag ACMODEFLAG persists across instruction boundary *)

```

IF (CR4.SMXE=0)
    THEN #UD;
ELSIF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
ELSIF (GETSEC leaf unsupported)
    THEN #UD;
ELSIF ((in VMX operation) or
    (CRO.PE=0) or (CRO.CD=1) or (CRO.NW=1) or (CRO.NE=0) or
    (CPL>0) or (EFLAGS.VM=1) or
    (IA32_APIC_BASE.BSP=0) or
    (TXT chipset not present) or
    (ACMODEFLAG=1) or (IN_SMM=1))
    THEN #GP(0);
FOR I = 0 to IA32_MCG_CAP.COUNT-1 DO
    IF (IA32_MC[I]_STATUS← uncorrectable error)
        THEN #GP(0);
OD;
IF (IA32_MCG_STATUS.MCIP=1) or (IERR pin is asserted)
    THEN #GP(0);
ACBASE← EBX;
ACSIZE← ECX;
IF (((ACBASE MOD 4096) != 0) or ((ACSIZE MOD 64) != 0) or (ACSIZE < minimum module size) OR
(ACSIZE > authenticated RAM capacity)) or ((ACBASE+ACSIZE) > (2^32 - 1)))
    THEN #GP(0);
IF (secondary thread(s) CRO.CD = 1) or ((secondary thread(s) NOT(wait-for-SIPI)) and
    (secondary thread(s) not in SENTER sleep state))
    THEN #GP(0);
Mask SMI, INIT, A20M, and NMI external pin events;
IA32_MISC_ENABLE← (IA32_MISC_ENABLE & MASK_CONST*)
(* The hexadecimal value of MASK_CONST may vary due to processor implementations *)
A20M← 0;
IA32_DEBUGCTL← 0;
Invalidate processor TLB(s);
Drain Outgoing Transactions;
ACMODEFLAG← 1;
SignalTXTMessage(ProcessorHold);
    
```

```

Load the internal ACRAM based on the AC module size;
(* Ensure that all ACRAM loads hit Write Back memory space *)
IF (ACRAM memory type != WB)
    THEN TXT-SHUTDOWN(#BadACMMType);
IF (AC module header version isnot supported) OR (ACRAM[ModuleType] <> 2)
    THEN TXT-SHUTDOWN(#UnsupportedACM);
(* Authenticate the AC Module and shutdown with an error if it fails *)
KEY← GETKEY(ACRAM, ACBASE);
KEYHASH← HASH(KEY);
CSKEYHASH← READ(TXT.PUBLIC.KEY);
IF (KEYHASH <> CSKEYHASH)
    THEN TXT-SHUTDOWN(#AuthenticateFail);
SIGNATURE← DECRYPT(ACRAM, ACBASE, KEY);
(* The value of SIGNATURE_LEN_CONST is implementation-specific*)
FOR I=0 to SIGNATURE_LEN_CONST - 1 DO
    ACRAM[SCRATCH.I]← SIGNATURE[I];
COMPUTEDSIGNATURE← HASH(ACRAM, ACBASE, ACSIZE);
FOR I=0 to SIGNATURE_LEN_CONST - 1 DO
    ACRAM[SCRATCH.SIGNATURE_LEN_CONST+I]← COMPUTEDSIGNATURE[I];
IF (SIGNATURE<>COMPUTEDSIGNATURE)
    THEN TXT-SHUTDOWN(#AuthenticateFail);
ACMCONTROL← ACRAM[CodeControl];
IF ((ACMCONTROL.0 = 0) and (ACMCONTROL.1 = 1) and (snoop hit to modified line detected on
ACRAM load))
    THEN TXT-SHUTDOWN(#UnexpectedHITM);
IF (ACMCONTROL reserved bits are set)
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACRAM[GDTBasePtr] < (ACRAM[HeaderLen] * 4 + Scratch_size)) OR
((ACRAM[GDTBasePtr] + ACRAM[GDTLimit]) >= ACSIZE))
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACMCONTROL.0 = 1) and (ACMCONTROL.1 = 1) and (snoop hit to modified line detected on
ACRAM load))
    THEN ACEntryPoint← ACBASE+ACRAM[ErrorEntryPoint];
ELSE
    ACEntryPoint← ACBASE+ACRAM[EntryPoint];
IF ((ACEntryPoint >= ACSIZE) OR (ACEntryPoint < (ACRAM[HeaderLen] * 4 + Scratch_size)))THEN
    TXT-SHUTDOWN(#BadACMFormat);
IF (ACRAM[GDTLimit] & FFFF0000h)
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACRAM[SegSel] > (ACRAM[GDTLimit] - 15)) OR (ACRAM[SegSel] < 8))
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACRAM[SegSel].TI=1) OR (ACRAM[SegSel].RPLI=0))
    THEN TXT-SHUTDOWN(#BadACMFormat);
CRO.[PG.AM.WP]← 0;

```

SAFER MODE EXTENSIONS REFERENCE

```
CR4.MCE← 0;
EFLAGS← 00000002h;
IA32_EFER← 0h;
[E|R]BX← [E|R]IP of the instruction after GETSEC[ENTERACCS];
ECX← Pre-GETSEC[ENTERACCS] GDT.limit:CS.sel;
[E|R]DX← Pre-GETSEC[ENTERACCS] GDT.base;
EBP← ACBASE;
GDTR.BASE← ACBASE+ACRAM[GDTBasePtr];
GDTR.LIMIT← ACRAM[GDTLimit];
CS.SEL← ACRAM[SegSel];
CS.BASE← 0;
CS.LIMIT← FFFFh;
CS.G← 1;
CS.D← 1;
CS.AR← 9Bh;
DS.SEL← ACRAM[SegSel]+8;
DS.BASE← 0;
DS.LIMIT← FFFFh;
DS.G← 1;
DS.D← 1;
DS.AR← 93h;
DR7← 00000400h;
IA32_DEBUGCTL← 0;
DR6.BS← 0;
SignalXTMsg(OpenPrivate);
SignalXTMsg(OpenLocality3);
EIP← ACEntryPoint;
END;
```

Flags Affected

All flags are cleared.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

#UD If CR4.SMXE = 0.

| | |
|--------|--|
| #GP(0) | <p>If GETSEC[ENTERACCS] is not reported as supported by GETSEC[CAPABILITIES].</p> <p>If CR0.CD = 1 or CR0.NW = 1 or CR0.NE = 0 or CR0.PE = 0 or CPL > 0 or EFLAGS.VM = 1.</p> <p>If a Intel® TXT-capable chipset is not present.</p> <p>If in VMX root operation.</p> <p>If the initiating processor is not designated as the bootstrap processor via the MSR bit IA32_APIC_BASE.BSP.</p> <p>If the processor is already in authenticated code execution mode.</p> <p>If the processor is in SMM.</p> <p>If a valid uncorrectable machine check error is logged in IA32_MC[1]_STATUS.</p> <p>If the authenticated code base is not on a 4096 byte boundary.</p> <p>If the authenticated code size > processor internal authenticated code area capacity.</p> <p>If the authenticated code size is not modulo 64.</p> <p>If other enabled logical processor(s) of the same package CR0.CD = 1.</p> <p>If other enabled logical processor(s) of the same package are not in the wait-for-SIPI or SENTER sleep state.</p> |
|--------|--|

Real-Address Mode Exceptions

| | |
|--------|---|
| #UD | <p>If CR4.SMXE = 0.</p> <p>If GETSEC[ENTERACCS] is not reported as supported by GETSEC[CAPABILITIES].</p> |
| #GP(0) | GETSEC[ENTERACCS] is not recognized in real-address mode. |

Virtual-8086 Mode Exceptions

| | |
|--------|---|
| #UD | <p>If CR4.SMXE = 0.</p> <p>If GETSEC[ENTERACCS] is not reported as supported by GETSEC[CAPABILITIES].</p> |
| #GP(0) | GETSEC[ENTERACCS] is not recognized in virtual-8086 mode. |

Compatibility Mode Exceptions

All protected mode exceptions apply.

| | |
|-----|--|
| #GP | IF AC code module does not reside in physical address below $2^{32} - 1$. |
|-----|--|

64-Bit Mode Exceptions

All protected mode exceptions apply.

#GP IF AC code module does not reside in physical address below $2^{32} - 1$.

VM-exit Condition

Reason (GETSEC) IF in VMX non-root operation.

GETSEC[EXITAC]—Exit Authenticated Code Execution Mode

| Opcode | Instruction | Description |
|------------------|----------------------|---|
| OF 37 (EAX=3) | GETSEC[EXITAC] CJ | Exit authenticated code execution mode. RBX holds the Near Absolute Indirect jump target and EDX hold the exit parameter flags |

Description

The GETSEC[EXITAC] leaf function exits the ILP out of authenticated code execution mode established by GETSEC[ENTERACCS] or GETSEC[SENDER]. The EXITAC leaf of GETSEC is selected with EAX set to 3 at entry. EBX (or RBX, if in 64-bit mode) holds the near jump target offset for where the processor execution resumes upon exiting authenticated code execution mode. EDX contains additional parameter control information. Currently only an input value of 0 in EDX is supported. All other EDX settings are considered reserved and result in a general protection violation.

GETSEC[EXITAC] can only be executed if the processor is in protected mode with CPL = 0 and EFLAGS.VM = 0. The processor must also be in authenticated code execution mode. To avoid potential operability conflicts between modes, the processor is not allowed to execute this instruction if it is in SMM or in VMX operation. A violation of these conditions results in a general protection violation.

Upon completion of the GETSEC[EXITAC] operation, the processor unmask responses to external event signals INIT#, NMI#, and SMI#. This unmasking is performed conditionally, based on whether the authenticated code execution mode was entered via execution of GETSEC[SENDER] or GETSEC[ENTERACCS]. If the processor is in authenticated code execution mode due to the execution of GETSEC[SENDER], then these external event signals will remain masked. In this case, A20M is kept disabled in the measured environment until the measured environment executes GETSEC[SEXIT]. INIT# is unconditionally unmasked by EXITAC. Note that any events that are pending, but have been blocked while in authenticated code execution mode, will be recognized at the completion of the GETSEC[EXITAC] instruction if the pin event is unmasked.

The intent of providing the ability to optionally leave the pin events SMI#, and NMI# masked is to support the completion of a measured environment bring-up that makes use of VMX. In this envisioned security usage scenario, these events will remain masked until an appropriate virtual machine has been established in order to field servicing of these events in a safer manner. Details on when and how events are masked and unmasked in VMX operation are described in *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B*. It should be cautioned that if no VMX environment is to be activated following GETSEC[EXITAC], that these events will remain masked until the measured environment is exited with GETSEC[SEXIT]. If this is not desired then the GETSEC function SMCTRL(0) can be used for unmasking SMI# in this context. NMI# can be correspondingly unmasked by execution of IRET.

A successful exit of the authenticated code execution mode requires the ILP to perform additional steps as outlined below:

- Invalidate the contents of the internal authenticated code execution area.
- Invalidate processor TLBs.
- Clear the internal processor AC Mode indicator flag.
- Re-lock the TPM locality 3 space.
- Unlock the Intel® TXT-capable chipset memory and I/O protections to allow memory and I/O activity by other processor agents.
- Perform a near absolute indirect jump to the designated instruction location.

The content of the authenticated code execution area is invalidated by hardware in order to protect it from further use or visibility. This internal processor storage area can no longer be used or relied upon after GETSEC[EXITAC]. Data structures need to be re-established outside of the authenticated code execution area if they are to be referenced after EXITAC. Since addressed memory content formerly mapped to the authenticated code execution area may no longer be coherent with external system memory after EXITAC, processor TLBs in support of linear to physical address translation are also invalidated.

Upon completion of GETSEC[EXITAC] a near absolute indirect transfer is performed with EIP loaded with the contents of EBX (based on the current operating mode size). In 64-bit mode, all 64 bits of RBX are loaded into RIP if REX.W precedes GETSEC[EXITAC]. Otherwise RBX is treated as 32 bits even while in 64-bit mode. Conventional CS limit checking is performed as part of this control transfer. Any exception conditions generated as part of this control transfer will be directed to the existing IDT; thus it is recommended that an IDTR should also be established prior to execution of the EXITAC function if there is a need for fault handling. In addition, any segmentation related (and paging) data structures to be used after EXITAC should be re-established or validated by the authenticated code prior to EXITAC.

In addition, any segmentation related (and paging) data structures to be used after EXITAC need to be re-established and mapped outside of the authenticated RAM designated area by the authenticated code prior to EXITAC. Any data structure held within the authenticated RAM allocated area will no longer be accessible after completion by EXITAC.

Operation

(* The state of the internal flag ACMODEFLAG and SENTERFLAG persist across instruction boundary *)

```
IF (CR4.SMXE=0)  
    THEN #UD;
```

```
ELSIF ( in VMX non-root operation)
```

```
    THEN VM Exit (reason="GETSEC instruction");
```

```
ELSIF (GETSEC leaf unsupported)
```

```
    THEN #UD;
```

```
ELSIF ((in VMX operation) or ( (in 64-bit mode) and ( RBX is non-canonical) )
```

```

(CR0.PE=0) or (CPL>0) or (EFLAGS.VM=1) or
(ACMODEFLAG=0) or (IN_SMM=1)) or (EDX != 0))
THEN #GP(0);
IF (OperandSize = 32)
    THEN tempEIP← EBX;
ELIF (OperandSize = 64)
    THEN tempEIP← RBX;
ELSE
    tempEIP← EBX AND 0000FFFFH;
IF (tempEIP > code segment limit)
    THEN #GP(0);
Invalidate ACRAM contents;
Invalidate processor TLB(s);
Drain outgoing messages;
SignalTXTMsg(CloseLocality3);
SignalTXTMsg(LockSMRAM);
SignalTXTMsg(ProcessorRelease);
Unmask INIT;
IF (SENTERFLAG=0)
    THEN Unmask SMI, INIT, NMI, and A20M pin event;
ACMODEFLAG← 0;
EIP← tempEIP;
END;

```

Flags Affected

None.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX.W | Sets 64-bit mode Operand size attribute |

Protected Mode Exceptions

| | |
|--------|---|
| #UD | If CR4.SMXE = 0. If GETSEC[EXITAC] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | If CR0.PE = 0 or CPL>0 or EFLAGS.VM = 1. If in VMX root operation. |

SAFER MODE EXTENSIONS REFERENCE

If the processor is not currently in authenticated code execution mode.

If the processor is in SMM.

If any reserved bit position is set in the EDX parameter register.

Real-Address Mode Exceptions

- #UD If CR4.SMXE = 0.
If GETSEC[EXITAC] is not reported as supported by GETSEC[CAPABILITIES].
- #GP(0) GETSEC[EXITAC] is not recognized in real-address mode.

Virtual-8086 Mode Exceptions

- #UD If CR4.SMXE = 0.
If GETSEC[EXITAC] is not reported as supported by GETSEC[CAPABILITIES].
- #GP(0) GETSEC[EXITAC] is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

All protected mode exceptions apply.

64-Bit Mode Exceptions

All protected mode exceptions apply.

- #GP(0) If the target address in RBX is not in a canonical form.

VM-Exit Condition

- Reason (GETSEC) IF in VMX non-root operation.

GETSEC[SENTER]—Enter a Measured Environment

| Opcode | Instruction | Description |
|------------------|----------------|--|
| OF 37 (EAX=4) | GETSEC[SENTER] | <p>Launch a measured environment</p> <p>EBX holds the SINIT authenticated code module physical base address.</p> <p>ECX holds the SINIT authenticated code module size (bytes).</p> <p>EDX controls the level of functionality supported by the measured environment launch.</p> |

Description

The GETSEC[SENTER] instruction initiates the launch of a measured environment and places the initiating logical processor (ILP) into the authenticated code execution mode. The SENTER leaf of GETSEC is selected with EAX set to 4 at execution. The physical base address of the AC module to be loaded and authenticated is specified in EBX. The size of the module in bytes is specified in ECX. EDX controls the level of functionality supported by the measured environment launch. To enable the full functionality of the protected environment launch, EDX must be initialized to zero.

The authenticated code base address and size parameters (in bytes) are passed to the GETSEC[SENTER] instruction using EBX and ECX respectively. The ILP evaluates the contents of these registers according to the rules for the AC module address in GETSEC[ENTERACCS]. AC module execution follows the same rules, as set by GETSEC[ENTERACCS].

The launching software must ensure that the TPM.ACCESS_0.activeLocality bit is clear before executing the GETSEC[SENTER] instruction.

There are restrictions enforced by the processor for execution of the GETSEC[SENTER] instruction:

- Execution is not allowed unless the processor is in protected mode or IA-32e mode with CPL = 0 and EFLAGS.VM = 0.
- Processor cache must be available and not disabled using the CR0.CD and NW bits.
- For enforcing consistency of operation with numeric exception reporting using Interrupt 16, CR0.NE must be set.
- An Intel TXT-capable chipset must be present as communicated to the processor by sampling of the power-on configuration capability field after reset.
- The processor can not be in authenticated code execution mode or already in a measured environment (as launched by a previous GETSEC[ENTERACCS] or GETSEC[SENTER] instruction).
- To avoid potential operability conflicts between modes, the processor is not allowed to execute this instruction if it currently is in SMM or VMX operation.

- To insure consistent handling of SIPI messages, the processor executing the GETSEC[SENDER] instruction must also be designated the BSP (boot-strap processor) as defined by A32_APIC_BASE.BSP (Bit 8).
- EDX must be initialized to a setting supportable by the processor. Unless enumeration by the GETSEC[PARAMETERS] leaf reports otherwise, only a value of zero is supported.

Failure to abide by the above conditions results in the processor signaling a general protection violation.

This instruction leaf starts the launch of a measured environment by initiating a rendezvous sequence for all logical processors in the platform. The rendezvous sequence involves the initiating logical processor sending a message (by executing GETSEC[SENDER]) and other responding logical processors (RLPs) acknowledging the message, thus synchronizing the RLP(s) with the ILP.

In response to a message signaling the completion of rendezvous, RLPs clear the bootstrap processor indicator flag (IA32_APIC_BASE.BSP) and enter an SENTER sleep state. In this sleep state, RLPs enter an idle processor condition while waiting to be activated after a measured environment has been established by the system executive. RLPs in the SENTER sleep state can only be activated by the GETSEC leaf function WAKEUP in a measured environment.

A successful launch of the measured environment results in the initiating logical processor entering the authenticated code execution mode. Prior to reaching this point, the ILP performs the following steps internally:

- Inhibit processor response to the external events: INIT, A20M, NMI, and SMI.
- Establish and check the location and size of the authenticated code module to be executed by the ILP.
- Check for the existence of an Intel® TXT-capable chipset.
- Verify the current power management configuration is acceptable.
- Broadcast a message to enable protection of memory and I/O from activities from other processor agents.
- Load the designated AC module into authenticated code execution area.
- Isolate the content of authenticated code execution area from further state modification by external agents.
- Authenticate the AC module.
- Updated the Trusted Platform Module (TPM) with the authenticated code module's hash.
- Initialize processor state based on the authenticated code module header information.
- Unlock the Intel® TXT-capable chipset private configuration register space and TPM locality 3 space.
- Begin execution in the authenticated code module at the defined entry point.

As an integrity check for proper processor hardware operation, execution of GETSEC[SENTER] will also check the contents of all the machine check status registers (as reported by the MSRs IA32_MCi_STATUS) for any valid uncorrectable error condition. In addition, the global machine check status register IA32_MCG_STATUS MCIP bit must be cleared and the IERR processor package pin (or its equivalent) must be not asserted, indicating that no machine check exception processing is currently in-progress. These checks are performed twice: once by the ILP prior to the broadcast of the rendezvous message to RLPs, and later in response to RLPs acknowledging the rendezvous message. Any outstanding valid uncorrectable machine check error condition present in the machine check status registers at the first check point will result in the ILP signaling a general protection violation. If an outstanding valid uncorrectable machine check error condition is present at the second check point, then this will result in the corresponding logical processor signaling the more severe TXT-shutdown condition with an error code of 12.

Before loading and authentication of the target code module is performed, the processor also checks that the current voltage and bus ratio encodings correspond to known good values supportable by the processor. The MSR IA32_PERF_STATUS values are compared against either the processor supported maximum operating target setting, system reset setting, or the thermal monitor operating target. If the current settings do not meet any of these criteria then the SENTER function will attempt to change the voltage and bus ratio select controls in a processor-specific manner. This adjustment may be to the thermal monitor, minimum (if different), or maximum operating target depending on the processor.

This implies that some thermal operating target parameters configured by BIOS may be overridden by SENTER. The measured environment software may need to take responsibility for restoring such settings that are deemed to be safe, but not necessarily recognized by SENTER. If an adjustment is not possible when an out of range setting is discovered, then the processor will abort the measured launch. This may be the case for chipset controlled settings of these values or if the controllability is not enabled on the processor. In this case it is the responsibility of the external software to program the chipset voltage ID and/or bus ratio select settings to known good values recognized by the processor, prior to executing SENTER.

NOTE

For a mobile processor, an adjustment can be made according to the thermal monitor operating target. For a quad-core processor the SENTER adjustment mechanism may result in a more conservative but non-uniform voltage setting, depending on the pre-SENTER settings per core.

The ILP and RLPs mask the response to the assertion of the external signals INIT#, A20M, NMI#, and SMI#. The purpose of this masking control is to prevent exposure to existing external event handlers until a protected handler has been put in place to directly handle these events. Masked external pin events may be unmasked conditionally or unconditionally via the GETSEC[EXITAC], GETSEC[SEXIT], GETSEC[SMCTRL] or for specific VMX related operations such as a VM entry or the

VMXOFF instruction (see respective GETSEC leaves and *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B* for more details). The state of the A20M pin is masked and forced internally to a de-asserted state so that external assertion is not recognized. A20M masking as set by GETSEC[SENER] is undone only after taking down the measured environment with the GETSEC[SEXIT] instruction or processor reset. INTR is masked by simply clearing the EFLAGS.IF bit. It is the responsibility of system software to control the processor response to INTR through appropriate management of EFLAGS.

To prevent other (logical) processors from interfering with the ILP operating in authenticated code execution mode, memory (excluding implicit write-back transactions) and I/O activities originating from other processor agents are blocked. This protection starts when the ILP enters into authenticated code execution mode. Only memory and I/O transactions initiated from the ILP are allowed to proceed. Exiting authenticated code execution mode is done by executing GETSEC[EXITAC]. The protection of memory and I/O activities remains in effect until the ILP executes GETSEC[EXITAC].

Once the authenticated code module has been loaded into the authenticated code execution area, it is protected against further modification from external bus snoops. There is also a requirement that the memory type for the authenticated code module address range be WB (via initialization of the MTRRs prior to execution of this instruction). If this condition is not satisfied, it is a violation of security and the processor will force a TXT system reset (after writing an error code to the chipset LT.ERROR-CODE register). This action is referred to as a Intel® TXT reset condition. It is performed when it is considered unreliable to signal an error through the conventional exception reporting mechanism.

To conform to the minimum granularity of MTRR MSRs for specifying the memory type, authenticated code RAM (ACRAM) is allocated to the processor in 4096 byte granular blocks. If an AC module size as specified in ECX is not a multiple of 4096 then the processor will allocate up to the next 4096 byte boundary for mapping as ACRAM with indeterminate data. This pad area will not be visible to the authenticated code module as external memory nor can it depend on the value of the data used to fill the pad area.

Once successful authentication has been completed by the ILP, the computed hash is stored in the TPM at PCR17 after this register is implicitly reset. PCR17 is a dedicated register for holding the computed hash of the authenticated code module loaded and subsequently executed by the GETSEC[SENER]. As part of this process, the dynamic PCRs 18-22 are reset so they can be utilized by subsequently software for registration of code and data modules. After successful execution of SENER, PCR17 contains the measurement of AC code and the SENER launching parameters.

After authentication is completed successfully, the private configuration space of the Intel® TXT-capable chipset is unlocked so that the authenticated code module and measured environment software can gain access to this normally restricted chipset state. The Intel® TXT-capable chipset private configuration space can be locked later by software writing to the chipset LT.CMD.CLOSE-PRIVATE register or unconditionally using the GETSEC[SEXIT] instruction.

The SENTER leaf function also initializes some processor architecture state for the ILP from contents held in the header of the authenticated code module. Since the authenticated code module is relocatable, all address references are relative to the base address passed in via EBX. The ILP GDTR base value is initialized to $EBX + [GDTBasePtr]$ and GDTR limit set to $[GDTLimit]$. The CS selector is initialized to the value held in the AC module header field SegSel, while the DS, SS, and ES selectors are initialized to CS+8. The segment descriptor fields are initialized implicitly with BASE=0, LIMIT=FFFFFh, G=1, D=1, P=1, S=1, read/write/accessed for DS, SS, and ES, while execute/read/accessed for CS. Execution in the authenticated code module for the ILP begins with the EIP set to $EBX + [EntryPoint]$. AC module defined fields used for initializing processor state are consistency checked with a failure resulting in an TXT-shutdown condition.

Table 6-6 provides a summary of processor state initialization for the ILP and RLP(s) after successful completion of GETSEC[SENTER]. For both ILP and RLP(s), paging is disabled upon entry to the measured environment. It is up to the ILP to establish a trusted paging environment, with appropriate mappings, to meet protection requirements established during the launch of the measured environment. RLP state initialization is not completed until a subsequent wake-up has been signaled by execution of the GETSEC[WAKEUP] function by the ILP.

Table 6-6. Register State Initialization after GETSEC[SENTER] and GETSEC[WAKEUP]

| Register State | ILP after GETSEC[SENTER] | RLP after GETSEC[WAKEUP] |
|----------------|--|---|
| CR0 | $PG \leftarrow 0$, $AM \leftarrow 0$, $WP \leftarrow 0$; Others unchanged | $PG \leftarrow 0$, $CD \leftarrow 0$, $NW \leftarrow 0$, $AM \leftarrow 0$, $WP \leftarrow 0$; $PE \leftarrow 1$, $NE \leftarrow 1$ |
| CR4 | 00004000H | 00004000H |
| EFLAGS | 00000002H | 00000002H |
| IA32_EFER | 0H | 0 |
| EIP | $[EntryPoint \text{ from MLE header}^1]$ | $[LT.MLE.JOIN + 12]$ |
| EBX | Unchanged $[SINIT.BASE]$ | Unchanged |
| EDX | SENTER control flags | Unchanged |
| EBP | SINIT.BASE | Unchanged |
| CS | Sel= $[SINIT.SegSel]$, base=0, limit=FFFFFh, G=1, D=1, AR=9BH | Sel = $[LT.MLE.JOIN + 8]$, base = 0, limit = FFFFFFFH, G = 1, D = 1, AR = 9BH |
| DS, ES, SS | Sel= $[SINIT.SegSel] + 8$, base=0, limit=FFFFFh, G=1, D=1, AR=93H | Sel = $[LT.MLE.JOIN + 8] + 8$, base = 0, limit = FFFFFFFH, G = 1, D = 1, AR = 93H |

Table 6-6. Register State Initialization after GETSEC[SENDER] and GETSEC[WAKEUP]

| | | |
|--|---|--|
| GDTR | Base= SINIT.base (EBX) + [SINIT.GDTBasePtr], Limit=[SINIT.GDTLimit] | Base = [LT.MLE.JOIN + 4], Limit = [LT.MLE.JOIN] |
| DR7 | 00000400H | 00000400H |
| IA32_DEBUGCTL | 0H | 0H |
| Performance counters and counter control registers | 0H | 0H |
| IA32_MISC_ENABLES | see Table 6-5 | see Table 6-5 |

NOTES:

1. See *Intel® Trusted Execution Technology Measured Launched Environment Programming Guide* for MLE header format.

Segmentation related processor state that has not been initialized by GETSEC[SENDER] requires appropriate initialization before use. Since a new GDT context has been established, the previous state of the segment selector values held in FS, GS, TR, and LDTR may no longer be valid. The IDTR will also require reloading with a new IDT context after launching the measured environment before exceptions or the external interrupts INTR and NMI can be handled. In the meantime, the programmer must take care in not executing an INT n instruction or any other condition that would result in an exception or trap signaling.

Debug exception and trap related signaling is also disabled as part of execution of GETSEC[SENDER]. This is achieved by clearing DR7, TF in EFLAGS, and the MSR IA32_DEBUGCTL as defined in Table 6-6. These can be re-enabled once supporting exception handler(s), descriptor tables, and debug registers have been properly re-initialized following SENTER. Also, any pending single-step trap condition will be cleared at the completion of SENTER for both the ILP and RLP(s).

Performance related counters and counter control registers are cleared as part of execution of SENTER on both the ILP and RLP. This implies any active performance counters at the time of SENTER execution will be disabled. To reactive the processor performance counters, this state must be re-initialized and re-enabled.

Since MCE along with all other state bits (with the exception of SMXE) are cleared in CR4 upon execution of SENTER processing, any enabled machine check error condition that occurs will result in the processor performing the TXT-shutdown action. This also applies to an RLP while in the SENTER sleep state. For each logical processor CR4.MCE must be reestablished with a valid machine check exception handler to otherwise avoid an TXT-shutdown under such conditions.

The MSR IA32_EFER is also unconditionally cleared as part of the processor state initialized by SENTER for both the ILP and RLP. Since paging is disabled upon entering authenticated code execution mode, a new paging environment will have to be re-established if it is desired to enable IA-32e mode while operating in authenticated code execution mode.

The miscellaneous feature control MSR, IA32_MISC_ENABLES, is initialized as part of the measured environment launch. Certain bits of this MSR are preserved because preserving these bits may be important to maintain previously established platform settings. See the footnote for Table 6-5 The remaining bits are cleared for the purpose of establishing a more consistent environment for the execution of authenticated code modules. Among the impact of initializing this MSR, any previous condition established by the MONITOR instruction will be cleared.

Effect of MSR IA32_FEATURE_CONTROL MSR

Bits 15:8 of the IA32_FEATURE_CONTROL MSR affect the execution of GETSEC[SENTER]. These bits consist of two fields:

- Bit 15: a global enable control for execution of SENTER.
- Bits 14:8: a parameter control field providing the ability to qualify SENTER execution based on the level of functionality specified with corresponding EDX parameter bits 6:0.

The layout of these fields in the IA32_FEATURE_CONTROL MSR is shown in Table 6-1.

Prior to the execution of GETSEC[SENTER], the lock bit of IA32_FEATURE_CONTROL MSR must be bit set to affirm the settings to be used. Once the lock bit is set, only a power-up reset condition will clear this MSR. The IA32_FEATURE_CONTROL MSR must be configured in accordance to the intended usage at platform initialization. Note that this MSR is only available on SMX or VMX enabled processors. Otherwise, IA32_FEATURE_CONTROL is treated as reserved.

The *Intel® Trusted Execution Technology Measured Launched Environment Programming Guide* provides additional details and requirements for programming measured environment software to launch in an Intel TXT platform.

Operation in a Uni-Processor Platform

(* The state of the internal flag ACMODEFLAG and SENTERFLAG persist across instruction boundary *)

GETSEC[SENTER] (ILP only):

```
IF (CR4.SMXE=0)
    THEN #UD;
ELSE IF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
ELSE IF (GETSEC leaf unsupported)
    THEN #UD;
ELSE IF ((in VMX root operation) or
    (CRO.PE=0) or (CRO.CD=1) or (CRO.NW=1) or (CRO.NE=0) or
    (CPL>0) or (EFLAGS.VM=1) or
```

SAFER MODE EXTENSIONS REFERENCE

```
(IA32_APIC_BASE.BSP=0) or (TXT chipset not present) or
(SENTERFLAG=1) or (ACMODEFLAG=1) or (IN_SMM=1) or
(TPM interface is not present) or
(EDX != (SENTER_EDX_support_mask & EDX)) or
(IA32_CR_FEATURE_CONTROL[0]=0) or (IA32_CR_FEATURE_CONTROL[15]=0) or
((IA32_CR_FEATURE_CONTROL[14:8] & EDX[6:0]) != EDX[6:0]))
    THEN #GP(0);
FOR I = 0 to IA32_MCG_CAP.COUNT-1 DO
    IF IA32_MC[I]_STATUS = uncorrectable error
        THEN #GP(0);
    FI;
OD;
IF (IA32_MCG_STATUS.MCIP=1) or (IERR pin is asserted)
    THEN #GP(0);
ACBASE← EBX;
ACSIZE← ECX;
IF (((ACBASE MOD 4096) != 0) or ((ACSIZE MOD 64) != 0) or (ACSIZE < minimum
    module size) or (ACSIZE > AC RAM capacity) or ((ACBASE+ACSIZE) > (2^32 -1)))
    THEN #GP(0);
Mask SMI, INIT, A20M, and NMI external pin events;
SignalTXTMsg(SENTER);
DO
WHILE (no SignalSENTER message);

TXT_SENTER__MSG_EVENT (ILP & RLP):
Mask and clear SignalSENTER event;
Unmask SignalSEXIT event;
IF (in VMX operation)
    THEN TXT-SHUTDOWN(#IllegalEvent);
FOR I = 0 to IA32_MCG_CAP.COUNT-1 DO
    IF IA32_MC[I]_STATUS = uncorrectable error
        THEN TXT-SHUTDOWN(#UnrecovMCError);
    FI;
OD;
IF (IA32_MCG_STATUS.MCIP=1) or (IERR pin is asserted)
    THEN TXT-SHUTDOWN(#UnrecovMCError);
IF (Voltage or bus ratio status are NOT at a known good state)
    THEN IF (Voltage select and bus ratio are internally adjustable)
        THEN
            Make product-specific adjustment on operating parameters;
        ELSE
            TXT-SHUTDOWN(#IllegalVIDBRatio);
    FI;
FI;
```

```

IA32_MISC_ENABLE← (IA32_MISC_ENABLE & MASK_CONST*)
(* The hexadecimal value of MASK_CONST may vary due to processor implementations *)
A20M← 0;
IA32_DEBUGCTL← 0;
Invalidate processor TLB(s);
Drain outgoing transactions;
Clear performance monitor counters and control;
SENDERFLAG← 1;
SignalXTMMsg(SENTERAck);
IF (logical processor is not ILP)
    THEN GOTO RLP_SENTER_ROUTINE;
(* ILP waits for all logical processors to ACK *)
DO
    DONE← TXT.READ(LT.STS);
WHILE (not DONE);
SignalXTMMsg(SENTERContinue);
SignalXTMMsg(ProcessorHold);
FOR I=ACBASE to ACBASE+ACSIZE-1 DO
    ACRAM[I-ACBASE].ADDR← I;
    ACRAM[I-ACBASE].DATA← LOAD(I);
OD;
IF (ACRAM memory type != WB)
    THEN TXT-SHUTDOWN(#BadACMMType);
IF (AC module header version is not supported) OR (ACRAM[ModuleType] <> 2)
    THEN TXT-SHUTDOWN(#UnsupportedACM);
KEY← GETKEY(ACRAM, ACBASE);
KEYHASH← HASH(KEY);
CSKEYHASH← LT.READ(LT.PUBLIC.KEY);
IF (KEYHASH <> CSKEYHASH)
    THEN TXT-SHUTDOWN(#AuthenticateFail);
SIGNATURE← DECRYPT(ACRAM, ACBASE, KEY);
(* The value of SIGNATURE_LEN_CONST is implementation-specific*)
FOR I=0 to SIGNATURE_LEN_CONST - 1 DO
    ACRAM[SCRATCH.I]← SIGNATURE[I];
COMPUTEDSIGNATURE← HASH(ACRAM, ACBASE, ACSIZE);
FOR I=0 to SIGNATURE_LEN_CONST - 1 DO
    ACRAM[SCRATCH.SIGNATURE_LEN_CONST+I]← COMPUTEDSIGNATURE[I];
IF (SIGNATURE != COMPUTEDSIGNATURE)
    THEN TXT-SHUTDOWN(#AuthenticateFail);
ACMCONTROL← ACRAM[CodeControl];
IF ((ACMCONTROL.0 = 0) and (ACMCONTROL.1 = 1) and (snoop hit to modified line detected on
ACRAM load))
    THEN TXT-SHUTDOWN(#UnexpectedHITM);

```

SAFER MODE EXTENSIONS REFERENCE

```
IF (ACMCONTROL reserved bits are set)
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACRAM[GDTBasePtr] < (ACRAM[HeaderLen] * 4 + Scratch_size)) OR
    ((ACRAM[GDTBasePtr] + ACRAM[GDTLimit]) >= ACSIZE))
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACMCONTROL.0 = 1) and (ACMCONTROL.1 = 1) and (snoop hit to modified
    line detected on ACRAM load))
    THEN ACRAM[ErrorEntryPoint]← ACBASE+ACRAM[ErrorEntryPoint];
ELSE
    ACRAM[EntryPoint]← ACBASE+ACRAM[EntryPoint];
IF ((ACRAM[EntryPoint] >= ACSIZE) or (ACRAM[EntryPoint] < (ACRAM[HeaderLen] * 4 + Scratch_size)))
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACRAM[SegSel] > (ACRAM[GDTLimit] - 15)) or (ACRAM[SegSel] < 8))
    THEN TXT-SHUTDOWN(#BadACMFormat);
IF ((ACRAM[SegSel].TI=1) or (ACRAM[SegSel].RPL!=0))
    THEN TXT-SHUTDOWN(#BadACMFormat);
ACRAM[SCRATCH.SIGNATURE_LEN_CONST]← EDX;
WRITE(TPM.HASH.START)← 0;
FOR I=0 to SIGNATURE_LEN_CONST + 3 DO
    WRITE(TPM.HASH.DATA)← ACRAM[SCRATCH.I];
WRITE(TPM.HASH.END)← 0;
ACMODEFLAG← 1;
CRO.[PG.AM.WP]← 0;
CR4← 00004000h;
EFLAGS← 00000002h;
IA32_EFER← 0;
EBP← ACBASE;
GDTR.BASE← ACBASE+ACRAM[GDTBasePtr];
GDTR.LIMIT← ACRAM[GDTLimit];
CS.SEL← ACRAM[SegSel];
CS.BASE← 0;
CS.LIMIT← FFFFh;
CS.G← 1;
CS.D← 1;
CS.AR← 9Bh;
DS.SEL← ACRAM[SegSel]+8;
DS.BASE← 0;
DS.LIMIT← FFFFh;
DS.G← 1;
DS.D← 1;
DS.AR← 93h;
SS← DS;
ES← DS;
```

```

DR7← 00000400h;
IA32_DEBUGCTL← 0;
DR6.BS← 0;
SignalXTMMsg(UnlockSMRAM);
SignalXTMMsg(OpenPrivate);
SignalXTMMsg(OpenLocality3);
EIP← ACEntryPoint;
END;

```

RLP_SENTER_ROUTINE: (RPL only)

```

Mask SMI, INIT, A20M, and NMI external pin events
Unmask SignalWAKEUP event;
Wait for SignalSENTERContinue message;
IA32_APIC_BASE.BSP← 0;
GOTO SENTER sleep state;
END;

```

Flags Affected

All flags are cleared.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

| | |
|--------|---|
| #UD | <p>If CR4.SMXE = 0.</p> <p>If GETSEC[SENTER] is not reported as supported by GETSEC[CAPABILITIES].</p> |
| #GP(0) | <p>If CR0.CD = 1 or CR0.NW = 1 or CR0.NE = 0 or CR0.PE = 0 or CPL > 0 or EFLAGS.VM = 1.</p> <p>If in VMX root operation.</p> <p>If the initiating processor is not designated as the bootstrap processor via the MSR bit IA32_APIC_BASE.BSP.</p> <p>If an Intel® TXT-capable chipset is not present.</p> |

SAFER MODE EXTENSIONS REFERENCE

If an Intel® TXT-capable chipset interface to TPM is not detected as present.

If a protected partition is already active or the processor is already in authenticated code mode.

If the processor is in SMM.

If a valid uncorrectable machine check error is logged in IA32_MC[1]_STATUS.

If the authenticated code base is not on a 4096 byte boundary.

If the authenticated code size > processor's authenticated code execution area storage capacity.

If the authenticated code size is not modulo 64.

Real-Address Mode Exceptions

- #UD If CR4.SMXE = 0.
If GETSEC[SENTER] is not reported as supported by GETSEC[CAPABILITIES].
- #GP(0) GETSEC[SENTER] is not recognized in real-address mode.

Virtual-8086 Mode Exceptions

- #UD If CR4.SMXE = 0.
If GETSEC[SENTER] is not reported as supported by GETSEC[CAPABILITIES].
- #GP(0) GETSEC[SENTER] is not recognized in virtual-8086 mode.

Compatibility Mode Exceptions

All protected mode exceptions apply.

- #GP IF AC code module does not reside in physical address below $2^{32} - 1$.

64-Bit Mode Exceptions

All protected mode exceptions apply.

- #GP IF AC code module does not reside in physical address below $2^{32} - 1$.

VM-Exit Condition

- Reason (GETSEC) IF in VMX non-root operation.

GETSEC[SEXIT]—Exit Measured Environment

| Opcode | Instruction | Description |
|------------------|---------------|---------------------------|
| OF 37 (EAX=5) | GETSEC[SEXIT] | Exit measured environment |

Description

The GETSEC[SEXIT] instruction initiates an exit of a measured environment established by GETSEC[SENDER]. The SEXIT leaf of GETSEC is selected with EAX set to 5 at execution. This instruction leaf sends a message to all logical processors in the platform to signal the measured environment exit.

There are restrictions enforced by the processor for the execution of the GETSEC[SEXIT] instruction:

- Execution is not allowed unless the processor is in protected mode (CR0.PE = 1) with CPL = 0 and EFLAGS.VM = 0.
- The processor must be in a measured environment as launched by a previous GETSEC[SENDER] instruction, but not still in authenticated code execution mode.
- To avoid potential inter-operability conflicts between modes, the processor is not allowed to execute this instruction if it currently is in SMM or in VMX operation.
- To insure consistent handling of SIPI messages, the processor executing the GETSEC[SEXIT] instruction must also be designated the BSP (bootstrap processor) as defined by the register bit IA32_APIC_BASE.BSP (bit 8).

Failure to abide by the above conditions results in the processor signaling a general protection violation.

This instruction initiates a sequence to rendezvous the RLPs with the ILP. It then clears the internal processor flag indicating the processor is operating in a measured environment.

In response to a message signaling the completion of rendezvous, all RLPs restart execution with the instruction that was to be executed at the time GETSEC[SEXIT] was recognized. This applies to all processor conditions, with the following exceptions:

- If an RLP executed HLT and was in this halt state at the time of the message initiated by GETSEC[SEXIT], then execution resumes in the halt state.
- If an RLP was executing MWAIT, then a message initiated by GETSEC[SEXIT] causes an exit of the MWAIT state, falling through to the next instruction.
- If an RLP was executing an intermediate iteration of a string instruction, then the processor resumes execution of the string instruction at the point which the message initiated by GETSEC[SEXIT] was recognized.
- If an RLP is still in the SENTER sleep state (never awakened with GETSEC[WAKEUP]), it will be sent to the wait-for-SIPI state after first clearing

the bootstrap processor indicator flag (IA32_APIC_BASE.BSP) and any pending SIPI state. In this case, such RLPs are initialized to an architectural state consistent with having taken a soft reset using the INIT# pin.

Prior to completion of the GETSEC[SEXIT] operation, both the ILP and any active RLPs unmask the response of the external event signals INIT#, A20M, NMI#, and SMI#. This unmasking is performed unconditionally to recognize pin events which are masked after a GETSEC[SENTER]. The state of A20M is unmasked, as the A20M pin is not recognized while the measured environment is active.

On a successful exit of the measured environment, the ILP re-locks the Intel® TXT-capable chipset private configuration space. GETSEC[SEXIT] does not affect the content of any PCR.

At completion of GETSEC[SEXIT] by the ILP, execution proceeds to the next instruction. Since EFLAGS and the debug register state are not modified by this instruction, a pending trap condition is free to be signaled if previously enabled.

Operation in a Uni-Processor Platform

(* The state of the internal flag ACMODEFLAG and SENTERFLAG persist across instruction boundary *)

GETSEC[SEXIT] (ILP only):

```
IF (CR4.SMXE=0)
    THEN #UD;
ELSE IF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
ELSE IF (GETSEC leaf unsupported)
    THEN #UD;
ELSE IF ((in VMX root operation) or
    (CRO.PE=0) or (CPL>0) or (EFLAGS.VM=1) or
    (IA32_APIC_BASE.BSP=0) or
    (TXT chipset not present) or
    (SENTERFLAG=0) or (ACMODEFLAG=1) or (IN_SMM=1))
    THEN #GP(0);
SignalTXTMsg(SEXIT);
DO
WHILE (no SignalSEXIT message);
```

TXT_SEXIT_MSG_EVENT (ILP & RLP):

```
Mask and clear SignalSEXIT event;
Clear MONITOR FSM;
Unmask SignalSENTER event;
IF (in VMX operation)
    THEN TXT-SHUTDOWN(#IllegalEvent);
SignalTXTMsg(SEXITAck);
IF (logical processor is not ILP)
```

```

    THEN GOTO RLP_SEXIT_ROUTINE;
(* ILP waits for all logical processors to ACK *)
DO
    DONE← READ(LT.STS);
    WHILE (NOT DONE);
    SignalXTMMsg(SEXITContinue);
    SignalXTMMsg(ClosePrivate);
    SENTERFLAG← 0;
    Unmask SMI, INIT, A20M, and NMI external pin events;
END;

```

RLP_SEXIT_ROUTINE (RLPs only):

```

Wait for SignalSEXITContinue message;
Unmask SMI, INIT, A20M, and NMI external pin events;
IF (prior execution state = HLT)
    THEN reenter HLT state;
IF (prior execution state = SENTER sleep)
    THEN
        IA32_APIC_BASE.BSP← 0;
        Clear pending SIPI state;
        Call INIT_PROCESSOR_STATE;
        Unmask SIPI event;
        GOTO WAIT-FOR-SIPI;
FI;
END;

```

Flags Affected

ILP: None.

RLPs: all flags are modified for an RLP. returning to wait-for-SIPI state, none otherwise

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

#UD If CR4.SMXE = 0.

SAFER MODE EXTENSIONS REFERENCE

| | |
|--------|--|
| | If GETSEC[SEXIT] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | If CR0.PE = 0 or CPL > 0 or EFLAGS.VM = 1. If in VMX root operation. If the initiating processor is not designated as the via the MSR bit IA32_APIC_BASE.BSP. If an Intel® TXT-capable chipset is not present. If a protected partition is not already active or the processor is already in authenticated code mode. If the processor is in SMM. |

Real-Address Mode Exceptions

| | |
|--------|--|
| #UD | If CR4.SMXE = 0. If GETSEC[SEXIT] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | GETSEC[SEXIT] is not recognized in real-address mode. |

Virtual-8086 Mode Exceptions

| | |
|--------|--|
| #UD | If CR4.SMXE = 0. If GETSEC[SEXIT] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | GETSEC[SEXIT] is not recognized in virtual-8086 mode. |

Compatibility Mode Exceptions

All protected mode exceptions apply.

64-Bit Mode Exceptions

All protected mode exceptions apply.

VM-Exit Condition

Reason (GETSEC) IF in VMX non-root operation.

GETSEC[PARAMETERS]—Report the SMX Parameters

| Opcode | Instruction | Description |
|------------------|--------------------|--|
| OF 37 (EAX=6) | GETSEC[PARAMETERS] | Report the SMX Parameters The parameters index is input in EBX with the result returned in EAX, EBX, and ECX. |

Description

The GETSEC[PARAMETERS] instruction returns specific parameter information for SMX features supported by the processor. Parameter information is returned in EAX, EBX, and ECX, with the input parameter selected using EBX.

Software retrieves parameter information by searching with an input index for EBX starting at 0, and then reading the returned results in EAX, EBX, and ECX. EAX[4:0] is designated to return a parameter type field indicating if a parameter is available and what type it is. If EAX[4:0] is returned with 0, this designates a null parameter and indicates no more parameters are available.

Table 6-7 defines the parameter types supported in current and future implementations.

Table 6-7. SMX Reporting Parameters Format

| Parameter Type EAX[4:0] | Parameter Description | EAX[31:5] | EBX[31:0] | ECX[31:0] |
|-------------------------|---|----------------------------------|-------------------------|---------------------------|
| 0 | NULL | Reserved (0 returned) | Reserved (unmodified) | Reserved (unmodified) |
| 1 | Supported AC module versions | Reserved (0 returned) | version comparison mask | version numbers supported |
| 2 | Max size of authenticated code execution area | Multiply by 32 for size in bytes | Reserved (unmodified) | Reserved (unmodified) |

Table 6-7. SMX Reporting Parameters Format (Contd.)

| Parameter Type EAX[4:0] | Parameter Description | EAX[31:5] | EBX[31:0] | ECX[31:0] |
|-------------------------|--|--|-----------------------|-----------------------|
| 3 | External memory types supported during AC mode | Memory type bit mask | Reserved (unmodified) | Reserved (unmodified) |
| 4 | Selective SENTER functionality control | EAX[14:8] correspond to available SENTER function disable controls | Reserved (unmodified) | Reserved (unmodified) |
| 5-31 | Undefined | Reserved (unmodified) | Reserved (unmodified) | Reserved (unmodified) |

Supported AC module versions (as defined by the AC module HeaderVersion field) can be determined for a particular SMX capable processor by the type 1 parameter. Using EBX to index through the available parameters reported by GETSEC[PARAMETERS] for each unique parameter set returned for type 1, software can determine the complete list of AC module version(s) supported.

For each parameter set, EBX returns the comparison mask and ECX returns the available HeaderVersion field values supported, after AND'ing the target HeaderVersion with the comparison mask. Software can then determine if a particular AC module version is supported by following the pseudo-code search routine given below:

```
parameter_search_index= 0
do {
    EBX= parameter_search_index++
    EAX= 6
    GETSEC
    if (EAX[4:0] == 1) {
        if ((version_query & EBX) == ECX) {
            version_is_supported= 1
            break
        }
    }
} while (EAX[4:0] != 0)
```

If only AC modules with a HeaderVersion of 0 are supported by the processor, then only one parameter set of type 1 will be returned, as follows: EAX = 00000001H, EBX = FFFFFFFFH and ECX = 00000000H.

The maximum capacity for an authenticated code execution area supported by the processor is reported with the parameter type of 2. The maximum supported size in bytes is determined by multiplying the returned size in EAX[31:5] by 32. Thus, for a maximum supported authenticated RAM size of 32KBytes, EAX returns with 00008002H.

Supportable memory types for memory mapped outside of the authenticated code execution area are reported with the parameter type of 3. While is active, as initiated by the GETSEC functions SENTER and ENTERACCS and terminated by EXITAC, there are restrictions on what memory types are allowed for the rest of system memory. It is the responsibility of the system software to initialize the memory type range register (MTRR) MSRs and/or the page attribute table (PAT) to only map memory types consistent with the reporting of this parameter. The reporting of supportable memory types of external memory is indicated using a bit map returned in EAX[31:8]. These bit positions correspond to the memory type encodings defined for the MTRR MSR and PAT programming. See Table 6-8.

The parameter type of 4 is used for enumerating the availability of selective GETSEC[SENDER] function disable controls. If a 1 is reported in bits 14:8 of the returned parameter EAX, then this indicates a disable control capability exists with SENTER for a particular function. The enumerated field in bits 14:8 corresponds to use of the EDX input parameter bits 6:0 for SENTER. If an enumerated field bit is set to 1, then the corresponding EDX input parameter bit of EDX may be set to 1 to disable that designated function. If the enumerated field bit is 0 or this parameter is not reported, then no disable capability exists with the corresponding EDX input parameter for SENTER, and EDX bit(s) must be cleared to 0 to enable execution of SENTER. If no selective disable capability for SENTER exists as enumerated, then the corresponding bits in the IA32_FEATURE_CONTROL MSR bits 14:8 must also be programmed to 1 if the SENTER global enable bit 15 of the MSR is set. This is required to enable future extensibility of SENTER selective disable capability with respect to potentially separate software initialization of the MSR.

Table 6-8. External Memory Types Using Parameter 3

| EAX Bit Position | Parameter Description |
|------------------|-----------------------|
| 8 | Uncacheable (UC) |
| 9 | Write Combining (WC) |
| 11:10 | Reserved |
| 12 | Write-through (WT) |
| 13 | Write-protected (WP) |
| 14 | Write-back (WB) |
| 31:15 | Reserved |

If the GETSEC[PARAMETERS] leaf or specific parameter is not present for a given SMX capable processor, then default parameter values should be assumed. These are defined in Table 6-9.

Table 6-9. Default Parameter Values

| Parameter Type EAX[4:0] | Default Setting | Parameter Description |
|----------------------------|--------------------|--|
| 1 | 0.0 only | Supported AC module versions |
| 2 | 32 KBytes | Authenticated code execution area size |
| 3 | UC only | External memory types supported during AC execution mode |
| 4 | None | Available SENTER selective disable controls |

Operation

(* example of a processor supporting only a 0.0 HeaderVersion, 32K ACRAM size, memory types UC and WC *)

```
IF (CR4.SMXE=0)
    THEN #UD;
```

```
ELSE IF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
```

```
ELSE IF (GETSEC leaf unsupported)
    THEN #UD;
```

(* example of a processor supporting a 0.0 HeaderVersion *)

```
IF (EBX=0) THEN
```

```
    EAX← 00000001h;
```

```
    EBX← FFFFFFFFh;
```

```
    ECX← 00000000h;
```

```
ELSE IF (EBX=1)
```

(* example of a processor supporting a 32K ACRAM size *)

```
    THEN EAX← 00008002h;
```

```
ESE IF (EBX= 2)
```

(* example of a processor supporting external memory types of UC and WC *)

```
    THEN EAX← 00000303h;
```

```
ELSE
```

```
    EAX" 00000000h;
```

```
END;
```

Flags Affected

None.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

| | |
|-----|---|
| #UD | If CR4.SMXE = 0. If GETSEC[PARAMETERS] is not reported as supported by GETSEC[CAPABILITIES]. |
|-----|---|

Real-Address Mode Exceptions

| | |
|-----|---|
| #UD | If CR4.SMXE = 0. If GETSEC[PARAMETERS] is not reported as supported by GETSEC[CAPABILITIES]. |
|-----|---|

Virtual-8086 Mode Exceptions

| | |
|-----|---|
| #UD | If CR4.SMXE = 0. If GETSEC[PARAMETERS] is not reported as supported by GETSEC[CAPABILITIES]. |
|-----|---|

Compatibility Mode Exceptions

All protected mode exceptions apply.

64-Bit Mode Exceptions

All protected mode exceptions apply.

VM-Exit Condition

Reason (GETSEC) IF in VMX non-root operation.

GETSEC[SMCTRL]—SMX Mode Control

| Opcode | Instruction | Description |
|-----------------|----------------|---|
| OF 37 (EAX = 7) | GETSEC[SMCTRL] | <i>Perform specified SMX mode control as selected with the input EBX.</i> |

Description

The GETSEC[SMCTRL] instruction is available for performing certain SMX specific mode control operations. The operation to be performed is selected through the input register EBX. Currently only an input value in EBX of 0 is supported. All other EBX settings will result in the signaling of a general protection violation.

If EBX is set to 0, then the SMCTRL leaf is used to re-enable SMI events. SMI is masked by the ILP executing the GETSEC[SENDER] instruction (SMI is also masked in the responding logical processors in response to SENTER rendezvous messages.). The determination of when this instruction is allowed and the events that are unmasked is dependent on the processor context (See Table 6-10). For brevity, the usage of SMCTRL where EBX=0 will be referred to as GETSEC[SMCTRL(0)].

As part of support for launching a measured environment, the SMI, NMI and INIT events are masked after GETSEC[SENDER], and remain masked after exiting authenticated execution mode. Unmasking these events should be accompanied by securely enabling these event handlers. These security concerns can be addressed in VMX operation by a MVMM.

The VM monitor can choose two approaches:

- In a dual monitor approach, the executive software will set up an SMM monitor in parallel to the executive VMM (i.e. the MVMM), see Chapter 26, “System Management” of *Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 3B*. The SMM monitor is dedicated to handling SMI events without compromising the security of the MVMM. This usage model of handling SMI while a measured environment is active does not require the use of GETSEC[SMCTRL(0)] as event re-enabling after the VMX environment launch is handled implicitly and through separate VMX based controls.
- If a dedicated SMM monitor will not be established and SMIs are to be handled within the measured environment, then GETSEC[SMCTRL(0)] can be used by the executive software to re-enable SMI that has been masked as a result of SENTER.

Table 6-10 defines the processor context in which GETSEC[SMCTRL(0)] can be used and which events will be unmasked. Note that the events that are unmasked are dependent upon the currently operating processor context.

Table 6-10. Supported Actions for GETSEC[SMCTRL(0)]

| ILP Mode of Operation | SMCTRL execution action |
|---|---|
| In VMX non-root operation | VM exit |
| SENTERFLAG = 0 | #GP(0), illegal context |
| In authenticated code execution mode (ACMODEFLAG = 1) | #GP(0), illegal context |
| SENTERFLAG = 1, not in VMX operation, not in SMM | Unmask SMI |
| SENTERFLAG = 1, in VMX root operation, not in SMM | Unmask SMI if SMM monitor is not configured, otherwise #GP(0) |
| SENTERFLAG = 1, In VMX root operation, in SMM | #GP(0), illegal context |

Operation

(* The state of the internal flag ACMODEFLAG and SENTERFLAG persist across instruction boundary *)

```

IF (CR4.SMXE=0)
    THEN #UD;
ELSE IF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
ELSE IF (GETSEC leaf unsupported)
    THEN #UD;
ELSE IF ((CR0.PE=0) or (CPL>0) OR (EFLAGS.VM=1))
    THEN #GP(0);
ELSE IF ((EBX=0) and (SENTERFLAG=1) and (ACMODEFLAG=0) and (IN_SMM=0) and
    (((in VMX root operation) and (SMM monitor not configured)) or (not in VMX operation)))
    THEN unmask SMI;
ELSE
    #GP(0);
END

```

Flags Affected

None.

Use of Prefixes

LOCK Causes #UD

SAFER MODE EXTENSIONS REFERENCE

| | |
|-------------------|---|
| REP* | Cause #UD (includes REPNE/REPZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |
| REX | Ignored |

Protected Mode Exceptions

| | |
|--------|--|
| #UD | If CR4.SMXE = 0. If GETSEC[SMCTRL] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | If CR0.PE = 0 or CPL > 0 or EFLAGS.VM = 1. If in VMX root operation. If a protected partition is not already active or the processor is currently in authenticated code mode. If the processor is in SMM. If the SMM monitor is not configured |

Real-Address Mode Exceptions

| | |
|--------|---|
| #UD | If CR4.SMXE = 0. If GETSEC[SMCTRL] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | GETSEC[SMCTRL] is not recognized in real-address mode. |

Virtual-8086 Mode Exceptions

| | |
|--------|---|
| #UD | If CR4.SMXE = 0. If GETSEC[SMCTRL] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | GETSEC[SMCTRL] is not recognized in virtual-8086 mode. |

Compatibility Mode Exceptions

All protected mode exceptions apply.

64-Bit Mode Exceptions

All protected mode exceptions apply.

VM-exit Condition

Reason (GETSEC) IF in VMX non-root operation.

GETSEC[WAKEUP]—Wake up sleeping processors in measured environment

| Opcode | Instruction | Description |
|------------------|--------------------|--|
| 0F 37 (EAX=8) | GETSEC[WAKE UP] | Wake up the responding logical processors from the SENTER sleep state. |

Description

The GETSEC[WAKEUP] leaf function broadcasts a wake-up message to all logical processors currently in the SENTER sleep state. Responding logical processors (RLPs) enter the SENTER sleep state after completion of the SENTER rendezvous sequence.

The GETSEC[WAKEUP] instruction may only be executed:

- In a measured environment as initiated by execution of GETSEC[SENDER].
- Outside of authenticated code execution mode.
- Execution is not allowed unless the processor is in protected mode with CPL = 0 and EFLAGS.VM = 0.
- In addition, the logical processor must be designated as the boot-strap processor as configured by setting IA32_APIC_BASE.BSP = 1.

If these conditions are not met, attempts to execute GETSEC[WAKEUP] result in a general protection violation.

An RLP exits the SENTER sleep state and start execution in response to a WAKEUP signal initiated by ILP's execution of GETSEC[WAKEUP]. The RLP retrieves a pointer to a data structure that contains information to enable execution from a defined entry point. This data structure is located using a physical address held in the Intel® TXT-capable chipset configuration register LT.MLE.JOIN. The register is publicly writable in the chipset by all processors and is not restricted by the Intel® TXT-capable chipset configuration register lock status. The format of this data structure is defined in Table 6-11.

Table 6-11. RLP MVMM JOIN Data Structure

| Offset | Field |
|--------|------------------------------|
| 0 | GDT limit |
| 4 | GDT base pointer |
| 8 | Segment selector initializer |
| 12 | EIP |

The MLE JOIN data structure contains the information necessary to initialize RLP processor state and permit the processor to join the measured environment. The GDTR, LIP, and CS, DS, SS, and ES selector values are initialized using this data structure. The CS selector index is derived directly from the segment selector initializer field; DS, SS, and ES selectors are initialized to CS+8. The segment descriptor fields are initialized implicitly with BASE = 0, LIMIT = FFFFFH, G = 1, D = 1, P = 1, S = 1; read/write/access for DS, SS, and ES; and execute/read/access for CS. It is the responsibility of external software to establish a GDT pointed to by the MLE JOIN data structure that contains descriptor entries consistent with the implicit settings initialized by the processor (see Table 6-6). Certain states from the content of Table 6-11 are checked for consistency by the processor prior to execution. A failure of any consistency check results in the RLP aborting entry into the protected environment and signaling an Intel® TXT shutdown condition. The specific checks performed are documented later in this section. After successful completion of processor consistency checks and subsequent initialization, RLP execution in the measured environment begins from the entry point at offset 12 (as indicated in Table 6-11).

Operation

(* The state of the internal flag ACMODEFLAG and SENTERFLAG persist across instruction boundary *)

```
IF (CR4.SMXE=0)
    THEN #UD;
ELSE IF (in VMX non-root operation)
    THEN VM Exit (reason="GETSEC instruction");
ELSE IF (GETSEC leaf unsupported)
    THEN #UD;
ELSE IF ((CR0.PE=0) or (CPL>0) or (EFLAGS.VM=1) or (SENTERFLAG=0) or (ACMODEFLAG=1) or
(IN_SMM=0) or (in VMX operation) or (IA32_APIC_BASE.BSP=0) or (TXT chipset not present))
    THEN #GP(0);
ELSE
    SignalTXTMsg(WAKEUP);
END;
```

RLP_SIPI_WAKEUP_FROM_SENTER_ROUTINE: (RLP only)

```
WHILE (no SignalWAKEUP event);
Mask SMI, A20M, and NMI external pin events (unmask INIT);
Mask SignalWAKEUP event;
Invalidate processor TLB(s);
Drain outgoing transactions;
TempGDTRLIMIT← LOAD(LT.MLE.JOIN);
TempGDTRBASE← LOAD(LT.MLE.JOIN+4);
TempSegSel← LOAD(LT.MLE.JOIN+8);
TempEIP← LOAD(LT.MLE.JOIN+12);
```

```

IF (TempGDTLimit & FFFF0000h)
    THEN TXT-SHUTDOWN(#BadJOINFormat);
IF ((TempSegSel > TempGDTRLIMIT-15) or (TempSegSel < 8))
    THEN TXT-SHUTDOWN(#BadJOINFormat);
IF ((TempSegSel.TI=1) or (TempSegSel.RPLI=0))
    THEN TXT-SHUTDOWN(#BadJOINFormat);
CR0.[PG,CD,W,AM,WP]← 0;
CR0.[NE,PE]← 1;
CR4← 00004000h;
EFLAGS← 00000002h;
IA32_EFER← 0;
GDTR.BASE← TempGDTRBASE;
GDTR.LIMIT← TempGDTRLIMIT;
CS.SEL← TempSegSel;
CS.BASE← 0;
CS.LIMIT← FFFFFh;
CS.G← 1;
CS.D← 1;
CS.AR← 9Bh;
DS.SEL← TempSegSel+8;
DS.BASE← 0;
DS.LIMIT← FFFFFh;
DS.G← 1;
DS.D← 1;
DS.AR← 93h;
SS← DS;
ES← DS;
DR7← 00000400h;
IA32_DEBUGCTL← 0;
DR6.BS← 0;
EIP← TempEIP;
END;

```

Flags Affected

None.

Use of Prefixes

| | |
|-------------------|--|
| LOCK | Causes #UD |
| REP* | Cause #UD (includes REPNE/REPNZ and REP/REPE/REPZ) |
| Operand size | Causes #UD |
| Segment overrides | Ignored |
| Address size | Ignored |

SAFER MODE EXTENSIONS REFERENCE

REX Ignored

Protected Mode Exceptions

| | |
|--------|---|
| #UD | If CR4.SMXE = 0. If GETSEC[WAKEUP] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | If CR0.PE = 0 or CPL > 0 or EFLAGS.VM = 1. If in VMX operation. If a protected partition is not already active or the processor is currently in authenticated code mode. If the processor is in SMM. |
| #UD | If CR4.SMXE = 0. If GETSEC[WAKEUP] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | GETSEC[WAKEUP] is not recognized in real-address mode. |

Virtual-8086 Mode Exceptions

| | |
|--------|---|
| #UD | If CR4.SMXE = 0. If GETSEC[WAKEUP] is not reported as supported by GETSEC[CAPABILITIES]. |
| #GP(0) | GETSEC[WAKEUP] is not recognized in virtual-8086 mode. |

Compatibility Mode Exceptions

All protected mode exceptions apply.

64-Bit Mode Exceptions

All protected mode exceptions apply.

VM-exit Condition

Reason (GETSEC) IF in VMX non-root operation.

Use the opcode tables in this chapter to interpret IA-32 and intel 64 architecture object code. Instructions are divided into encoding groups:

- 1-byte, 2-byte and 3-byte opcode encodings are used to encode integer, system, MMX technology, SSE/SSE2/SSE3/SSSE3, and VMX instructions. Maps for these instructions are given in Table A-2 through Table A-6.
- Escape opcodes (in the format: ESC character, opcode, ModR/M byte) are used for floating-point instructions. The maps for these instructions are provided in Table A-7 through Table A-22.

NOTE

All blanks in opcode maps are reserved and must not be used. Do not depend on the operation of undefined or blank opcodes.

A.1 USING OPCODE TABLES

Tables in this appendix list opcodes of instructions (including required instruction prefixes, opcode extensions in associated ModR/M byte). Blank cells in the tables indicate opcodes that are reserved or undefined.

The opcode map tables are organized by hex values of the upper and lower 4 bits of an opcode byte. For 1-byte encodings (Table A-2), use the four high-order bits of an opcode to index a row of the opcode table; use the four low-order bits to index a column of the table. For 2-byte opcodes beginning with 0FH (Table A-3), skip any instruction prefixes, the 0FH byte (0FH may be preceded by 66H, F2H, or F3H) and use the upper and lower 4-bit values of the next opcode byte to index table rows and columns. Similarly, for 3-byte opcodes beginning with 0F38H or 0F3AH (Table A-4), skip any instruction prefixes, 0F38H or 0F3AH and use the upper and lower 4-bit values of the third opcode byte to index table rows and columns. See Section A.2.4, “Opcode Look-up Examples for One, Two, and Three-Byte Opcodes.”

When a ModR/M byte provides opcode extensions, this information qualifies opcode execution. For information on how an opcode extension in the ModR/M byte modifies the opcode map in Table A-2 and Table A-3, see Section A.4.

The escape (ESC) opcode tables for floating point instructions identify the eight high order bits of opcodes at the top of each page. See Section A.5. If the accompanying ModR/M byte is in the range of 00H-BFH, bits 3-5 (the top row of the third table on each page) along with the reg bits of ModR/M determine the opcode. ModR/M bytes

outside the range of 00H-BFH are mapped by the bottom two tables on each page of the section.

A.2 KEY TO ABBREVIATIONS

Operands are identified by a two-character code of the form Zz. The first character, an uppercase letter, specifies the addressing method; the second character, a lower-case letter, specifies the type of operand.

A.2.1 Codes for Addressing Method

The following abbreviations are used to document addressing methods:

- A Direct address: the instruction has no ModR/M byte; the address of the operand is encoded in the instruction. No base register, index register, or scaling factor can be applied (for example, far JMP (EA)).
- C The reg field of the ModR/M byte selects a control register (for example, MOV (0F20, 0F22)).
- D The reg field of the ModR/M byte selects a debug register (for example, MOV (0F21,0F23)).
- E A ModR/M byte follows the opcode and specifies the operand. The operand is either a general-purpose register or a memory address. If it is a memory address, the address is computed from a segment register and any of the following values: a base register, an index register, a scaling factor, a displacement.
- F EFLAGS/RFLAGS Register.
- G The reg field of the ModR/M byte selects a general register (for example, AX (000)).
- I Immediate data: the operand value is encoded in subsequent bytes of the instruction.
- J The instruction contains a relative offset to be added to the instruction pointer register (for example, JMP (0E9), LOOP).
- M The ModR/M byte may refer only to memory (for example, BOUND, LES, LDS, LSS, LFS, LGS, CMPXCHG8B).
- N The R/M field of the ModR/M byte selects a packed-quadword, MMX technology register.
- O The instruction has no ModR/M byte. The offset of the operand is coded as a word or double word (depending on address size attribute) in the instruction. No base register, index register, or scaling factor can be applied (for example, MOV (A0–A3)).

- P The reg field of the ModR/M byte selects a packed quadword MMX technology register.
- Q A ModR/M byte follows the opcode and specifies the operand. The operand is either an MMX technology register or a memory address. If it is a memory address, the address is computed from a segment register and any of the following values: a base register, an index register, a scaling factor, and a displacement.
- R The R/M field of the ModR/M byte may refer only to a general register (for example, MOV (0F20-0F23)).
- S The reg field of the ModR/M byte selects a segment register (for example, MOV (8C,8E)).
- U The R/M field of the ModR/M byte selects a 128-bit XMM register.
- V The reg field of the ModR/M byte selects a 128-bit XMM register.
- W A ModR/M byte follows the opcode and specifies the operand. The operand is either a 128-bit XMM register or a memory address. If it is a memory address, the address is computed from a segment register and any of the following values: a base register, an index register, a scaling factor, and a displacement.
- X Memory addressed by the DS:rSI register pair (for example, MOVS, CMPS, OUTS, or LODS).
- Y Memory addressed by the ES:rDI register pair (for example, MOVS, CMPS, INS, STOS, or SCAS).

A.2.2 Codes for Operand Type

The following abbreviations are used to document operand types:

- a Two one-word operands in memory or two double-word operands in memory, depending on operand-size attribute (used only by the BOUND instruction).
- b Byte, regardless of operand-size attribute.
- c Byte or word, depending on operand-size attribute.
- d Doubleword, regardless of operand-size attribute.
- dq Double-quadword, regardless of operand-size attribute.
- p 32-bit, 48-bit, or 80-bit pointer, depending on operand-size attribute.
- pd 128-bit packed double-precision floating-point data.
- pi Quadword MMX technology register (for example: mm0).
- ps 128-bit packed single-precision floating-point data.
- q Quadword, regardless of operand-size attribute.
- s 6-byte or 10-byte pseudo-descriptor.
- ss Scalar element of a 128-bit packed single-precision floating data.

OPCODE MAP

| | |
|----|---|
| si | Doubleword integer register (for example: <code>eax</code>). |
| v | Word, doubleword or quadword (in 64-bit mode), depending on operand-size attribute. |
| w | Word, regardless of operand-size attribute. |
| z | Word for 16-bit operand-size or doubleword for 32 or 64-bit operand-size. |

A.2.3 Register Codes

When an opcode requires a specific register as an operand, the register is identified by name (for example, `AX`, `CL`, or `ESI`). The name indicates whether the register is 64, 32, 16, or 8 bits wide.

A register identifier of the form `eXX` or `rXX` is used when register width depends on the operand-size attribute. `eXX` is used when 16 or 32-bit sizes are possible; `rXX` is used when 16, 32, or 64-bit sizes are possible. For example: `eAX` indicates that the `AX` register is used when the operand-size attribute is 16 and the `EAX` register is used when the operand-size attribute is 32. `rAX` can indicate `AX`, `EAX` or `RAX`.

When the `REX.B` bit is used to modify the register specified in the `reg` field of the opcode, this fact is indicated by adding `/x` to the register name to indicate the additional possibility. For example, `rCX/r9` is used to indicate that the register could either be `rCX` or `r9`. Note that the size of `r9` in this case is determined by the operand size attribute (just as for `rCX`).

A.2.4 Opcode Look-up Examples for One, Two, and Three-Byte Opcodes

This section provides examples that demonstrate how opcode maps are used.

A.2.4.1 One-Byte Opcode Instructions

The opcode map for 1-byte opcodes is shown in Table A-2. The opcode map for 1-byte opcodes is arranged by row (the least-significant 4 bits of the hexadecimal value) and column (the most-significant 4 bits of the hexadecimal value). Each entry in the table lists one of the following types of opcodes:

- Instruction mnemonics and operand types using the notations listed in Section A.2
- Opcodes used as an instruction prefix

For each entry in the opcode map that corresponds to an instruction, the rules for interpreting the byte following the primary opcode fall into one of the following cases:

- A `ModR/M` byte is required and is interpreted according to the abbreviations listed in Section A.1 and Chapter 2, "Instruction Format," of the *Intel® 64 and IA-32*

Architectures Software Developer's Manual, Volume 2A. Operand types are listed according to notations listed in Section A.2.

- A ModR/M byte is required and includes an opcode extension in the reg field in the ModR/M byte. Use Table A-6 when interpreting the ModR/M byte.
- Use of the ModR/M byte is reserved or undefined. This applies to entries that represent an instruction prefix or entries for instructions without operands that use ModR/M (for example: 60H, PUSHA; 06H, PUSH ES).

Example A-1. Look-up Example for 1-Byte Opcodes

Opcode 030500000000H for an ADD instruction is interpreted using the 1-byte opcode map (Table A-2) as follows:

- The first digit (0) of the opcode indicates the table row and the second digit (3) indicates the table column. This locates an opcode for ADD with two operands.
- The first operand (type Gv) indicates a general register that is a word or doubleword depending on the operand-size attribute. The second operand (type Ev) indicates a ModR/M byte follows that specifies whether the operand is a word or doubleword general-purpose register or a memory address.
- The ModR/M byte for this instruction is 05H, indicating that a 32-bit displacement follows (00000000H). The reg/opcode portion of the ModR/M byte (bits 3-5) is 000, indicating the EAX register.

The instruction for this opcode is ADD EAX, mem_op, and the offset of mem_op is 00000000H.

Some 1- and 2-byte opcodes point to group numbers (shaded entries in the opcode map table). Group numbers indicate that the instruction uses the reg/opcode bits in the ModR/M byte as an opcode extension (refer to Section A.4).

A.2.4.2 Two-Byte Opcode Instructions

The two-byte opcode map shown in Table A-3 includes primary opcodes that are either two bytes or three bytes in length. Primary opcodes that are 2 bytes in length begin with an escape opcode 0FH. The upper and lower four bits of the second opcode byte are used to index a particular row and column in Table A-3.

Two-byte opcodes that are 3 bytes in length begin with a mandatory prefix (66H, F2H, or F3H) and the escape opcode (0FH). The upper and lower four bits of the third byte are used to index a particular row and column in Table A-3 (except when the second opcode byte is the 3-byte escape opcodes 38H or 3AH; in this situation refer to Section A.2.4.3).

For each entry in the opcode map, the rules for interpreting the byte following the primary opcode fall into one of the following cases:

- A ModR/M byte is required and is interpreted according to the abbreviations listed in Section A.1 and Chapter 2, "Instruction Format," of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A*. The operand types are listed according to notations listed in Section A.2.

OPCODE MAP

- A ModR/M byte is required and includes an opcode extension in the reg field in the ModR/M byte. Use Table A-6 when interpreting the ModR/M byte.
- Use of the ModR/M byte is reserved or undefined. This applies to entries that represent an instruction without operands that are encoded using ModR/M (for example: 0F77H, EMMS).

Example A-2. Look-up Example for 2-Byte Opcodes

Look-up opcode 0FA405000000003H for a SHLD instruction using Table A-3.

- The opcode is located in row A, column 4. The location indicates a SHLD instruction with operands Ev, Gv, and Ib. Interpret the operands as follows:
 - Ev: The ModR/M byte follows the opcode to specify a word or doubleword operand.
 - Gv: The reg field of the ModR/M byte selects a general-purpose register.
 - Ib: Immediate data is encoded in the subsequent byte of the instruction.
- The third byte is the ModR/M byte (05H). The mod and opcode/reg fields of ModR/M indicate that a 32-bit displacement is used to locate the first operand in memory and eAX as the second operand.
- The next part of the opcode is the 32-bit displacement for the destination memory operand (00000000H). The last byte stores immediate byte that provides the count of the shift (03H).
- By this breakdown, it has been shown that this opcode represents the instruction: SHLD DS:00000000H, EAX, 3.

A.2.4.3 Three-Byte Opcode Instructions

The three-byte opcode maps shown in Table A-4 and Table A-5 includes primary opcodes that are either 3 or 4 bytes in length. Primary opcodes that are 3 bytes in length begin with two escape bytes 0F38H or 0F3A. The upper and lower four bits of the third opcode byte are used to index a particular row and column in Table A-4 or Table A-5.

Three-byte opcodes that are 4 bytes in length begin with a mandatory prefix (66H, F2H, or F3H) and two escape bytes (0F38H or 0F3AH). The upper and lower four bits of the fourth byte are used to index a particular row and column in Table A-4 or Table A-5.

For each entry in the opcode map, the rules for interpreting the byte following the primary opcode fall into the following case:

- A ModR/M byte is required and is interpreted according to the abbreviations listed in A.1 and Chapter 2, "Instruction Format," of the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A*. The operand types are listed according to notations listed in Section A.2.

Example A-3. Look-up Example for 3-Byte Opcodes

Look-up opcode 660F3A0FC108H for a PALIGNR instruction using Table A-5.

- 66H is a prefix and 0F3AH indicate to use Table A-5. The opcode is located in row 0, column F indicating a PALIGNR instruction with operands Vdq, Wdq, and Ib. Interpret the operands as follows:
 - Vdq: The reg field of the ModR/M byte selects a 128-bit XMM register.
 - Wdq: The R/M field of the ModR/M byte selects either a 128-bit XMM register or memory location.
 - Ib: Immediate data is encoded in the subsequent byte of the instruction.
- The next byte is the ModR/M byte (C1H). The reg field indicates that the first operand is XMM0. The mod shows that the R/M field specifies a register and the R/M indicates that the second operand is XMM1.
- The last byte is the immediate byte (08H).
- By this breakdown, it has been shown that this opcode represents the instruction: PALIGNR XMM0, XMM1, 8.

A.2.5 Superscripts Utilized in Opcode Tables

Table A-1 contains notes on particular encodings. These notes are indicated in the following opcode maps by superscripts. Gray cells indicate instruction groupings.

Table A-1. Superscripts Utilized in Opcode Tables

| Superscript Symbol | Meaning of Symbol |
|--------------------|--|
| 1A | Bits 5, 4, and 3 of ModR/M byte used as an opcode extension (refer to Section A.4, "Opcode Extensions For One-Byte And Two-byte Opcodes"). |
| 1B | Use the 0F0B opcode (UD2 instruction) or the 0FB9H opcode when deliberately trying to generate an invalid opcode exception (#UD). |
| 1C | Some instructions added in the Pentium III processor may use the same two-byte opcode. If the instruction has variations, or the opcode represents different instructions, the ModR/M byte will be used to differentiate the instruction. For the value of the ModR/M byte needed to decode the instruction, see Table A-6. These instructions include SFENCE, STMXCSR, LDMXCSR, FXRSTOR, and FXSAVE, as well as PREFETCH and its variations. |
| i64 | The instruction is invalid or not encodable in 64-bit mode. 40 through 4F (single-byte INC and DEC) are REX prefix combinations when in 64-bit mode (use FE/FF Grp 4 and 5 for INC and DEC). |
| o64 | Instruction is only available when in 64-bit mode. |
| d64 | When in 64-bit mode, instruction defaults to 64-bit operand size and cannot encode 32-bit operand size. |

Table A-1. Superscripts Utilized in Opcode Tables

| Superscript Symbol | Meaning of Symbol |
|---------------------------|--|
| f64 | The operand size is forced to a 64-bit operand size when in 64-bit mode (prefixes that change operand size are ignored for this instruction in 64-bit mode). |

A.3 ONE, TWO, AND THREE-BYTE OPCODE MAPS

See Table A-2 through Table A-5 below. The tables are multiple page presentations. Rows and columns with sequential relationships are placed on facing pages to make look-up tasks easier. Note that table footnotes are not presented on each page. Table footnotes for each table are presented on the last page of the table.

This page intentionally left blank

Table A-2. One-byte Opcode Map: (00H — F7H) *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|--------------------------------|---|------------------------------|------------------------------|----------------------------|-----------------------|
| 0 | ADD | | | | | | PUSH ES ¹⁶⁴ | POP ES ¹⁶⁴ |
| | Eb, Gb | Ev, Gv | Gb, Eb | Gv, Ev | AL, lb | rAX, lz | | |
| 1 | ADC | | | | | | PUSH SS ¹⁶⁴ | POP SS ¹⁶⁴ |
| | Eb, Gb | Ev, Gv | Gb, Eb | Gv, Ev | AL, lb | rAX, lz | | |
| 2 | AND | | | | | | SEG=ES (Prefix) | DAA ¹⁶⁴ |
| | Eb, Gb | Ev, Gv | Gb, Eb | Gv, Ev | AL, lb | rAX, lz | | |
| 3 | XOR | | | | | | SEG=SS (Prefix) | AAA ¹⁶⁴ |
| | Eb, Gb | Ev, Gv | Gb, Eb | Gv, Ev | AL, lb | rAX, lz | | |
| 4 | INC ¹⁶⁴ general register / REX ¹⁶⁴ Prefixes | | | | | | | |
| | eAX REX | eCX REX.B | eDX REX.X | eBX REX.XB | eSP REX.R | eBP REX.RB | eSI REX.RX | eDI REX.RXB |
| 5 | PUSH ¹⁶⁴ general register | | | | | | | |
| | rAX/r8 | rCX/r9 | rDX/r10 | rBX/r11 | rSP/r12 | rBP/r13 | rSI/r14 | rDI/r15 |
| 6 | PUSHA ¹⁶⁴ / PUSHAD ¹⁶⁴ | POPA ¹⁶⁴ / POPAD ¹⁶⁴ | BOUND ¹⁶⁴ Gv, Ma | ARPL ¹⁶⁴ Ew, Gw MOVSD ¹⁶⁴ Gv, Ev | SEG=FS (Prefix) | SEG=GS (Prefix) | Operand Size (Prefix) | Address Size (Prefix) |
| 7 | Jcc ¹⁶⁴ , Jb - Short-displacement jump on condition | | | | | | | |
| | O | NO | B/NAE/C | NB/AE/NC | Z/E | NZ/NE | BE/NA | NBE/A |
| 8 | Immediate Grp 1 ^{1A} | | | | TEST | | XCHG | |
| | Eb, lb | Ev, lz | Eb, lb ¹⁶⁴ | Ev, lb | Eb, Gb | Ev, Gv | Eb, Gb | Ev, Gv |
| 9 | NOP PAUSE(F3) XCHG r8, rAX | XCHG word, double-word or quad-word register with rAX | | | | | | |
| | | rCX/r9 | rDX/r10 | rBX/r11 | rSP/r12 | rBP/r13 | rSI/r14 | rDI/r15 |
| A | MOV | | | | MOVS/B Xb, Yb | MOVS/W/D/Q Xv, Yv | CMPS/B Xb, Yb | CMPS/W/D Xv, Yv |
| | AL, Ob | rAX, Ov | Ob, AL | Ov, rAX | | | | |
| B | MOV immediate byte into byte register | | | | | | | |
| | AL/R8L, lb | CL/R9L, lb | DL/R10L, lb | BL/R11L, lb | AH/R12L, lb | CH/R13L, lb | DH/R14L, lb | BH/R15L, lb |
| C | Shift Grp 2 ^{1A} | | RETN ¹⁶⁴ lw | RETN ¹⁶⁴ | LES ¹⁶⁴ Gz, Mp | LDS ¹⁶⁴ Gz, Mp | Grp 11 ^{1A} - MOV | |
| | Eb, lb | Ev, lb | | | | | Eb, lb | Ev, lz |
| D | Shift Grp 2 ^{1A} | | | | AAM ¹⁶⁴ lb | AAD ¹⁶⁴ lb | | XLAT/ XLATB |
| | Eb, 1 | Ev, 1 | Eb, CL | Ev, CL | | | | |
| E | LOOPNE ¹⁶⁴ / LOOPNZ ¹⁶⁴ Jb | LOOPE ¹⁶⁴ / LOOPZ ¹⁶⁴ Jb | LOOP ¹⁶⁴ Jb | JrCXZ ¹⁶⁴ / Jb | IN | | OUT | |
| | | | | | AL, lb | eAX, lb | lb, AL | lb, eAX |
| F | LOCK (Prefix) | | REPNE (Prefix) | REP/ REPE (Prefix) | HLT | CMC | Unary Grp 3 ^{1A} | |
| | | | | | | | Eb | Ev |

Table A-2. One-byte Opcode Map: (08H – FFH) *

| | 8 | 9 | A | B | C | D | E | F | |
|---|--|-----------------------|--------------------------|------------------------|----------------------------|---------------------------|-----------------------------|---|--|
| 0 | OR Eb, Gb Ev, Gv Gb, Eb Gv, Ev AL, lb rAX, lz | | | | | | PUSH CS ⁶⁴ | 2-byte escape (Table A-3) | |
| 1 | SBB Eb, Gb Ev, Gv Gb, Eb Gv, Ev AL, lb rAX, lz | | | | | | PUSH DS ⁶⁴ | POP DS ⁶⁴ | |
| 2 | SUB Eb, Gb Ev, Gv Gb, Eb Gv, Ev AL, lb rAX, lz | | | | | | SEG=CS (Prefix) | DAS ⁶⁴ | |
| 3 | CMP Eb, Gb Ev, Gv Gb, Eb Gv, Ev AL, lb rAX, lz | | | | | | SEG=DS (Prefix) | AAS ⁶⁴ | |
| 4 | DEC ⁶⁴ general register / REX ⁶⁴ Prefixes | | | | | | | | |
| | eAX REX.W | eCX REX.WB | eDX REX.WX | eBX REX.WXB | eSP REX.WR | eBP REX.WRB | eSI REX.WRX | eDI REX.WRXB | |
| 5 | POP ⁶⁴ into general register | | | | | | | | |
| | rAX/r8 | rCX/r9 | rDX/r10 | rBX/r11 | rSP/r12 | rBP/r13 | rSI/r14 | rDI/r15 | |
| 6 | PUSH ⁶⁴ lz | IMUL Gv, Ev, lz | PUSH ⁶⁴ lb | IMUL Gv, Ev, lb | INS/INSB Yb, DX | INS/INSW/INSD Yz, DX | OUTS/OUTSB DX, Xb | OUTS/OUTSW/OUTSD DX, Xz | |
| 7 | Jcc ⁶⁴ , Jb- Short displacement jump on condition | | | | | | | | |
| | S | NS | P/PE | NP/PO | L/NGE | NL/GE | LE/NG | NLE/G | |
| 8 | MOV Eb, Gb Ev, Gv Gb, Eb Gv, Ev | | | | MOV Ev, Sw | LEA Gv, M | MOV Sw, Ew | Grp 1A ^{1A} POP ⁶⁴ Ev | |
| 9 | CBW/CWDE/CDQE | CWD/CDQ/CQO | CALLF ⁶⁴ Ap | FWAIT/WAIT | PUSHF/D/Q ⁶⁴ Fv | POPF/D/Q ⁶⁴ Fv | SAHF | LAHF | |
| A | TEST AL, lb rAX, lz | | STOS/B Yb, AL | STOS/W/D/Q Yv, rAX | LODS/B AL, Xb | LODS/W/D/Q rAX, Xv | SCAS/B AL, Yb | SCAS/W/D/Q rAX, Xv | |
| B | MOV immediate word or double into word, double, or quad register | | | | | | | | |
| | rAX/r8, lv | rCX/r9, lv | rDX/r10, lv | rBX/r11, lv | rSP/r12, lv | rBP/r13, lv | rSI/r14, lv | rDI/r15, lv | |
| C | ENTER lw, lb | LEAVE ⁶⁴ | RETF lw | RETF | INT 3 | INT lb | INTO ⁶⁴ | IRET/D/Q | |
| D | ESC (Escape to coprocessor instruction set) | | | | | | | | |
| E | CALL ⁶⁴ Jz | near ⁶⁴ Jz | JMP far ⁶⁴ AP | short ⁶⁴ Jb | IN AL, DX eAX, DX | | OUT DX, AL DX, eAX | | |
| F | CLC | STC | CLI | STI | CLD | STD | INC/DEC Grp 4 ^{1A} | INC/DEC Grp 5 ^{1A} | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-3. Two-byte Opcode Map: 00H — 77H (First Byte is 0FH) *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|--|---|
| 0 | Grp 6 ^{1A} | Grp 7 ^{1A} | LAR Gv, Ew | LSL Gv, Ew | | SYSCALL ⁰⁶⁴ | CLTS | SYSRET ⁰⁶⁴ |
| 1 | movups Vps, Wps movss (F3) Vss, Wss movupd (66) Vpd, Wpd movsd (F2) Vsd, Wsd | movups Wps, Vps movss (F3) Wss, Vss movupd (66) Wpd, Vpd movsd (F2) Wsd, Vsd | movlps Vq, Mq movlpd (66) Vq, Mq movhlps Vq, Uq movddup(F2) Vq, Wq movsldup(F3) Vq, Wq | movlps Mq, Vq movlpd (66) Mq, Vq | unpcklps Vps, Wq unpcklpd (66) Vpd, Wq | unpckhps Vps, Wq unpckhpd (66) Vpd, Wq | movhps Vq, Mq movhpd (66) Vq, Mq movlhps Vq, Uq movshdup(F3) Vq, Wq | movhps Mq, Vq movhpd(66) Mq, Vq |
| 2 | MOV Rd, Cd | MOV Rd, Dd | MOV Cd, Rd | MOV Dd, Rd | | | | |
| 3 | WRMSR | RDTSC | RDMSR | RDPMC | SYSENTER | SYSEXIT | | GETSEC |
| 4 | CMOVcc, (Gv, Ev) - Conditional Move | | | | | | | |
| | O | NO | B/C/NAE | AE/NB/NC | E/Z | NE/NZ | BE/NA | A/NBE |
| 5 | movmskps Gd/q, Ups movmskpd (66)Gd/q, Upd | sqrtps Vps, Wps sqrtps (F3) Vss, Wss sqrtpd (66) Vpd, Wpd sqrtsd (F2) Vsd, Wsd | rsqrtps Vps, Wps rsqrtps (F3) Vss, Wss | rcpps Vps, Wps rcpps (F3) Vss, Wss | andps Vps, Wps andpd (66) Vpd, Wpd | andnps Vps, Wps andnpd (66) Vpd, Wpd | orps Vps, Wps orpd (66) Vpd, Wpd | xorps Vps, Wps xorpd (66) Vpd, Wpd |
| 6 | punpcklbw Pq, Qd punpcklbw (66) Vdq, Wdq | punpcklwd Pq, Qd punpcklwd (66) Vdq, Wdq | punpckldq Pq, Qd punpckldq (66) Vdq, Wdq | packsswb Pq, Qq packsswb (66) Vdq, Wdq | pcmpgtb Pq, Qq pcmpgtb (66) Vdq, Wdq | pcmpgtw Pq, Qq pcmpgtw (66) Vdq, Wdq | pcmpgtd Pq, Qq pcmpgtd (66) Vdq, Wdq | packuswb Pq, Qq packuswb (66) Vdq, Wdq |
| 7 | pshufw Pq, Qq, Ib pshufd (66) Vdq, Wdq, Ib pshufhw(F3) Vdq, Wdq, Ib pshufw (F2) Vdq, Wdq, Ib | (Grp 12 ^{1A}) | (Grp 13 ^{1A}) | (Grp 14 ^{1A}) | pcmpeqb Pq, Qq pcmpeqb (66) Vdq, Wdq | pcmpeqw Pq, Qq pcmpeqw (66) Vdq, Wdq | pcmpeqd Pq, Qq pcmpeqd (66) Vdq, Wdq | emms |

Table A-3. Two-byte Opcode Map: 08H — 7FH (First Byte is 0FH) *

| | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|
| 0 | INVD | WBINVD | | 2-byte Illegal Opcodes UD2 ^{1B} | | NOP Ev | | |
| 1 | Prefetch ^{1C} (Grp 16 ^{1A}) | | | | | | | NOP Ev |
| 2 | movaps Vps, Wps movapd (66) Vpd, Wpd | movaps Wps, Vps movapd (66) Wpd, Vpd | cvtpi2ps Vps, Qpi cvtsi2ss (F3) Vss, Ed/q cvtpi2pd (66) Vpd, Qpi cvtsi2sd (F2) Vsd, Ed/q | movntps Mps, Vps movntpd (66) Mpd, Vpd | cvttps2pi Ppi, Wps cvttss2si (F3) Gd/q, Wss cvttpd2pi (66) Ppi, Wpd cvttss2si (F2) Gd/q, Wsd | cvtps2pi Ppi, Wps cvtss2si (F3) Gd/q, Wss cvtpd2pi (66) Qpi, Wpd cvtsd2si (F2) Gd/q, Wsd | ucomiss Vss, Wss ucomisd (66) Vsd, Wsd | comiss Vss, Wss comisd (66) Vsd, Wsd |
| 3 | 3-byte escape (Table A-4) | | 3-byte escape (Table A-5) | | | | | |
| 4 | CMOVcc(Gv, Ev) - Conditional Move | | | | | | | |
| | S | NS | P/PE | NP/PO | L/NGE | NL/GE | LE/NG | NLE/G |
| 5 | addps Vps, Wps addss (F3) Vss, Wss addpd (66) Vpd, Wpd addsd (F2) Vsd, Wsd | mulps Vps, Wps mulss (F3) Vss, Wss mulpd (66) Vpd, Wpd mulsd (F2) Vsd, Wsd | cvtps2pd Vpd, Wps cvtss2sd (F3) Vsd, Wss cvtpd2ps (66) Vps, Wpd cvtsd2ss (F2) Vsd, Wsd | cvtdq2ps Vps, Wdq cvtps2dq (66) Vdq, Wps cvttps2dq (F3) Vdq, Wps | subps Vps, Wps subss (F3) Vss, Wss subpd (66) Vpd, Wpd subsd (F2) Vsd, Wsd | minps Vps, Wps minss (F3) Vss, Wss minpd (66) Vpd, Wpd minsd (F2) Vsd, Wsd | divps Vps, Wps divss (F3) Vss, Wss divpd (66) Vpd, Wpd divsd (F2) Vsd, Wsd | maxps Vps, Wps maxss (F3) Vss, Wss maxpd (66) Vpd, Wpd maxsd (F2) Vsd, Wsd |
| 6 | punpckhbw Pq, Qd punpckhbw (66) Vdq, Wdq | punpckhwd Pq, Qd punpckhwd (66) Vdq, Wdq | punpckhdq Pq, Qd punpckhdq (66) Vdq, Wdq | packssdw Pq, Qd packssdw (66) Vdq, Wdq | punpcklqdq (66) Vdq, Wdq | punpckhqdq (66) Vdq, Wdq | movd/q/ Pd, Ed/q movd/q (66) Vdq, Ed/q | movq Pq, Qq movdqa (66) Vdq, Wdq movdqu (F3) Vdq, Wdq |
| 7 | VMREAD Ed/q, Gd/q | VMWRITE Gd/q, Ed/q | | | haddps(F2) Vps, Wps haddpd(66) Vpd, Wpd | hsubps(F2) Vps, Wps hsubpd(66) Vpd, Wpd | movd/q Ed/q, Pd movd/q (66) Ed/q, Vdq movq (F3) Vq, Wq | movq Qq, Pq movdqa (66) Wdq, Vdq movdqu (F3) Wdq, Vdq |

Table A-3. Two-byte Opcode Map: 80H — F7H (First Byte is 0FH) *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|--|---|---|---|--|--|---|---|
| 8 | Jcc ⁶⁴ , Jz - Long-displacement jump on condition | | | | | | | |
| | O | NO | B/CNAE | AE/NB/NC | E/Z | NE/NZ | BE/NA | A/NBE |
| 9 | SETcc, Eb - Byte Set on condition | | | | | | | |
| | O | NO | B/CNAE | AE/NB/NC | E/Z | NE/NZ | BE/NA | A/NBE |
| A | PUSH ^{d64} FS | POP ^{d64} FS | CPUID | BT Ev, Gv | SHLD Ev, Gv, Ib | SHLD Ev, Gv, CL | | |
| B | CMPXCHG Eb, Gb Ev, Gv | | LSS Gv, Mp | BTR Ev, Gv | LFS Gv, Mp | LGS Gv, Mp | MOVZX Gv, Eb Gv, Ew | |
| C | XADD Eb, Gb | XADD Ev, Gv | cmpps Vps, Wps, Ib cmpss (F3) Vss, Wss, Ib cmppd (66) Vpd, Wpd, Ib cmpsd (F2) Vsd, Wsd, Ib | movnti Md/q, Gd/q | pinsrw Pq, Rd/q/Mw, Ib pinsrw (66) Vdq, Rd/q/Mw, Ib | pextrw Gd, Nq, Ib pextrw (66) Gd, Udq, Ib | shufps Vps, Wps, Ib shufpd (66) Vpd, Wpd, Ib | Grp 9 ^{1A} |
| D | addsubps(F2) Vps, Wps addsubpd(66) Vpd, Wpd | psrlw Pq, Qq psrlw (66) Vdq, Wdq | psrld Pq, Qq psrld (66) Vdq, Wdq | psrlq Pq, Qq psrlq (66) Vdq, Wdq | paddq Pq, Qq paddq (66) Vdq, Wdq | pmullw Pq, Qq pmullw (66) Vdq, Wdq | movq (66) Wq, Vq movq2dq (F3) Vdq, Nq movdq2q (F2) Pq, Uq | pmovmskb Gd, Nq pmovmskb(66) Gd, Udq |
| E | pavgb Pq, Qq pavgb (66) Vdq, Wdq | psraw Pq, Qq psraw (66) Vdq, Wdq | psrad Pq, Qq psrad (66) Vdq, Wdq | pavgw Pq, Qq pavgw (66) Vdq, Wdq | pmulhw Pq, Qq pmulhw (66) Vdq, Wdq | pmulhw Pq, Qq pmulhw (66) Vdq, Wdq | cvtpd2dq (F2) Vdq, Wpd cvttpd2dq(66) Vdq, Wpd cvtdq2pd (F3) Vpd, Wdq | movntq Mq, Pq movntdq (66) Mdq, Vdq |
| F | lddq (F2) Vdq, Mdq | psllw Pq, Qq psllw (66) Vdq, Wdq | pslld Pq, Qq pslld (66) Vdq, Wdq | psllq Pq, Qq psllq (66) Vdq, Wdq | pmuludq Pq, Qq pmuludq (66) Vdq, Wdq | pmaddwd Pq, Qq pmaddwd(66) Vdq, Wdq | psadbw Pq, Qq psadbw (66) Vdq, Wdq | maskmovq Pq, Nq maskmovdqu (66) Vdq, Udq |

Table A-3. Two-byte Opcode Map: 88H — FFH (First Byte is 0FH) *

| | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|
| 8 | Jcc ⁶⁴ , Jz - Long-displacement jump on condition | | | | | | | |
| | S | NS | P/PE | NP/PO | L/NGE | NL/GE | LE/NG | NLE/G |
| 9 | SETcc, Eb - Byte Set on condition | | | | | | | |
| | S | NS | P/PE | NP/PO | L/NGE | NL/GE | LE/NG | NLE/G |
| A | PUSH ⁶⁴ GS | POP ⁶⁴ GS | RSM | BTS Ev, Gv | SHRD Ev, Gv, lb | SHRD Ev, Gv, CL | (Grp 15 ^{1A}) ^{1C} | IMUL Gv, Ev |
| B | <i>JMPE</i> (reserved for emulator on IPF) POPCNT (F3) Gv, Ev | Grp 10 ^{1A} Invalid Opcode ^{1B} | Grp 8 ^{1A} Ev, lb | BTC Ev, Gv | BSF Gv, Ev | BSR Gv, Ev | MOVSB Gv, Eb Gv, Ew | |
| C | BSWAP | | | | | | | |
| | RAX/EAX/ R8/R8D | RCX/ECX/ R9/R9D | RDX/EDX/ R10/R10D | RBX/EBX/ R11/R11D | RSP/ESP/ R12/R12D | RBP/EBP/ R13/R13D | RSI/ESI/ R14/R14D | RDI/EDI/ R15/R15D |
| D | psubusb Pq, Qq psubusb (66) Vdq, Wdq | psubsw Pq, Qq psubsw (66) Vdq, Wdq | pminub Pq, Qq pminub (66) Vdq, Wdq | pand Pq, Qq pand (66) Vdq, Wdq | paddusb Pq, Qq paddusb (66) Vdq, Wdq | paddusw Pq, Qq paddusw (66) Vdq, Wdq | pmaxub Pq, Qq pmaxub (66) Vdq, Wdq | pandn Pq, Qq pandn (66) Vdq, Wdq |
| E | psubsb Pq, Qq psubsb (66) Vdq, Wdq | psubsw Pq, Qq psubsw (66) Vdq, Wdq | pminsw Pq, Qq pminsw (66) Vdq, Wdq | por Pq, Qq por (66) Vdq, Wdq | paddsb Pq, Qq paddsb (66) Vdq, Wdq | paddsw Pq, Qq paddsw (66) Vdq, Wdq | pmaxsw Pq, Qq pmaxsw (66) Vdq, Wdq | pxor Pq, Qq pxor (66) Vdq, Wdq |
| F | psubb Pq, Qq psubb (66) Vdq, Wdq | psubw Pq, Qq psubw (66) Vdq, Wdq | psubd Pq, Qq psubd (66) Vdq, Wdq | psubq Pq, Qq psubq (66) Vdq, Wdq | paddb Pq, Qq paddb (66) Vdq, Wdq | paddw Pq, Qq paddw (66) Vdq, Wdq | paddd Pq, Qq paddd (66) Vdq, Wdq | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-4. Three-byte Opcode Map: 00H – F7H (First Two Bytes are OF 38H) *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | pshufb Pq, Qq pshufb (66) Vdq, Wdq | phaddw Pq, Qq phaddw (66) Vdq, Wdq | phadd Pq, Qq phadd (66) Vdq, Wdq | phaddsw Pq, Qq phaddsw (66) Vdq, Wdq | pmaddubsw Pq, Qq pmaddubsw (66) Vdq, Wdq | phsubw Pq, Qq phsubw (66) Vdq, Wdq | phsubd Pq, Qq phsubd (66) Vdq, Wdq | phsubsw Pq, Qq phsubsw (66) Vdq, Wdq |
| 1 | pblendvb(66) Vdq, Wdq | | | | blendvps(66) Vdq, Wdq | blendvpd(66) Vdq, Wdq | | ptest (66) Vdq, Wdq |
| 2 | pmovsxbw(66) Vdq, Udq/Mq | pmovsxbd(66) Vdq, Udq/Md | pmovsxbq(66) Vdq, Udq/Mw | pmovsxd(66) Vdq, Udq/Mq | pmovsxwq(66) Vdq, Udq/Md | pmovsxdq (66) Vdq, Udq/Mq | | |
| 3 | pmovzxbw(66) Vdq, Udq/Mq | pmovzxbd(66) Vdq, Udq/Md | pmovzxbq(66) Vdq, Udq/Mw | pmovzxd(66) Vdq, Udq/Mq | pmovzxwq(66) Vdq, Udq/Md | pmovzxdq(66) Vdq, Udq/Mq | | pcmpgtq (66) Vdq, Wdq |
| 4 | pmulld (66) Vdq, Wdq | phminposuw (66) Vdq, Wdq | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | NVEPT (66) Gd/q, Mdq | NVVPID (66) Gd/q, Mdq | | | | | | |
| 9 | | | | | | | | |
| A | | | | | | | | |
| B | | | | | | | | |
| C | | | | | | | | |
| D | | | | | | | | |
| E | | | | | | | | |
| F | MOVBE Gv, Mv CRC32 (F2) Gd, Eb | MOVBE Mv, Gv CRC32 (F2) Gd, Ev | | | | | | |

Table A-4. Three-byte Opcode Map: 08H – FFH (First Two Bytes are 0F 38H) *

| | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|-------------------------|
| 0 | psignb Pq, Qq psignb (66) Vdq, Wdq | psignw Pq, Qq psignw (66) Vdq, Wdq | psignd Pq, Qq psignd (66) Vdq, Wdq | pmulhrsw Pq, Qq pmulhrsw (66) Vdq, Wdq | | | | |
| 1 | | | | | pabsb Pq, Qq pabsb (66) Vdq, Wdq | pabsw Pq, Qq pabsw (66) Vdq, Wdq | pabsd Pq, Qq pabsd (66) Vdq, Wdq | |
| 2 | pmuldq (66) Vdq, Wdq | pcmpeq (66) Vdq, Wdq | movntdqa(66) Vdq, Wdq | packusdw(66) Vdq, Wdq | | | | |
| 3 | pminsb (66) Vdq, Wdq | pminsd (66) Vdq, Wdq | pminuw (66) Vdq, Wdq | pminud (66) Vdq, Wdq | pmaxsb (66) Vdq, Wdq | pmaxsd (66) Vdq, Wdq | pmaxuw (66) Vdq, Wdq | pmaxud (66) Vdq, Wdq |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| A | | | | | | | | |
| B | | | | | | | | |
| C | | | | | | | | |
| D | | | | | | | | |
| E | | | | | | | | |
| F | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-5. Three-byte Opcode Map: 00H — F7H (First two bytes are 0F 3AH) *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---------------------------------|----------------------------------|--|-------------------------------|-------------------------------|-------------------------------|--|-------------------------------|
| 0 | | | | | | | | |
| 1 | | | | | pextrb (66) Rd/Mb, Vdq, Ib | pextrw (66) Rd/Mw, Vdq, Ib | pextrd/pextrq (66) Ed/q, Vdq, Ib | extractps (66) Ed, Vdq, Ib |
| 2 | pinsrb (66) Vdq, Rd/q/Mb, Ib | insertps (66) Vdq, Udq/Md, Ib | pinsrd/pinsrq (66) Vdq, Ed/q, Ib | | | | | |
| 3 | | | | | | | | |
| 4 | dpps (66) Vdq, Wdq, Ib | dppd (66) Vdq, Wdq, Ib | mpsadbw(66) Vdq, Wdq, Ib | | | | | |
| 5 | | | | | | | | |
| 6 | pcmpestrm(66) Vdq, Wdq, Ib | pcmpetri(66) Vdq, Wdq, Ib | pcmpistm(66) Vdq, Wdq, Ib | pcmpistri(66) Vdq, Wdq, Ib | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| A | | | | | | | | |
| B | | | | | | | | |
| C | | | | | | | | |
| D | | | | | | | | |
| E | | | | | | | | |
| F | | | | | | | | |

Table A-5. Three-byte Opcode Map: 08H – FFH (First Two Bytes are 0F 3AH) *

| | 8 | 9 | A | B | C | D | E | F |
|---|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|--|
| 0 | roundps (66) Vdq, Wdq, lb | roundpd (66) Vdq, Wdq, lb | roundss (66) Vss, Wss, lb | roundsd (66) Vsd, Wsd, lb | blendps (66) Vdq, Wdq, lb | blendpd (66) Vdq, Wdq, lb | pblendw (66) Vdq, Wdq, lb | palignr Pq, Qq, lb palignr(66) Vdq, Wdq, lb |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |
| 8 | | | | | | | | |
| 9 | | | | | | | | |
| A | | | | | | | | |
| B | | | | | | | | |
| C | | | | | | | | |
| D | | | | | | | | |
| E | | | | | | | | |
| F | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.4 OPCODE EXTENSIONS FOR ONE-BYTE AND TWO-BYTE OPCODES

Some 1-byte and 2-byte opcodes use bits 3-5 of the ModR/M byte (the nnn field in Figure A-1) as an extension of the opcode.

| | | |
|------------|------------|------------|
| mod | nnn | R/M |
|------------|------------|------------|

Figure A-1. ModR/M Byte nnn Field (Bits 5, 4, and 3)

Opcodes that have opcode extensions are indicated in Table A-6 and organized by group number. Group numbers (from 1 to 16, second column) provide a table entry point. The encoding for the r/m field for each instruction can be established using the third column of the table.

A.4.1 Opcode Look-up Examples Using Opcode Extensions

An Example is provided below.

Example A-3. Interpreting an ADD Instruction

An ADD instruction with a 1-byte opcode of 80H is a Group 1 instruction:

- Table A-6 indicates that the opcode extension field encoded in the ModR/M byte for this instruction is 000B.
- The r/m field can be encoded to access a register (11B) or a memory address using a specified addressing mode (for example: mem = 00B, 01B, 10B).

Example A-2. Looking Up 0F01C3H

Look up opcode 0F01C3 for a VMRESUME instruction by using Table A-2, Table A-3 and Table A-6:

- 0F tells us that this instruction is in the 2-byte opcode map.
- 01 (row 0, column 1 in Table A-3) reveals that this opcode is in Group 7 of Table A-6.
- C3 is the ModR/M byte. The first two bits of C3 are 11B. This tells us to look at the second of the Group 7 rows in Table A-6.
- The Op/Reg bits [5,4,3] are 000B. This tells us to look in the 000 column for Group 7.
- Finally, the R/M bits [2,1,0] are 011B. This identifies the opcode as the VMRESUME instruction.

A.4.2 Opcode Extension Tables

See Table A-6 below.

Table A-6. Opcode Extensions for One- and Two-byte Opcodes by Group Number *

| Opcode | Group | Mod 7,6 | Encoding of Bits 5,4,3 of the ModR/M Byte (bits 2,1,0 in parenthesis) | | | | | | | |
|--|-------|----------|--|-------------------------------------|------------------------------------|-------------|--------------------------|----------------|--|----------------|
| | | | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 80-83 | 1 | mem, 11B | ADD | OR | ADC | SBB | AND | SUB | XOR | CMP |
| 8F | 1A | mem, 11B | POP | | | | | | | |
| C0, C1 reg, imm D0, D1 reg, 1 D2, D3 reg, CL | 2 | mem, 11B | ROL | ROR | RCL | RCR | SHL/SAL | SHR | | SAR |
| F6, F7 | 3 | mem, 11B | TEST lb/lz | | NOT | NEG | MUL AL/rAX | IMUL AL/rAX | DIV AL/rAX | IDIV AL/rAX |
| FE | 4 | mem, 11B | INC Eb | DEC Eb | | | | | | |
| FF | 5 | mem, 11B | INC Ev | DEC Ev | CALLN ⁶⁴ Ev | CALLF Ep | JMPN ⁶⁴ Ev | JMPF Ep | PUSH ^{d64} Ev | |
| 0F 00 | 6 | mem, 11B | SLDT Rv/Mw | STR Rv/Mw | LLDT Ew | LTR Ew | VERR Ew | VERW Ew | | |
| 0F 01 | 7 | mem | SGDT Ms | SIDT Ms | LGDT Ms | LIDT Ms | SMSW Mw/Rv | | LMSW Ew | INVLPG Mb |
| | | 11B | VMCALL (001) VMLAUNCH (010) VMRESUME (011) VMXOFF (100) | MONITOR (000) MWAIT (001) | XGETBV (000) XSETBV (001) | | | | SWAPGS ⁶⁴ (000) | |
| 0F BA | 8 | mem, 11B | | | | | BT | BTS | BTR | BTC |
| 0F C7 | 9 | mem | | CMPXCH8B Mq CMPXCHG16B Mdq | | | | | VMPTRLD Mq VMCLEAR (66) Mq VMXON (F3) Mq | VMPTRST Mq |
| | | 11B | | | | | | | | |
| 0F B9 | 10 | mem | | | | | | | | |
| | | 11B | | | | | | | | |
| C6 | 11 | mem, 11B | MOV Eb, Ib | | | | | | | |
| C7 | | mem | MOV Ev, Iz | | | | | | | |
| | | 11B | | | | | | | | |

Table A-6. Opcode Extensions for One- and Two-byte Opcodes by Group Number *

| Opcode | Group | Mod 7,6 | Encoding of Bits 5,4,3 of the ModR/M Byte (bits 2,1,0 in parenthesis) | | | | | | | |
|--------|-------|---------|---|----------------|--|-----------------------|--|--------|--|------------------------|
| | | | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| 0F 71 | 12 | mem | | | | | | | | |
| | | 11B | | | psrlw Nq, lb psrlw (66) Udq, lb | | psraw Nq, lb psraw (66) Udq, lb | | psllw Nq, lb psllw (66) Udq, lb | |
| 0F 72 | 13 | mem | | | | | | | | |
| | | 11B | | | psrld Nq, lb psrld (66) Udq, lb | | psrad Nq, lb psrad (66) Udq, lb | | pslld Nq, lb pslld (66) Udq, lb | |
| 0F 73 | 14 | mem | | | | | | | | |
| | | 11B | | | psrlq Nq, lb psrlq (66) Udq, lb | psrlq (66) Udq, lb | | | psllq Nq, lb psllq (66) Udq, lb | pslldq (66) Udq, lb |
| 0F AE | 15 | mem | fxsave | fxrstor | ldmxcsr | stmxcsr | XSAVE | XRSTOR | | clflush |
| | | 11B | | | | | | lfence | mfence | sfence |
| 0F 18 | 16 | mem | prefetch NTA | prefetch T0 | prefetch T1 | prefetch T2 | | | | |
| | | 11B | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5 ESCAPE OPCODE INSTRUCTIONS

Opcode maps for coprocessor escape instruction opcodes (x87 floating-point instruction opcodes) are in Table A-7 through Table A-22. These maps are grouped by the first byte of the opcode, from D8-DF. Each of these opcodes has a ModR/M byte. If the ModR/M byte is within the range of 00H-BFH, bits 3-5 of the ModR/M byte are used as an opcode extension, similar to the technique used for 1- and 2-byte opcodes (see A.4). If the ModR/M byte is outside the range of 00H through BFH, the entire ModR/M byte is used as an opcode extension.

A.5.1 Opcode Look-up Examples for Escape Instruction Opcodes

Examples are provided below.

Example A-5. Opcode with ModR/M Byte in the 00H through BFH Range

DD0504000000H can be interpreted as follows:

- The instruction encoded with this opcode can be located in Section . Since the ModR/M byte (05H) is within the 00H through BFH range, bits 3 through 5 (000) of this byte indicate the opcode for an FLD double-real instruction (see Table A-9).
- The double-real value to be loaded is at 00000004H (the 32-bit displacement that follows and belongs to this opcode).

Example A-3. Opcode with ModR/M Byte outside the 00H through BFH Range

D8C1H can be interpreted as follows:

- This example illustrates an opcode with a ModR/M byte outside the range of 00H through BFH. The instruction can be located in Section A.4.
- In Table A-8, the ModR/M byte C1H indicates row C, column 1 (the FADD instruction using ST(0), ST(1) as operands).

A.5.2 Escape Opcode Instruction Tables

Tables are listed below.

A.5.2.1 Escape Opcodes with D8 as First Byte

Table A-7 and A-8 contain maps for the escape instruction opcodes that begin with D8H. Table A-7 shows the map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-7. D8 Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte (refer to Figure A.4) | | | | | | | |
|--|------------------|------------------|-------------------|------------------|-------------------|------------------|-------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FADD single-real | FMUL single-real | FCOM single-real | FCOMP single-real | FSUB single-real | FSUBR single-real | FDIV single-real | FDIVR single-real |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-8 shows the map if the ModR/M byte is outside the range of 00H-BFH. Here, the first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-8. D8 Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FADD | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FCOM | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),T(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| E | FSUB | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| F | FDIV | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FMUL | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FCOMP | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),T(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| E | FSUBR | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| F | FDIVR | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.2 Escape Opcodes with D9 as First Byte

Table A-9 and A-10 contain maps for escape instruction opcodes that begin with D9H. Table A-9 shows the map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-9. D9 Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte | | | | | | | |
|--------------------------|------|--------------------|---------------------|-----------------------|------------------|-----------------------|------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FLD single-real | | FST single-real | FSTP single-real | FLDENV 14/28 bytes | FLDCW 2 bytes | FSTENV 14/28 bytes | FSTCW 2 bytes |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-10 shows the map if the ModR/M byte is outside the range of 00H-BFH. Here, the first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-10. D9 Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FLD | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FNOP | | | | | | | |
| E | FCFS | FABS | | | FTST | FXAM | | |
| F | F2XM1 | FYL2X | FPTAN | FPATAN | FXTRACT | FPREM1 | FDECSTP | FINCSTP |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FXCH | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | | | | | | | | |
| E | FLD1 | FLDL2T | FLDL2E | FLDPI | FLDLG2 | FLDLN2 | FLDZ | |
| F | FPREM | FYL2XP1 | FSQRT | FSINCOS | FRNDINT | FSCALE | FSIN | FCOS |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.3 Escape Opcodes with DA as First Byte

Table A-11 and A-12 contain maps for escape instruction opcodes that begin with DAH. Table A-11 shows the map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-11. DA Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte | | | | | | | |
|--------------------------|------------------------|------------------------|-------------------------|------------------------|-------------------------|------------------------|-------------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FIADD dword-integer | FIMUL dword-integer | FICOM dword-integer | FICOMP dword-integer | FISUB dword-integer | FISUBR dword-integer | FIDIV dword-integer | FIDIVR dword-integer |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-11 shows the map if the ModR/M byte is outside the range of 00H-BFH. Here, the first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-12. DA Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FCMOV B | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FCMOV BE | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| E | | | | | | | | |
| F | | | | | | | | |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FCMOV E | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FCMOV U | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| E | | FUCOMPP | | | | | | |
| F | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.4 Escape Opcodes with DB as First Byte

Table A-13 and A-14 contain maps for escape instruction opcodes that begin with DBH. Table A-13 shows the map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-13. DB Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte | | | | | | | |
|--------------------------|-------------------------|-----------------------|------------------------|------|----------------------|------|-----------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FILD dword-integer | FISTTP dword-integer | FIST dword-integer | FISTP dword-integer | | FLD extended-real | | FSTP extended-real |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-14 shows the map if the ModR/M byte is outside the range of 00H-BFH. Here, the first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-14. DB Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FCMOVNB | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FCMOVNBE | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| E | | | FCLEX | FINIT | | | | |
| F | FCOMI | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FCMOVNE | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| D | FCMOVNU | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| E | FUCOMI | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| F | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.5 Escape Opcodes with DC as First Byte

Table A-15 and A-16 contain maps for escape instruction opcodes that begin with DCH. Table A-15 shows the map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-15. DC Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte (refer to Figure A-1) | | | | | | | |
|--|------------------|------------------|-------------------|------------------|-------------------|------------------|-------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FADD double-real | FMUL double-real | FCOM double-real | FCOMP double-real | FSUB double-real | FSUBR double-real | FDIV double-real | FDIVR double-real |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-16 shows the map if the ModR/M byte is outside the range of 00H-BFH. In this case the first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-16. DC Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FADD | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| D | | | | | | | | |
| | | | | | | | | |
| E | FSUBR | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| F | FDIVR | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FMUL | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| D | | | | | | | | |
| | | | | | | | | |
| E | FSUB | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| F | FDIV | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.6 Escape Opcodes with DD as First Byte

Table A-17 and A-18 contain maps for escape instruction opcodes that begin with DDH. Table A-17 shows the map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-17. DD Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte | | | | | | | |
|--------------------------|------------------|-----------------|------------------|--------------------|------|-------------------|---------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FLD double-real | FISTTP integer64 | FST double-real | FSTP double-real | FRSTOR 98/108bytes | | FSAVE 98/108bytes | FSTSW 2 bytes |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-18 shows the map if the ModR/M byte is outside the range of 00H-BFH. The first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-18. DD Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FFREE | | | | | | | |
| | ST(0) | ST(1) | ST(2) | ST(3) | ST(4) | ST(5) | ST(6) | ST(7) |
| D | FST | | | | | | | |
| | ST(0) | ST(1) | ST(2) | ST(3) | ST(4) | ST(5) | ST(6) | ST(7) |
| E | FUCOM | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| F | | | | | | | | |

| | 8 | 9 | A | B | C | D | E | F |
|---|--------|-------|-------|-------|-------|-------|-------|-------|
| C | | | | | | | | |
| | | | | | | | | |
| D | FSTP | | | | | | | |
| | ST(0) | ST(1) | ST(2) | ST(3) | ST(4) | ST(5) | ST(6) | ST(7) |
| E | FUCOMP | | | | | | | |
| | ST(0) | ST(1) | ST(2) | ST(3) | ST(4) | ST(5) | ST(6) | ST(7) |
| F | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.7 Escape Opcodes with DE as First Byte

Table A-19 and A-20 contain opcode maps for escape instruction opcodes that begin with DEH. Table A-19 shows the opcode map if the ModR/M byte is in the range of 00H-BFH. In this case, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-19. DE Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte | | | | | | | |
|--------------------------|-----------------------|-----------------------|------------------------|-----------------------|------------------------|-----------------------|------------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FIADD word-integer | FIMUL word-integer | FICOM word-integer | FICOMP word-integer | FISUB word-integer | FISUBR word-integer | FIDIV word-integer | FIDIVR word-integer |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-20 shows the opcode map if the ModR/M byte is outside the range of 00H-BFH. The first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-20. DE Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FADDP | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| D | | | | | | | | |
| | | | | | | | | |
| E | FSUBRP | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| F | FDIVRP | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | FMULP | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| D | | FCOMPP | | | | | | |
| | | | | | | | | |
| E | FSUBP | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |
| F | FDIVP | | | | | | | |
| | ST(0),ST(0) | ST(1),ST(0) | ST(2),ST(0) | ST(3),ST(0) | ST(4),ST(0) | ST(5),ST(0) | ST(6),ST(0) | ST(7),ST(0) |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

A.5.2.8 Escape Opcodes with DF As First Byte

Table A-21 and A-22 contain the opcode maps for escape instruction opcodes that begin with DFH. Table A-21 shows the opcode map if the ModR/M byte is in the range of 00H-BFH. Here, the value of bits 3-5 (the nnn field in Figure A-1) selects the instruction.

Table A-21. DF Opcode Map When ModR/M Byte is Within 00H to BFH *

| nnn Field of ModR/M Byte | | | | | | | |
|--------------------------|------------------------|----------------------|-----------------------|---------------------|-----------------------|----------------------|------------------------|
| 000B | 001B | 010B | 011B | 100B | 101B | 110B | 111B |
| FILD word-integer | FISTTP word-integer | FIST word-integer | FISTP word-integer | FBLD packed- BCD | FILD qword-integer | FBSTP packed- BCD | FISTP qword-integer |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

Table A-22 shows the opcode map if the ModR/M byte is outside the range of 00H-BFH. The first digit of the ModR/M byte selects the table row and the second digit selects the column.

Table A-22. DF Opcode Map When ModR/M Byte is Outside 00H to BFH *

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | | | | | | | | |
| D | | | | | | | | |
| E | FSTSW AX | | | | | | | |
| F | FCOMIP | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |

| | 8 | 9 | A | B | C | D | E | F |
|---|-------------|-------------|-------------|-------------|-------------|-------------|-------------|-------------|
| C | | | | | | | | |
| D | | | | | | | | |
| E | FUCOMIP | | | | | | | |
| | ST(0),ST(0) | ST(0),ST(1) | ST(0),ST(2) | ST(0),ST(3) | ST(0),ST(4) | ST(0),ST(5) | ST(0),ST(6) | ST(0),ST(7) |
| F | | | | | | | | |

NOTES:

* All blanks in all opcode maps are reserved and must not be used. Do not depend on the operation of undefined or reserved locations.

OPCODE MAP

APPENDIX B

INSTRUCTION FORMATS AND ENCODINGS

This appendix provides machine instruction formats and encodings of IA-32 instructions. The first section describes the IA-32 architecture's machine instruction format. The remaining sections show the formats and encoding of general-purpose, MMX, P6 family, SSE/SSE2/SSE3, x87 FPU instructions, and VMX instructions. Those instruction formats also apply to Intel 64 architecture. Instruction formats used in 64-bit mode are provided as supersets of the above.

B.1 MACHINE INSTRUCTION FORMAT

All Intel Architecture instructions are encoded using subsets of the general machine instruction format shown in Figure B-1. Each instruction consists of:

- an opcode
- a register and/or address mode specifier consisting of the ModR/M byte and sometimes the scale-index-base (SIB) byte (if required)
- a displacement and an immediate data field (if required)

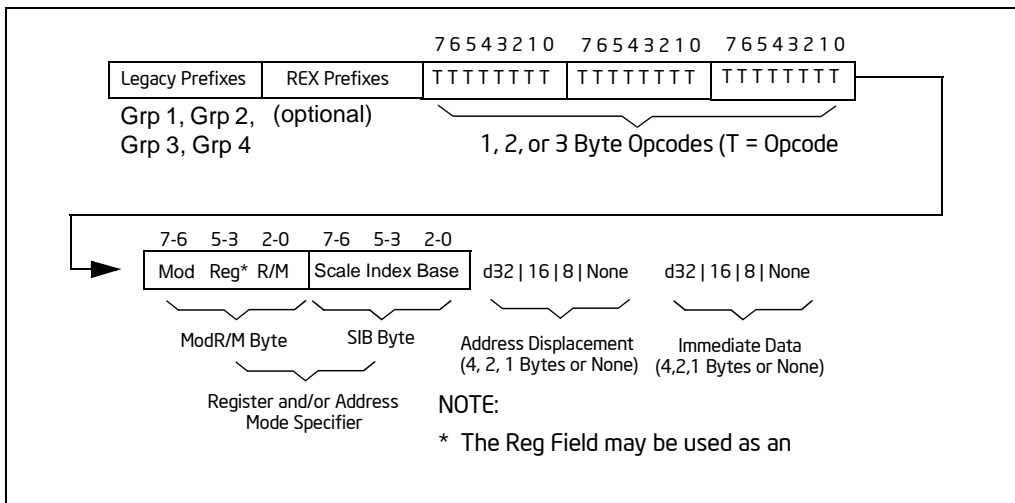


Figure B-1. General Machine Instruction Format

The following sections discuss this format.

B.1.1 Legacy Prefixes

The legacy prefixes noted in Figure B-1 include 66H, 67H, F2H and F3H. They are optional, except when F2H, F3H and 66H are used in new instruction extensions. Legacy prefixes must be placed before REX prefixes.

Refer to Chapter 2, "Instruction Format," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A*, for more information on legacy prefixes.

B.1.2 REX Prefixes

REX prefixes are a set of 16 opcodes that span one row of the opcode map and occupy entries 40H to 4FH. These opcodes represent valid instructions (INC or DEC) in IA-32 operating modes and in compatibility mode. In 64-bit mode, the same opcodes represent the instruction prefix REX and are not treated as individual instructions.

Refer to Chapter 2, "Instruction Format," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A*, for more information on REX prefixes.

B.1.3 Opcode Fields

The primary opcode for an instruction is encoded in one to three bytes of the instruction. Within the primary opcode, smaller encoding fields may be defined. These fields vary according to the class of operation being performed.

Almost all instructions that refer to a register and/or memory operand have a register and/or address mode byte following the opcode. This byte, the ModR/M byte, consists of the mod field (2 bits), the reg field (3 bits; this field is sometimes an opcode extension), and the R/M field (3 bits). Certain encodings of the ModR/M byte indicate that a second address mode byte, the SIB byte, must be used.

If the addressing mode specifies a displacement, the displacement value is placed immediately following the ModR/M byte or SIB byte. Possible sizes are 8, 16, or 32 bits. If the instruction specifies an immediate value, the immediate value follows any displacement bytes. The immediate, if specified, is always the last field of the instruction.

Refer to Chapter 2, "Instruction Format," in the *Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A*, for more information on opcodes.

B.1.4 Special Fields

Table B-1 lists bit fields that appear in certain instructions, sometimes within the opcode bytes. All of these fields (except the d bit) occur in the general-purpose instruction formats in Table B-13.

Table B-1. Special Fields Within Instruction Encodings

| Field Name | Description | Number of Bits |
|------------|--|----------------|
| reg | General-register specifier (see Table B-4 or B-5) | 3 |
| w | Specifies if data is byte or full-sized, where full-sized is 16 or 32 bits (see Table B-6) | 1 |
| s | Specifies sign extension of an immediate field (see Table B-7) | 1 |
| sreg2 | Segment register specifier for CS, SS, DS, ES (see Table B-8) | 2 |
| sreg3 | Segment register specifier for CS, SS, DS, ES, FS, GS (see Table B-8) | 3 |
| eee | Specifies a special-purpose (control or debug) register (see Table B-9) | 3 |
| ttn | For conditional instructions, specifies a condition asserted or negated (see Table B-12) | 4 |
| d | Specifies direction of data operation (see Table B-11) | 1 |

B.1.4.1 Reg Field (reg) for Non-64-Bit Modes

The reg field in the ModR/M byte specifies a general-purpose register operand. The group of registers specified is modified by the presence and state of the w bit in an encoding (refer to Section B.1.4.3). Table B-2 shows the encoding of the reg field when the w bit is not present in an encoding; Table B-3 shows the encoding of the reg field when the w bit is present.

Table B-2. Encoding of reg Field When w Field is Not Present in Instruction

| reg Field | Register Selected during 16-Bit Data Operations | Register Selected during 32-Bit Data Operations |
|-----------|---|---|
| 000 | AX | EAX |
| 001 | CX | ECX |
| 010 | DX | EDX |
| 011 | BX | EBX |
| 100 | SP | ESP |
| 101 | BP | EBP |
| 110 | SI | ESI |
| 111 | DI | EDI |

Table B-3. Encoding of reg Field When w Field is Present in Instruction

| Register Specified by reg Field During 16-Bit Data Operations | | | Register Specified by reg Field During 32-Bit Data Operations | | |
|---|---------------------|------------|---|---------------------|------------|
| reg | Function of w Field | | reg | Function of w Field | |
| | When w = 0 | When w = 1 | | When w = 0 | When w = 1 |
| 000 | AL | AX | 000 | AL | EAX |
| 001 | CL | CX | 001 | CL | ECX |
| 010 | DL | DX | 010 | DL | EDX |
| 011 | BL | BX | 011 | BL | EBX |
| 100 | AH | SP | 100 | AH | ESP |
| 101 | CH | BP | 101 | CH | EBP |
| 110 | DH | SI | 110 | DH | ESI |
| 111 | BH | DI | 111 | BH | EDI |

B.1.4.2 Reg Field (reg) for 64-Bit Mode

Just like in non-64-bit modes, the reg field in the ModR/M byte specifies a general-purpose register operand. The group of registers specified is modified by the presence of and state of the w bit in an encoding (refer to Section B.1.4.3). Table B-4 shows the encoding of the reg field when the w bit is not present in an encoding; Table B-5 shows the encoding of the reg field when the w bit is present.

Table B-4. Encoding of reg Field When w Field is Not Present in Instruction

| reg Field | Register Selected during 16-Bit Data Operations | Register Selected during 32-Bit Data Operations | Register Selected during 64-Bit Data Operations |
|-----------|---|---|---|
| 000 | AX | EAX | RAX |
| 001 | CX | ECX | RCX |
| 010 | DX | EDX | RDX |
| 011 | BX | EBX | RBX |
| 100 | SP | ESP | RSP |
| 101 | BP | EBP | RBP |
| 110 | SI | ESI | RSI |
| 111 | DI | EDI | RDI |

Table B-5. Encoding of reg Field When w Field is Present in Instruction

| Register Specified by reg Field During 16-Bit Data Operations | | | Register Specified by reg Field During 32-Bit Data Operations | | |
|---|---------------------|------------|---|---------------------|------------|
| reg | Function of w Field | | reg | Function of w Field | |
| | When w = 0 | When w = 1 | | When w = 0 | When w = 1 |
| 000 | AL | AX | 000 | AL | EAX |
| 001 | CL | CX | 001 | CL | ECX |
| 010 | DL | DX | 010 | DL | EDX |
| 011 | BL | BX | 011 | BL | EBX |
| 100 | AH ¹ | SP | 100 | AH* | ESP |
| 101 | CH ¹ | BP | 101 | CH* | EBP |
| 110 | DH ¹ | SI | 110 | DH* | ESI |
| 111 | BH ¹ | DI | 111 | BH* | EDI |

NOTES:

1. AH, CH, DH, BH can not be encoded when REX prefix is used. Such an expression defaults to the low byte.

B.1.4.3 Encoding of Operand Size (w) Bit

The current operand-size attribute determines whether the processor is performing 16-bit, 32-bit or 64-bit operations. Within the constraints of the current operand-size attribute, the operand-size bit (w) can be used to indicate operations on 8-bit operands or the full operand size specified with the operand-size attribute. Table B-6 shows the encoding of the w bit depending on the current operand-size attribute.

Table B-6. Encoding of Operand Size (w) Bit

| w Bit | Operand Size When Operand-Size Attribute is 16 Bits | Operand Size When Operand-Size Attribute is 32 Bits |
|-------|---|---|
| 0 | 8 Bits | 8 Bits |
| 1 | 16 Bits | 32 Bits |

B.1.4.4 Sign-Extend (s) Bit

The sign-extend (s) bit occurs in instructions with immediate data fields that are being extended from 8 bits to 16 or 32 bits. See Table B-7.

Table B-7. Encoding of Sign-Extend (s) Bit

| s | Effect on 8-Bit Immediate Data | Effect on 16- or 32-Bit Immediate Data |
|----------|--|---|
| 0 | None | None |
| 1 | Sign-extend to fill 16-bit or 32-bit destination | None |

B.1.4.5 Segment Register (sreg) Field

When an instruction operates on a segment register, the reg field in the ModR/M byte is called the sreg field and is used to specify the segment register. Table B-8 shows the encoding of the sreg field. This field is sometimes a 2-bit field (sreg2) and other times a 3-bit field (sreg3).

Table B-8. Encoding of the Segment Register (sreg) Field

| 2-Bit sreg2 Field | Segment Register Selected | 3-Bit sreg3 Field | Segment Register Selected |
|--------------------------|----------------------------------|--------------------------|----------------------------------|
| 00 | ES | 000 | ES |
| 01 | CS | 001 | CS |
| 10 | SS | 010 | SS |
| 11 | DS | 011 | DS |
| | | 100 | FS |
| | | 101 | GS |
| | | 110 | Reserved ¹ |
| | | 111 | Reserved |

NOTES:

1. Do not use reserved encodings.

B.1.4.6 Special-Purpose Register (eee) Field

When control or debug registers are referenced in an instruction they are encoded in the eee field, located in bits 5 through 3 of the ModR/M byte (an alternate encoding of the sreg field). See Table B-9.

Table B-9. Encoding of Special-Purpose Register (eee) Field

| eee | Control Register | Debug Register |
|-----|-----------------------|----------------|
| 000 | CR0 | DR0 |
| 001 | Reserved ⁷ | DR1 |
| 010 | CR2 | DR2 |
| 011 | CR3 | DR3 |
| 100 | CR4 | Reserved |
| 101 | Reserved | Reserved |
| 110 | Reserved | DR6 |
| 111 | Reserved | DR7 |

NOTES:

1. Do not use reserved encodings.

B.1.4.7 Condition Test (ttn) Field

For conditional instructions (such as conditional jumps and set on condition), the condition test field (ttn) is encoded for the condition being tested. The ttt part of the field gives the condition to test and the n part indicates whether to use the condition ($n = 0$) or its negation ($n = 1$).

- For 1-byte primary opcodes, the ttn field is located in bits 3, 2, 1, and 0 of the opcode byte.
- For 2-byte primary opcodes, the ttn field is located in bits 3, 2, 1, and 0 of the second opcode byte.

Table B-10 shows the encoding of the ttn field.

Table B-10. Encoding of Conditional Test (tttn) Field

| tttn | Mnemonic | Condition |
|------|----------|---|
| 0000 | O | Overflow |
| 0001 | NO | No overflow |
| 0010 | B, NAE | Below, Not above or equal |
| 0011 | NB, AE | Not below, Above or equal |
| 0100 | E, Z | Equal, Zero |
| 0101 | NE, NZ | Not equal, Not zero |
| 0110 | BE, NA | Below or equal, Not above |
| 0111 | NBE, A | Not below or equal, Above |
| 1000 | S | Sign |
| 1001 | NS | Not sign |
| 1010 | P, PE | Parity, Parity Even |
| 1011 | NP, PO | Not parity, Parity Odd |
| 1100 | L, NGE | Less than, Not greater than or equal to |
| 1101 | NL, GE | Not less than, Greater than or equal to |
| 1110 | LE, NG | Less than or equal to, Not greater than |
| 1111 | NLE, G | Not less than or equal to, Greater than |

B.1.4.8 Direction (d) Bit

In many two-operand instructions, a direction bit (d) indicates which operand is considered the source and which is the destination. See Table B-11.

- When used for integer instructions, the d bit is located at bit 1 of a 1-byte primary opcode. Note that this bit does not appear as the symbol “d” in Table B-13; the actual encoding of the bit as 1 or 0 is given.
- When used for floating-point instructions (in Table B-16), the d bit is shown as bit 2 of the first byte of the primary opcode.

Table B-11. Encoding of Operation Direction (d) Bit

| d | Source | Destination |
|---|--------------------|--------------------|
| 0 | reg Field | ModR/M or SIB Byte |
| 1 | ModR/M or SIB Byte | reg Field |

B.1.5 Other Notes

Table B-12 contains notes on particular encodings. These notes are indicated in the tables shown in the following sections by superscripts.

Table B-12. Notes on Instruction Encoding

| Symbol | Note |
|--------|---|
| A | A value of 11B in bits 7 and 6 of the ModR/M byte is reserved. |
| B | A value of 01B (or 10B) in bits 7 and 6 of the ModR/M byte is reserved. |

B.2 GENERAL-PURPOSE INSTRUCTION FORMATS AND ENCODINGS FOR NON-64-BIT MODES

Table B-13 shows machine instruction formats and encodings for general purpose instructions in non-64-bit modes.

Table B-13. General Purpose Instruction Formats and Encodings for Non-64-Bit Modes

| Instruction and Format | Encoding |
|--|--|
| AAA - ASCII Adjust after Addition | 0011 0111 |
| AAD - ASCII Adjust AX before Division | 1101 0101 : 0000 1010 |
| AAM - ASCII Adjust AX after Multiply | 1101 0100 : 0000 1010 |
| AAS - ASCII Adjust AL after Subtraction | 0011 1111 |
| ADC - ADD with Carry | |
| register1 to register2 | 0001 000w : 11 reg1 reg2 |
| register2 to register1 | 0001 001w : 11 reg1 reg2 |
| memory to register | 0001 001w : mod reg r/m |
| register to memory | 0001 000w : mod reg r/m |
| immediate to register | 1000 00sw : 11 010 reg : immediate data |
| immediate to AL, AX, or EAX | 0001 010w : immediate data |
| immediate to memory | 1000 00sw : mod 010 r/m : immediate data |
| ADD - Add | |
| register1 to register2 | 0000 000w : 11 reg1 reg2 |
| register2 to register1 | 0000 001w : 11 reg1 reg2 |
| memory to register | 0000 001w : mod reg r/m |
| register to memory | 0000 000w : mod reg r/m |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| immediate to register | 1000 00sw : 11 000 reg : immediate data |
| immediate to AL, AX, or EAX | 0000 010w : immediate data |
| immediate to memory | 1000 00sw : mod 000 r/m : immediate data |
| AND - Logical AND | |
| register1 to register2 | 0010 000w : 11 reg1 reg2 |
| register2 to register1 | 0010 001w : 11 reg1 reg2 |
| memory to register | 0010 001w : mod reg r/m |
| register to memory | 0010 000w : mod reg r/m |
| immediate to register | 1000 00sw : 11 100 reg : immediate data |
| immediate to AL, AX, or EAX | 0010 010w : immediate data |
| immediate to memory | 1000 00sw : mod 100 r/m : immediate data |
| ARPL - Adjust RPL Field of Selector | |
| from register | 0110 0011 : 11 reg1 reg2 |
| from memory | 0110 0011 : mod reg r/m |
| BOUND - Check Array Against Bounds | 0110 0010 : mod ^A reg r/m |
| BSF - Bit Scan Forward | |
| register1, register2 | 0000 1111 : 1011 1100 : 11 reg1 reg2 |
| memory, register | 0000 1111 : 1011 1100 : mod reg r/m |
| BSR - Bit Scan Reverse | |
| register1, register2 | 0000 1111 : 1011 1101 : 11 reg1 reg2 |
| memory, register | 0000 1111 : 1011 1101 : mod reg r/m |
| BSWAP - Byte Swap | 0000 1111 : 1100 1 reg |
| BT - Bit Test | |
| register, immediate | 0000 1111 : 1011 1010 : 11 100 reg: imm8 data |
| memory, immediate | 0000 1111 : 1011 1010 : mod 100 r/m : imm8 data |
| register1, register2 | 0000 1111 : 1010 0011 : 11 reg2 reg1 |
| memory, reg | 0000 1111 : 1010 0011 : mod reg r/m |
| BTC - Bit Test and Complement | |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| register, immediate | 0000 1111 : 1011 1010 : 11 111 reg: imm8 data |
| memory, immediate | 0000 1111 : 1011 1010 : mod 111 r/m : imm8 data |
| register1, register2 | 0000 1111 : 1011 1011 : 11 reg2 reg1 |
| memory, reg | 0000 1111 : 1011 1011 : mod reg r/m |
| BTR - Bit Test and Reset | |
| register, immediate | 0000 1111 : 1011 1010 : 11 110 reg: imm8 data |
| memory, immediate | 0000 1111 : 1011 1010 : mod 110 r/m : imm8 data |
| register1, register2 | 0000 1111 : 1011 0011 : 11 reg2 reg1 |
| memory, reg | 0000 1111 : 1011 0011 : mod reg r/m |
| BTS - Bit Test and Set | |
| register, immediate | 0000 1111 : 1011 1010 : 11 101 reg: imm8 data |
| memory, immediate | 0000 1111 : 1011 1010 : mod 101 r/m : imm8 data |
| register1, register2 | 0000 1111 : 1010 1011 : 11 reg2 reg1 |
| memory, reg | 0000 1111 : 1010 1011 : mod reg r/m |
| CALL - Call Procedure (in same segment) | |
| direct | 1110 1000 : full displacement |
| register indirect | 1111 1111 : 11 010 reg |
| memory indirect | 1111 1111 : mod 010 r/m |
| CALL - Call Procedure (in other segment) | |
| direct | 1001 1010 : unsigned full offset, selector |
| indirect | 1111 1111 : mod 011 r/m |
| CBW - Convert Byte to Word | 1001 1000 |
| CDQ - Convert Doubleword to Qword | 1001 1001 |
| CLC - Clear Carry Flag | 1111 1000 |
| CLD - Clear Direction Flag | 1111 1100 |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| CLI - Clear Interrupt Flag | 1111 1010 |
| CLTS - Clear Task-Switched Flag in CRO | 0000 1111 : 0000 0110 |
| CMC - Complement Carry Flag | 1111 0101 |
| CMP - Compare Two Operands | |
| register1 with register2 | 0011 100w : 11 reg1 reg2 |
| register2 with register1 | 0011 101w : 11 reg1 reg2 |
| memory with register | 0011 100w : mod reg r/m |
| register with memory | 0011 101w : mod reg r/m |
| immediate with register | 1000 00sw : 11 111 reg : immediate data |
| immediate with AL, AX, or EAX | 0011 110w : immediate data |
| immediate with memory | 1000 00sw : mod 111 r/m : immediate data |
| CMPS/CMPSB/CMPSW/CMPSD - Compare String Operands | 1010 011w |
| CMPXCHG - Compare and Exchange | |
| register1, register2 | 0000 1111 : 1011 000w : 11 reg2 reg1 |
| memory, register | 0000 1111 : 1011 000w : mod reg r/m |
| CPUID - CPU Identification | 0000 1111 : 1010 0010 |
| CWD - Convert Word to Doubleword | 1001 1001 |
| CWDE - Convert Word to Doubleword | 1001 1000 |
| DAA - Decimal Adjust AL after Addition | 0010 0111 |
| DAS - Decimal Adjust AL after Subtraction | 0010 1111 |
| DEC - Decrement by 1 | |
| register | 1111 111w : 11 001 reg |
| register (alternate encoding) | 0100 1 reg |
| memory | 1111 111w : mod 001 r/m |
| DIV - Unsigned Divide | |
| AL, AX, or EAX by register | 1111 011w : 11 110 reg |
| AL, AX, or EAX by memory | 1111 011w : mod 110 r/m |
| HLT - Halt | 1111 0100 |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| IDIV - Signed Divide | |
| AL, AX, or EAX by register | 1111 011w : 11 111 reg |
| AL, AX, or EAX by memory | 1111 011w : mod 111 r/m |
| IMUL - Signed Multiply | |
| AL, AX, or EAX with register | 1111 011w : 11 101 reg |
| AL, AX, or EAX with memory | 1111 011w : mod 101 reg |
| register1 with register2 | 0000 1111 : 1010 1111 : 11 : reg1 reg2 |
| register with memory | 0000 1111 : 1010 1111 : mod reg r/m |
| register1 with immediate to register2 | 0110 10s1 : 11 reg1 reg2 : immediate data |
| memory with immediate to register | 0110 10s1 : mod reg r/m : immediate data |
| IN - Input From Port | |
| fixed port | 1110 010w : port number |
| variable port | 1110 110w |
| INC - Increment by 1 | |
| reg | 1111 111w : 11 000 reg |
| reg (alternate encoding) | 0100 0 reg |
| memory | 1111 111w : mod 000 r/m |
| INS - Input from DX Port | 0110 110w |
| INT n - Interrupt Type n | 1100 1101 : type |
| INT - Single-Step Interrupt 3 | 1100 1100 |
| INTO - Interrupt 4 on Overflow | 1100 1110 |
| INVD - Invalidate Cache | 0000 1111 : 0000 1000 |
| INVLPG - Invalidate TLB Entry | 0000 1111 : 0000 0001 : mod 111 r/m |
| IRET/IRETD - Interrupt Return | 1100 1111 |
| Jcc - Jump if Condition is Met | |
| 8-bit displacement | 0111 tttt : 8-bit displacement |
| full displacement | 0000 1111 : 1000 tttt : full displacement |
| JCXZ/JECXZ - Jump on CX/ECX Zero Address-size prefix differentiates JCXZ and JECXZ | 1110 0011 : 8-bit displacement |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| JMP - Unconditional Jump (to same segment) | |
| short | 1110 1011 : 8-bit displacement |
| direct | 1110 1001 : full displacement |
| register indirect | 1111 1111 : 11 100 reg |
| memory indirect | 1111 1111 : mod 100 r/m |
| JMP - Unconditional Jump (to other segment) | |
| direct intersegment | 1110 1010 : unsigned full offset, selector |
| indirect intersegment | 1111 1111 : mod 101 r/m |
| LAHF - Load Flags into AH Register | 1001 1111 |
| LAR - Load Access Rights Byte | |
| from register | 0000 1111 : 0000 0010 : 11 reg1 reg2 |
| from memory | 0000 1111 : 0000 0010 : mod reg r/m |
| LDS - Load Pointer to DS | 1100 0101 : mod ^{A,B} reg r/m |
| LEA - Load Effective Address | 1000 1101 : mod ^A reg r/m |
| LEAVE - High Level Procedure Exit | 1100 1001 |
| LES - Load Pointer to ES | 1100 0100 : mod ^{A,B} reg r/m |
| LFS - Load Pointer to FS | 0000 1111 : 1011 0100 : mod ^A reg r/m |
| LGDT - Load Global Descriptor Table Register | 0000 1111 : 0000 0001 : mod ^A 010 r/m |
| LGS - Load Pointer to GS | 0000 1111 : 1011 0101 : mod ^A reg r/m |
| LIDT - Load Interrupt Descriptor Table Register | 0000 1111 : 0000 0001 : mod ^A 011 r/m |
| LLDT - Load Local Descriptor Table Register | |
| LDTR from register | 0000 1111 : 0000 0000 : 11 010 reg |
| LDTR from memory | 0000 1111 : 0000 0000 : mod 010 r/m |
| LMSW - Load Machine Status Word | |
| from register | 0000 1111 : 0000 0001 : 11 110 reg |
| from memory | 0000 1111 : 0000 0001 : mod 110 r/m |
| LOCK - Assert LOCK# Signal Prefix | 1111 0000 |
| LODS/LODSB/LODSW/LODSD - Load String Operand | 1010 110w |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| LOOP - Loop Count | 1110 0010 : 8-bit displacement |
| LOOPZ/LOOPE - Loop Count while Zero/Equal | 1110 0001 : 8-bit displacement |
| LOOPNZ/LOOPNE - Loop Count while not Zero/Equal | 1110 0000 : 8-bit displacement |
| LSL - Load Segment Limit | |
| from register | 0000 1111 : 0000 0011 : 11 reg1 reg2 |
| from memory | 0000 1111 : 0000 0011 : mod reg r/m |
| LSS - Load Pointer to SS | 0000 1111 : 1011 0010 : mod ^A reg r/m |
| LTR - Load Task Register | |
| from register | 0000 1111 : 0000 0000 : 11 011 reg |
| from memory | 0000 1111 : 0000 0000 : mod 011 r/m |
| MOV - Move Data | |
| register1 to register2 | 1000 100w : 11 reg1 reg2 |
| register2 to register1 | 1000 101w : 11 reg1 reg2 |
| memory to reg | 1000 101w : mod reg r/m |
| reg to memory | 1000 100w : mod reg r/m |
| immediate to register | 1100 011w : 11 000 reg : immediate data |
| immediate to register (alternate encoding) | 1011 w reg : immediate data |
| immediate to memory | 1100 011w : mod 000 r/m : immediate data |
| memory to AL, AX, or EAX | 1010 000w : full displacement |
| AL, AX, or EAX to memory | 1010 001w : full displacement |
| MOV - Move to/from Control Registers | |
| CR0 from register | 0000 1111 : 0010 0010 : 11 000 reg |
| CR2 from register | 0000 1111 : 0010 0010 : 11 010reg |
| CR3 from register | 0000 1111 : 0010 0010 : 11 011 reg |
| CR4 from register | 0000 1111 : 0010 0010 : 11 100 reg |
| register from CR0-CR4 | 0000 1111 : 0010 0000 : 11 eee reg |
| MOV - Move to/from Debug Registers | |
| DR0-DR3 from register | 0000 1111 : 0010 0011 : 11 eee reg |
| DR4-DR5 from register | 0000 1111 : 0010 0011 : 11 eee reg |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| DR6-DR7 from register | 0000 1111 : 0010 0011 : 11 eee reg |
| register from DR6-DR7 | 0000 1111 : 0010 0001 : 11 eee reg |
| register from DR4-DR5 | 0000 1111 : 0010 0001 : 11 eee reg |
| register from DR0-DR3 | 0000 1111 : 0010 0001 : 11 eee reg |
| MOV - Move to/from Segment Registers | |
| register to segment register | 1000 1110 : 11 sreg3 reg |
| register to SS | 1000 1110 : 11 sreg3 reg |
| memory to segment reg | 1000 1110 : mod sreg3 r/m |
| memory to SS | 1000 1110 : mod sreg3 r/m |
| segment register to register | 1000 1100 : 11 sreg3 reg |
| segment register to memory | 1000 1100 : mod sreg3 r/m |
| MOVBE - Move data after swapping bytes | |
| memory to register | 0000 1111 : 0011 1000:1111 0000 : mod reg r/m |
| register to memory | 0000 1111 : 0011 1000:1111 0001 : mod reg r/m |
| MOVS/MOVSb/MOVSsw/MOVSd - Move Data from String to String | 1010 010w |
| MOVsx - Move with Sign-Extend | |
| memory to reg | 0000 1111 : 1011 111w : mod reg r/m |
| MOVzx - Move with Zero-Extend | |
| register2 to register1 | 0000 1111 : 1011 011w : 11 reg1 reg2 |
| memory to register | 0000 1111 : 1011 011w : mod reg r/m |
| MUL - Unsigned Multiply | |
| AL, AX, or EAX with register | 1111 011w : 11 100 reg |
| AL, AX, or EAX with memory | 1111 011w : mod 100 r/m |
| NEG - Two's Complement Negation | |
| register | 1111 011w : 11 011 reg |
| memory | 1111 011w : mod 011 r/m |
| NOP - No Operation | 1001 0000 |
| NOP - Multi-byte No Operation¹ | |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| register | 0000 1111 0001 1111 : 11 000 reg |
| memory | 0000 1111 0001 1111 : mod 000 r/m |
| NOT - One's Complement Negation | |
| register | 1111 011w : 11 010 reg |
| memory | 1111 011w : mod 010 r/m |
| OR - Logical Inclusive OR | |
| register1 to register2 | 0000 100w : 11 reg1 reg2 |
| register2 to register1 | 0000 101w : 11 reg1 reg2 |
| memory to register | 0000 101w : mod reg r/m |
| register to memory | 0000 100w : mod reg r/m |
| immediate to register | 1000 00sw : 11 001 reg : immediate data |
| immediate to AL, AX, or EAX | 0000 110w : immediate data |
| immediate to memory | 1000 00sw : mod 001 r/m : immediate data |
| OUT - Output to Port | |
| fixed port | 1110 011w : port number |
| variable port | 1110 111w |
| OUTS - Output to DX Port | |
| | 0110 111w |
| POP - Pop a Word from the Stack | |
| register | 1000 1111 : 11 000 reg |
| register (alternate encoding) | 0101 1 reg |
| memory | 1000 1111 : mod 000 r/m |
| POP - Pop a Segment Register from the Stack (Note: CS cannot be sreg2 in this usage.) | |
| segment register DS, ES | 000 sreg2 111 |
| segment register SS | 000 sreg2 111 |
| segment register FS, GS | 0000 1111: 10 sreg3 001 |
| POPA/POPAD - Pop All General Registers | |
| | 0110 0001 |
| POPF/POPFD - Pop Stack into FLAGS or EFLAGS Register | |
| | 1001 1101 |
| PUSH - Push Operand onto the Stack | |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|-------------------------------------|
| register | 1111 1111 : 11 110 reg |
| register (alternate encoding) | 0101 0 reg |
| memory | 1111 1111 : mod 110 r/m |
| immediate | 0110 10s0 : immediate data |
| PUSH - Push Segment Register onto the Stack | |
| segment register CS,DS,ES,SS | 000 sreg2 110 |
| segment register FS,GS | 0000 1111 : 10 sreg3 000 |
| PUSHA/PUSHAD - Push All General Registers | 0110 0000 |
| PUSHF/PUSHFD - Push Flags Register onto the Stack | 1001 1100 |
| RCL - Rotate thru Carry Left | |
| register by 1 | 1101 000w : 11 010 reg |
| memory by 1 | 1101 000w : mod 010 r/m |
| register by CL | 1101 001w : 11 010 reg |
| memory by CL | 1101 001w : mod 010 r/m |
| register by immediate count | 1100 000w : 11 010 reg : imm8 data |
| memory by immediate count | 1100 000w : mod 010 r/m : imm8 data |
| RCR - Rotate thru Carry Right | |
| register by 1 | 1101 000w : 11 011 reg |
| memory by 1 | 1101 000w : mod 011 r/m |
| register by CL | 1101 001w : 11 011 reg |
| memory by CL | 1101 001w : mod 011 r/m |
| register by immediate count | 1100 000w : 11 011 reg : imm8 data |
| memory by immediate count | 1100 000w : mod 011 r/m : imm8 data |
| RDMSR - Read from Model-Specific Register | 0000 1111 : 0011 0010 |
| RDPMS - Read Performance Monitoring Counters | 0000 1111 : 0011 0011 |
| RDTSC - Read Time-Stamp Counter | 0000 1111 : 0011 0001 |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|-------------------------------------|
| REP INS - Input String | 1111 0011 : 0110 110w |
| REP LODS - Load String | 1111 0011 : 1010 110w |
| REP MOVS - Move String | 1111 0011 : 1010 010w |
| REP OUTS - Output String | 1111 0011 : 0110 111w |
| REP STOS - Store String | 1111 0011 : 1010 101w |
| REPE CMPS - Compare String | 1111 0011 : 1010 011w |
| REPE SCAS - Scan String | 1111 0011 : 1010 111w |
| REPNE CMPS - Compare String | 1111 0010 : 1010 011w |
| REPNE SCAS - Scan String | 1111 0010 : 1010 111w |
| RET - Return from Procedure (to same segment) | |
| no argument | 1100 0011 |
| adding immediate to SP | 1100 0010 : 16-bit displacement |
| RET - Return from Procedure (to other segment) | |
| intersegment | 1100 1011 |
| adding immediate to SP | 1100 1010 : 16-bit displacement |
| ROL - Rotate Left | |
| register by 1 | 1101 000w : 11 000 reg |
| memory by 1 | 1101 000w : mod 000 r/m |
| register by CL | 1101 001w : 11 000 reg |
| memory by CL | 1101 001w : mod 000 r/m |
| register by immediate count | 1100 000w : 11 000 reg : imm8 data |
| memory by immediate count | 1100 000w : mod 000 r/m : imm8 data |
| ROR - Rotate Right | |
| register by 1 | 1101 000w : 11 001 reg |
| memory by 1 | 1101 000w : mod 001 r/m |
| register by CL | 1101 001w : 11 001 reg |
| memory by CL | 1101 001w : mod 001 r/m |
| register by immediate count | 1100 000w : 11 001 reg : imm8 data |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| memory by immediate count | 1100 000w : mod 001 r/m : imm8 data |
| RSM - Resume from System Management Mode | 0000 1111 : 1010 1010 |
| SAHF - Store AH into Flags | 1001 1110 |
| SAL - Shift Arithmetic Left | same instruction as SHL |
| SAR - Shift Arithmetic Right | |
| register by 1 | 1101 000w : 11 111 reg |
| memory by 1 | 1101 000w : mod 111 r/m |
| register by CL | 1101 001w : 11 111 reg |
| memory by CL | 1101 001w : mod 111 r/m |
| register by immediate count | 1100 000w : 11 111 reg : imm8 data |
| memory by immediate count | 1100 000w : mod 111 r/m : imm8 data |
| SBB - Integer Subtraction with Borrow | |
| register1 to register2 | 0001 100w : 11 reg1 reg2 |
| register2 to register1 | 0001 101w : 11 reg1 reg2 |
| memory to register | 0001 101w : mod reg r/m |
| register to memory | 0001 100w : mod reg r/m |
| immediate to register | 1000 00sw : 11 011 reg : immediate data |
| immediate to AL, AX, or EAX | 0001 110w : immediate data |
| immediate to memory | 1000 00sw : mod 011 r/m : immediate data |
| SCAS/SCASB/SCASw/SCASD - Scan String | 1010 111w |
| SETcc - Byte Set on Condition | |
| register | 0000 1111 : 1001 ttn : 11 000 reg |
| memory | 0000 1111 : 1001 ttn : mod 000 r/m |
| SGDT - Store Global Descriptor Table Register | 0000 1111 : 0000 0001 : mod ^A 000 r/m |
| SHL - Shift Left | |
| register by 1 | 1101 000w : 11 100 reg |
| memory by 1 | 1101 000w : mod 100 r/m |
| register by CL | 1101 001w : 11 100 reg |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| memory by CL | 1101 001w : mod 100 r/m |
| register by immediate count | 1100 000w : 11 100 reg : imm8 data |
| memory by immediate count | 1100 000w : mod 100 r/m : imm8 data |
| SHLD - Double Precision Shift Left | |
| register by immediate count | 0000 1111 : 1010 0100 : 11 reg2 reg1 : imm8 |
| memory by immediate count | 0000 1111 : 1010 0100 : mod reg r/m : imm8 |
| register by CL | 0000 1111 : 1010 0101 : 11 reg2 reg1 |
| memory by CL | 0000 1111 : 1010 0101 : mod reg r/m |
| SHR - Shift Right | |
| register by 1 | 1101 000w : 11 101 reg |
| memory by 1 | 1101 000w : mod 101 r/m |
| register by CL | 1101 001w : 11 101 reg |
| memory by CL | 1101 001w : mod 101 r/m |
| register by immediate count | 1100 000w : 11 101 reg : imm8 data |
| memory by immediate count | 1100 000w : mod 101 r/m : imm8 data |
| SHRD - Double Precision Shift Right | |
| register by immediate count | 0000 1111 : 1010 1100 : 11 reg2 reg1 : imm8 |
| memory by immediate count | 0000 1111 : 1010 1100 : mod reg r/m : imm8 |
| register by CL | 0000 1111 : 1010 1101 : 11 reg2 reg1 |
| memory by CL | 0000 1111 : 1010 1101 : mod reg r/m |
| SIDT - Store Interrupt Descriptor Table Register | 0000 1111 : 0000 0001 : mod ^A 001 r/m |
| SLDT - Store Local Descriptor Table Register | |
| to register | 0000 1111 : 0000 0000 : 11 000 reg |
| to memory | 0000 1111 : 0000 0000 : mod 000 r/m |
| SMSW - Store Machine Status Word | |
| to register | 0000 1111 : 0000 0001 : 11 100 reg |
| to memory | 0000 1111 : 0000 0001 : mod 100 r/m |
| STC - Set Carry Flag | 1111 1001 |
| STD - Set Direction Flag | 1111 1101 |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| STI - Set Interrupt Flag | 1111 1011 |
| STOS/STOSB/STOSW/STOSD - Store String Data | 1010 101w |
| STR - Store Task Register | |
| to register | 0000 1111 : 0000 0000 : 11 001 reg |
| to memory | 0000 1111 : 0000 0000 : mod 001 r/m |
| SUB - Integer Subtraction | |
| register1 to register2 | 0010 100w : 11 reg1 reg2 |
| register2 to register1 | 0010 101w : 11 reg1 reg2 |
| memory to register | 0010 101w : mod reg r/m |
| register to memory | 0010 100w : mod reg r/m |
| immediate to register | 1000 00sw : 11 101 reg : immediate data |
| immediate to AL, AX, or EAX | 0010 110w : immediate data |
| immediate to memory | 1000 00sw : mod 101 r/m : immediate data |
| TEST - Logical Compare | |
| register1 and register2 | 1000 010w : 11 reg1 reg2 |
| memory and register | 1000 010w : mod reg r/m |
| immediate and register | 1111 011w : 11 000 reg : immediate data |
| immediate and AL, AX, or EAX | 1010 100w : immediate data |
| immediate and memory | 1111 011w : mod 000 r/m : immediate data |
| UD2 - Undefined instruction | 0000 FFFF : 0000 1011 |
| VERR - Verify a Segment for Reading | |
| register | 0000 1111 : 0000 0000 : 11 100 reg |
| memory | 0000 1111 : 0000 0000 : mod 100 r/m |
| VERW - Verify a Segment for Writing | |
| register | 0000 1111 : 0000 0000 : 11 101 reg |
| memory | 0000 1111 : 0000 0000 : mod 101 r/m |
| WAIT - Wait | 1001 1011 |
| WBINVD - Writeback and Invalidate Data Cache | 0000 1111 : 0000 1001 |

**Table B-13. General Purpose Instruction Formats and Encodings
for Non-64-Bit Modes (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| WRMSR - Write to Model-Specific Register | 0000 1111 : 0011 0000 |
| XADD - Exchange and Add | |
| register1, register2 | 0000 1111 : 1100 000w : 11 reg2 reg1 |
| memory, reg | 0000 1111 : 1100 000w : mod reg r/m |
| XCHG - Exchange Register/Memory with Register | |
| register1 with register2 | 1000 011w : 11 reg1 reg2 |
| AX or EAX with reg | 1001 0 reg |
| memory with reg | 1000 011w : mod reg r/m |
| XLAT/XLATB - Table Look-up Translation | 1101 0111 |
| XOR - Logical Exclusive OR | |
| register1 to register2 | 0011 000w : 11 reg1 reg2 |
| register2 to register1 | 0011 001w : 11 reg1 reg2 |
| memory to register | 0011 001w : mod reg r/m |
| register to memory | 0011 000w : mod reg r/m |
| immediate to register | 1000 00sw : 11 110 reg : immediate data |
| immediate to AL, AX, or EAX | 0011 010w : immediate data |
| immediate to memory | 1000 00sw : mod 110 r/m : immediate data |
| Prefix Bytes | |
| address size | 0110 0111 |
| LOCK | 1111 0000 |
| operand size | 0110 0110 |
| CS segment override | 0010 1110 |
| DS segment override | 0011 1110 |
| ES segment override | 0010 0110 |
| FS segment override | 0110 0100 |
| GS segment override | 0110 0101 |
| SS segment override | 0011 0110 |

NOTES:

1. The multi-byte NOP instruction does not alter the content of the register and will not issue a memory operation.

B.2.1 General Purpose Instruction Formats and Encodings for 64-Bit Mode

Table B-15 shows machine instruction formats and encodings for general purpose instructions in 64-bit mode.

Table B-14. Special Symbols

| Symbol | Application |
|--------|--|
| S | If the value of REX.W. is 1, it overrides the presence of 66H. |
| w | The value of bit W. in REX is has no effect. |

Table B-15. General Purpose Instruction Formats and Encodings for 64-Bit Mode

| Instruction and Format | Encoding |
|----------------------------------|--|
| ADC - ADD with Carry | |
| register1 to register2 | 0100 0ROB : 0001 000w : 11 reg1 reg2 |
| qwordregister1 to qwordregister2 | 0100 1ROB : 0001 0001 : 11 qwordreg1 qwordreg2 |
| register2 to register1 | 0100 0ROB : 0001 001w : 11 reg1 reg2 |
| qwordregister1 to qwordregister2 | 0100 1ROB : 0001 0011 : 11 qwordreg1 qwordreg2 |
| memory to register | 0100 0RXB : 0001 001w : mod reg r/m |
| memory to qwordregister | 0100 1RXB : 0001 0011 : mod qwordreg r/m |
| register to memory | 0100 0RXB : 0001 000w : mod reg r/m |
| qwordregister to memory | 0100 1RXB : 0001 0001 : mod qwordreg r/m |
| immediate to register | 0100 000B : 1000 00sw : 11 010 reg : immediate |
| immediate to qwordregister | 0100 100B : 1000 0001 : 11 010 qwordreg : imm32 |
| immediate to qwordregister | 0100 1ROB : 1000 0011 : 11 010 qwordreg : imm8 |
| immediate to AL, AX, or EAX | 0001 010w : immediate data |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|----------------------------------|---|
| immediate to RAX | 0100 1000 : 0000 0101 : imm32 |
| immediate to memory | 0100 00XB : 1000 00sw : mod 010 r/m : immediate |
| immediate32 to memory64 | 0100 10XB : 1000 0001 : mod 010 r/m : imm32 |
| immediate8 to memory64 | 0100 10XB : 1000 0031 : mod 010 r/m : imm8 |
| ADD - Add | |
| register1 to register2 | 0100 0ROB : 0000 000w : 11 reg1 reg2 |
| qwordregister1 to qwordregister2 | 0100 1ROB 0000 0000 : 11 qwordreg1 qwordreg2 |
| register2 to register1 | 0100 0ROB : 0000 001w : 11 reg1 reg2 |
| qwordregister1 to qwordregister2 | 0100 1ROB 0000 0010 : 11 qwordreg1 qwordreg2 |
| memory to register | 0100 0RXB : 0000 001w : mod reg r/m |
| memory64 to qwordregister | 0100 1RXB : 0000 0000 : mod qwordreg r/m |
| register to memory | 0100 0RXB : 0000 000w : mod reg r/m |
| qwordregister to memory64 | 0100 1RXB : 0000 0011 : mod qwordreg r/m |
| immediate to register | 0100 0000B : 1000 00sw : 11 000 reg : immediate data |
| immediate32 to qwordregister | 0100 100B : 1000 0001 : 11 010 qwordreg : imm |
| immediate to AL, AX, or EAX | 0000 010w : immediate8 |
| immediate to RAX | 0100 1000 : 0000 0101 : imm32 |
| immediate to memory | 0100 00XB : 1000 00sw : mod 000 r/m : immediate |
| immediate32 to memory64 | 0100 10XB : 1000 0001 : mod 010 r/m : imm32 |
| immediate8 to memory64 | 0100 10XB : 1000 0011 : mod 010 r/m : imm8 |
| AND - Logical AND | |
| register1 to register2 | 0100 0ROB 0010 000w : 11 reg1 reg2 |
| qwordregister1 to qwordregister2 | 0100 1ROB 0010 0001 : 11 qwordreg1 qwordreg2 |
| register2 to register1 | 0100 0ROB 0010 001w : 11 reg1 reg2 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--------------------------------|---|
| register1 to register2 | 0100 1R0B 0010 0011 : 11 qwordreg1 qwordreg2 |
| memory to register | 0100 0RXB 0010 001w : mod reg r/m |
| memory64 to qwordregister | 0100 1RXB : 0010 0011 : mod qwordreg r/m |
| register to memory | 0100 0RXB : 0010 000w : mod reg r/m |
| qwordregister to memory64 | 0100 1RXB : 0010 0001 : mod qwordreg r/m |
| immediate to register | 0100 000B : 1000 00sw : 11 100 reg : immediate |
| immediate32 to qwordregister | 0100 100B 1000 0001 : 11 100 qwordreg : imm32 |
| immediate to AL, AX, or EAX | 0010 010w : immediate |
| immediate32 to RAX | 0100 1000 0010 1001 : imm32 |
| immediate to memory | 0100 00XB : 1000 00sw : mod 100 r/m : immediate |
| immediate32 to memory64 | 0100 10XB : 1000 0001 : mod 100 r/m : immediate32 |
| immediate8 to memory64 | 0100 10XB : 1000 0011 : mod 100 r/m : imm8 |
| BSF - Bit Scan Forward | |
| register1, register2 | 0100 0R0B 0000 1111 : 1011 1100 : 11 reg1 reg2 |
| qwordregister1, qwordregister2 | 0100 1R0B 0000 1111 : 1011 1100 : 11 qwordreg1 qwordreg2 |
| memory, register | 0100 0RXB 0000 1111 : 1011 1100 : mod reg r/m |
| memory64, qwordregister | 0100 1RXB 0000 1111 : 1011 1100 : mod qwordreg r/m |
| BSR - Bit Scan Reverse | |
| register1, register2 | 0100 0R0B 0000 1111 : 1011 1101 : 11 reg1 reg2 |
| qwordregister1, qwordregister2 | 0100 1R0B 0000 1111 : 1011 1101 : 11 qwordreg1 qwordreg2 |
| memory, register | 0100 0RXB 0000 1111 : 1011 1101 : mod reg r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--------------------------------------|--|
| memory64, qwordregister | 0100 1RXB 0000 1111 : 1011 1101 : mod qwordreg r/m |
| BSWAP - Byte Swap | 0000 1111 : 1100 1 reg |
| BSWAP - Byte Swap | 0100 100B 0000 1111 : 1100 1 qwordreg |
| BT - Bit Test | |
| register, immediate | 0100 000B 0000 1111 : 1011 1010 : 11 100 reg: imm8 |
| qwordregister, immediate8 | 0100 100B 1111 : 1011 1010 : 11 100 qwordreg: imm8 data |
| memory, immediate | 0100 00XB 0000 1111 : 1011 1010 : mod 100 r/m : imm8 |
| memory64, immediate8 | 0100 10XB 0000 1111 : 1011 1010 : mod 100 r/m : imm8 data |
| register1, register2 | 0100 0ROB 0000 1111 : 1010 0011 : 11 reg2 reg1 |
| qwordregister1, qwordregister2 | 0100 1ROB 0000 1111 : 1010 0011 : 11 qwordreg2 qwordreg1 |
| memory, reg | 0100 0RXB 0000 1111 : 1010 0011 : mod reg r/m |
| memory, qwordreg | 0100 1RXB 0000 1111 : 1010 0011 : mod qwordreg r/m |
| BTC - Bit Test and Complement | |
| register, immediate | 0100 000B 0000 1111 : 1011 1010 : 11 111 reg: imm8 |
| qwordregister, immediate8 | 0100 100B 0000 1111 : 1011 1010 : 11 111 qwordreg: imm8 |
| memory, immediate | 0100 00XB 0000 1111 : 1011 1010 : mod 111 r/m : imm8 |
| memory64, immediate8 | 0100 10XB 0000 1111 : 1011 1010 : mod 111 r/m : imm8 |
| register1, register2 | 0100 0ROB 0000 1111 : 1011 1011 : 11 reg2 reg1 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---------------------------------|---|
| qwordregister1, qwordregister2 | 0100 1R0B 0000 1111 : 1011 1011 : 11 qwordreg2 qwordreg1 |
| memory, register | 0100 0RXB 0000 1111 : 1011 1011 : mod reg r/m |
| memory, qwordreg | 0100 1RXB 0000 1111 : 1011 1011 : mod qwordreg r/m |
| BTR - Bit Test and Reset | |
| register, immediate | 0100 000B 0000 1111 : 1011 1010 : 11 110 reg: imm8 |
| qwordregister, immediate8 | 0100 100B 0000 1111 : 1011 1010 : 11 110 qwordreg: imm8 |
| memory, immediate | 0100 00XB 0000 1111 : 1011 1010 : mod 110 r/m : imm8 |
| memory64, immediate8 | 0100 10XB 0000 1111 : 1011 1010 : mod 110 r/m : imm8 |
| register1, register2 | 0100 0R0B 0000 1111 : 1011 0011 : 11 reg2 reg1 |
| qwordregister1, qwordregister2 | 0100 1R0B 0000 1111 : 1011 0011 : 11 qwordreg2 qwordreg1 |
| memory, register | 0100 0RXB 0000 1111 : 1011 0011 : mod reg r/m |
| memory64, qwordreg | 0100 1RXB 0000 1111 : 1011 0011 : mod qwordreg r/m |
| BTS - Bit Test and Set | |
| register, immediate | 0100 000B 0000 1111 : 1011 1010 : 11 101 reg: imm8 |
| qwordregister, immediate8 | 0100 100B 0000 1111 : 1011 1010 : 11 101 qwordreg: imm8 |
| memory, immediate | 0100 00XB 0000 1111 : 1011 1010 : mod 101 r/m : imm8 |
| memory64, immediate8 | 0100 10XB 0000 1111 : 1011 1010 : mod 101 r/m : imm8 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| register1, register2 | 0100 0ROB 0000 1111 : 1010 1011 : 11 reg2 reg1 |
| qwordregister1, qwordregister2 | 0100 1ROB 0000 1111 : 1010 1011 : 11 qwordreg2 qwordreg1 |
| memory, register | 0100 0RXB 0000 1111 : 1010 1011 : mod reg r/m |
| memory64, qwordreg | 0100 1RXB 0000 1111 : 1010 1011 : mod qwordreg r/m |
| CALL - Call Procedure (in same segment) | |
| direct | 1110 1000 : displacement32 |
| register indirect | 0100 WRO0 ^w 1111 1111 : 11 010 reg |
| memory indirect | 0100 W0XB ^w 1111 1111 : mod 010 r/m |
| CALL - Call Procedure (in other segment) | |
| indirect | 1111 1111 : mod 011 r/m |
| indirect | 0100 10XB 0100 1000 1111 1111 : mod 011 r/m |
| CBW - Convert Byte to Word | 1001 1000 |
| CDQ - Convert Doubleword to Qword+ | 1001 1001 |
| CDQE - RAX, Sign-Extend of EAX | 0100 1000 1001 1001 |
| CLC - Clear Carry Flag | 1111 1000 |
| CLD - Clear Direction Flag | 1111 1100 |
| CLI - Clear Interrupt Flag | 1111 1010 |
| CLTS - Clear Task-Switched Flag in CRO | 0000 1111 : 0000 0110 |
| CMC - Complement Carry Flag | 1111 0101 |
| CMP - Compare Two Operands | |
| register1 with register2 | 0100 0ROB 0011 100w : 11 reg1 reg2 |
| qwordregister1 with qwordregister2 | 0100 1ROB 0011 1001 : 11 qwordreg1 qwordreg2 |
| register2 with register1 | 0100 0ROB 0011 101w : 11 reg1 reg2 |
| qwordregister2 with qwordregister1 | 0100 1ROB 0011 101w : 11 qwordreg1 qwordreg2 |
| memory with register | 0100 0RXB 0011 100w : mod reg r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| memory64 with qwordregister | 0100 1RXB 0011 1001 : mod qwordreg r/m |
| register with memory | 0100 0RXB 0011 101w : mod reg r/m |
| qwordregister with memory64 | 0100 1RXB 0011 101w1 : mod qwordreg r/m |
| immediate with register | 0100 000B 1000 00sw : 11 111 reg : imm |
| immediate32 with qwordregister | 0100 100B 1000 0001 : 11 111 qwordreg : imm64 |
| immediate with AL, AX, or EAX | 0011 110w : imm |
| immediate32 with RAX | 0100 1000 0011 1101 : imm32 |
| immediate with memory | 0100 00XB 1000 00sw : mod 111 r/m : imm |
| immediate32 with memory64 | 0100 1RXB 1000 0001 : mod 111 r/m : imm64 |
| immediate8 with memory64 | 0100 1RXB 1000 0011 : mod 111 r/m : imm8 |
| CMPS/CMPSB/CMPSW/CMPSD/CMPSQ - Compare String Operands | |
| compare string operands [X at DS:(E)SI with Y at ES:(E)DI] | 1010 011w |
| qword at address RSI with qword at address RDI | 0100 1000 1010 0111 |
| CMPXCHG - Compare and Exchange | |
| register1, register2 | 0000 1111 : 1011 000w : 11 reg2 reg1 |
| byteregister1, byteregister2 | 0100 000B 0000 1111 : 1011 0000 : 11 bytereg2 reg1 |
| qwordregister1, qwordregister2 | 0100 100B 0000 1111 : 1011 0001 : 11 qwordreg2 reg1 |
| memory, register | 0000 1111 : 1011 000w : mod reg r/m |
| memory8, byteregister | 0100 00XB 0000 1111 : 1011 0000 : mod bytereg r/m |
| memory64, qwordregister | 0100 10XB 0000 1111 : 1011 0001 : mod qwordreg r/m |
| CPUID - CPU Identification | 0000 1111 : 1010 0010 |
| CQO - Sign-Extend RAX | 0100 1000 1001 1001 |
| CWD - Convert Word to Doubleword | 1001 1001 |
| CWDE - Convert Word to Doubleword | 1001 1000 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| DEC - Decrement by 1 | |
| register | 0100 000B 1111 111w : 11 001 reg |
| qwordregister | 0100 100B 1111 1111 : 11 001 qwordreg |
| memory | 0100 00XB 1111 111w : mod 001 r/m |
| memory64 | 0100 10XB 1111 1111 : mod 001 r/m |
| DIV - Unsigned Divide | |
| AL, AX, or EAX by register | 0100 000B 1111 011w : 11 110 reg |
| Divide RDX:RAX by qwordregister | 0100 100B 1111 0111 : 11 110 qwordreg |
| AL, AX, or EAX by memory | 0100 00XB 1111 011w : mod 110 r/m |
| Divide RDX:RAX by memory64 | 0100 10XB 1111 0111 : mod 110 r/m |
| ENTER - Make Stack Frame for High Level Procedure | 1100 1000 : 16-bit displacement : 8-bit level (L) |
| HLT - Halt | 1111 0100 |
| IDIV - Signed Divide | |
| AL, AX, or EAX by register | 0100 000B 1111 011w : 11 111 reg |
| RDX:RAX by qwordregister | 0100 100B 1111 0111 : 11 111 qwordreg |
| AL, AX, or EAX by memory | 0100 00XB 1111 011w : mod 111 r/m |
| RDX:RAX by memory64 | 0100 10XB 1111 0111 : mod 111 r/m |
| IMUL - Signed Multiply | |
| AL, AX, or EAX with register | 0100 000B 1111 011w : 11 101 reg |
| RDX:RAX <- RAX with qwordregister | 0100 100B 1111 0111 : 11 101 qwordreg |
| AL, AX, or EAX with memory | 0100 00XB 1111 011w : mod 101 r/m |
| RDX:RAX <- RAX with memory64 | 0100 10XB 1111 0111 : mod 101 r/m |
| register1 with register2 | 0000 1111 : 1010 1111 : 11 : reg1 reg2 |
| qwordregister1 <- qwordregister1 with qwordregister2 | 0100 1R0B 0000 1111 : 1010 1111 : 11 : qwordreg1 qwordreg2 |
| register with memory | 0100 0RXB 0000 1111 : 1010 1111 : mod reg r/m |
| qwordregister <- qwordregister withmemory64 | 0100 1RXB 0000 1111 : 1010 1111 : mod qwordreg r/m |
| register1 with immediate to register2 | 0100 0R0B 0110 10s1 : 11 reg1 reg2 : imm |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| qwordregister1 <- qwordregister2 with sign-extended immediate8 | 0100 1R0B 0110 1011 : 11 qwordreg1 qwordreg2 : imm8 |
| qwordregister1 <- qwordregister2 with immediate32 | 0100 1R0B 0110 1001 : 11 qwordreg1 qwordreg2 : imm32 |
| memory with immediate to register | 0100 0RXB 0110 10s1 : mod reg r/m : imm |
| qwordregister <- memory64 with sign-extended immediate8 | 0100 1RXB 0110 1011 : mod qwordreg r/m : imm8 |
| qwordregister <- memory64 with immediate32 | 0100 1RXB 0110 1001 : mod qwordreg r/m : imm32 |
| IN - Input From Port | |
| fixed port | 1110 010w : port number |
| variable port | 1110 110w |
| INC - Increment by 1 | |
| reg | 0100 000B 1111 111w : 11 000 reg |
| qwordreg | 0100 100B 1111 1111 : 11 000 qwordreg |
| memory | 0100 00XB 1111 111w : mod 000 r/m |
| memory64 | 0100 10XB 1111 1111 : mod 000 r/m |
| INS - Input from DX Port | 0110 110w |
| INT n - Interrupt Type n | 1100 1101 : type |
| INT - Single-Step Interrupt 3 | 1100 1100 |
| INTO - Interrupt 4 on Overflow | 1100 1110 |
| INVD - Invalidate Cache | 0000 1111 : 0000 1000 |
| INVLPG - Invalidate TLB Entry | 0000 1111 : 0000 0001 : mod 111 r/m |
| IRETO - Interrupt Return | 1100 1111 |
| Jcc - Jump if Condition is Met | |
| 8-bit displacement | 0111 tttt : 8-bit displacement |
| displacements (excluding 16-bit relative offsets) | 0000 1111 : 1000 tttt : displacement32 |
| JCXZ/JECXZ - Jump on CX/ECX Zero | |
| Address-size prefix differentiates JCXZ and JECXZ | 1110 0011 : 8-bit displacement |
| JMP - Unconditional Jump (to same segment) | |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| short | 1110 1011 : 8-bit displacement |
| direct | 1110 1001 : displacement32 |
| register indirect | 0100 W00B ^W : 1111 1111 : 11 100 reg |
| memory indirect | 0100 W0XB ^W : 1111 1111 : mod 100 r/m |
| JMP - Unconditional Jump (to other segment) | |
| indirect intersegment | 0100 00XB : 1111 1111 : mod 101 r/m |
| 64-bit indirect intersegment | 0100 10XB : 1111 1111 : mod 101 r/m |
| LAR - Load Access Rights Byte | |
| from register | 0100 0ROB : 0000 1111 : 0000 0010 : 11 reg1 reg2 |
| from dwordregister to qwordregister, masked by 00FxFF00H | 0100 WROB : 0000 1111 : 0000 0010 : 11 qwordreg1 dwordreg2 |
| from memory | 0100 0RXB : 0000 1111 : 0000 0010 : mod reg r/m |
| from memory32 to qwordregister, masked by 00FxFF00H | 0100 WRXB 0000 1111 : 0000 0010 : mod r/m |
| LEA - Load Effective Address | |
| in wordregister/dwordregister | 0100 0RXB : 1000 1101 : mod ^A reg r/m |
| in qwordregister | 0100 1RXB : 1000 1101 : mod ^A qwordreg r/m |
| LEAVE - High Level Procedure Exit | |
| 1100 1001 | |
| LFS - Load Pointer to FS | |
| FS:r16/r32 with far pointer from memory | 0100 0RXB : 0000 1111 : 1011 0100 : mod ^A reg r/m |
| FS:r64 with far pointer from memory | 0100 1RXB : 0000 1111 : 1011 0100 : mod ^A qwordreg r/m |
| LGDT - Load Global Descriptor Table Register | |
| | 0100 10XB : 0000 1111 : 0000 0001 : mod ^A 010 r/m |
| LGS - Load Pointer to GS | |
| GS:r16/r32 with far pointer from memory | 0100 0RXB : 0000 1111 : 1011 0101 : mod ^A reg r/m |
| GS:r64 with far pointer from memory | 0100 1RXB : 0000 1111 : 1011 0101 : mod ^A qwordreg r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| LIDT - Load Interrupt Descriptor Table Register | 0100 10XB : 0000 1111 : 0000 0001 : mod ^A 011 r/m |
| LLDT - Load Local Descriptor Table Register | |
| LDTR from register | 0100 000B : 0000 1111 : 0000 0000 : 11 010 reg |
| LDTR from memory | 0100 00XB : 0000 1111 : 0000 0000 : mod 010 r/m |
| LMSW - Load Machine Status Word | |
| from register | 0100 000B : 0000 1111 : 0000 0001 : 11 110 reg |
| from memory | 0100 00XB : 0000 1111 : 0000 0001 : mod 110 r/m |
| LOCK - Assert LOCK# Signal Prefix | 1111 0000 |
| LODS/LODSB/LODSW/LODSD/LODSQ - Load String Operand | |
| at DS:(E)SI to AL/EAX/EAX | 1010 110w |
| at (R)SI to RAX | 0100 1000 1010 1101 |
| LOOP - Loop Count | |
| if count != 0, 8-bit displacement | 1110 0010 |
| if count !=0, RIP + 8-bit displacement sign-extended to 64-bits | 0100 1000 1110 0010 |
| LOOPE - Loop Count while Zero/Equal | |
| if count != 0 & ZF = 1, 8-bit displacement | 1110 0001 |
| if count !=0 & ZF = 1, RIP + 8-bit displacement sign-extended to 64-bits | 0100 1000 1110 0001 |
| LOOPNE/LOOPNZ - Loop Count while not Zero/Equal | |
| if count != 0 & ZF = 0, 8-bit displacement | 1110 0000 |
| if count !=0 & ZF = 0, RIP + 8-bit displacement sign-extended to 64-bits | 0100 1000 1110 0000 |
| LSL - Load Segment Limit | |
| from register | 0000 1111 : 0000 0011 : 11 reg1 reg2 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| from qwordregister | 0100 1R00 0000 1111 : 0000 0011 : 11 qwordreg1 reg2 |
| from memory16 | 0000 1111 : 0000 0011 : mod reg r/m |
| from memory64 | 0100 1RXB 0000 1111 : 0000 0011 : mod qwordreg r/m |
| LSS - Load Pointer to SS | |
| SS:r16/r32 with far pointer from memory | 0100 0RXB : 0000 1111 : 1011 0010 : mod ^A reg r/m |
| SS:r64 with far pointer from memory | 0100 1WXB : 0000 1111 : 1011 0010 : mod ^A qwordreg r/m |
| LTR - Load Task Register | |
| from register | 0100 0R00 : 0000 1111 : 0000 0000 : 11 011 reg |
| from memory | 0100 00XB : 0000 1111 : 0000 0000 : mod 011 r/m |
| MOV - Move Data | |
| register1 to register2 | 0100 0R0B : 1000 100w : 11 reg1 reg2 |
| qwordregister1 to qwordregister2 | 0100 1R0B 1000 1001 : 11 qwordreg1 qwordreg2 |
| register2 to register1 | 0100 0R0B : 1000 101w : 11 reg1 reg2 |
| qwordregister2 to qwordregister1 | 0100 1R0B 1000 1011 : 11 qwordreg1 qwordreg2 |
| memory to reg | 0100 0RXB : 1000 101w : mod reg r/m |
| memory64 to qwordregister | 0100 1RXB 1000 1011 : mod qwordreg r/m |
| reg to memory | 0100 0RXB : 1000 100w : mod reg r/m |
| qwordregister to memory64 | 0100 1RXB 1000 1001 : mod qwordreg r/m |
| immediate to register | 0100 000B : 1100 011w : 11 000 reg : imm |
| immediate32 to qwordregister (zero extend) | 0100 100B 1100 0111 : 11 000 qwordreg : imm32 |
| immediate to register (alternate encoding) | 0100 000B : 1011 w reg : imm |
| immediate64 to qwordregister (alternate encoding) | 0100 100B 1011 1000 reg : imm64 |
| immediate to memory | 0100 00XB : 1100 011w : mod 000 r/m : imm |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| immediate32 to memory64 (zero extend) | 0100 10XB 1100 0111 : mod 000 r/m : imm32 |
| memory to AL, AX, or EAX | 0100 0000 : 1010 000w : displacement |
| memory64 to RAX | 0100 1000 1010 0001 : displacement64 |
| AL, AX, or EAX to memory | 0100 0000 : 1010 001w : displacement |
| RAX to memory64 | 0100 1000 1010 0011 : displacement64 |
| MOV - Move to/from Control Registers | |
| CR0-CR4 from register | 0100 0R0B : 0000 1111 : 0010 0010 : 11 eee reg (eee = CR#) |
| CRx from qwordregister | 0100 1R0B : 0000 1111 : 0010 0010 : 11 eee qwordreg (Reee = CR#) |
| register from CR0-CR4 | 0100 0R0B : 0000 1111 : 0010 0000 : 11 eee reg (eee = CR#) |
| qwordregister from CRx | 0100 1R0B 0000 1111 : 0010 0000 : 11 eee qwordreg (Reee = CR#) |
| MOV - Move to/from Debug Registers | |
| DR0-DR7 from register | 0000 1111 : 0010 0011 : 11 eee reg (eee = DR#) |
| DR0-DR7 from quadregister | 0100 100B 0000 1111 : 0010 0011 : 11 eee reg (eee = DR#) |
| register from DR0-DR7 | 0000 1111 : 0010 0001 : 11 eee reg (eee = DR#) |
| quadregister from DR0-DR7 | 0100 100B 0000 1111 : 0010 0001 : 11 eee quadreg (eee = DR#) |
| MOV - Move to/from Segment Registers | |
| register to segment register | 0100 W00B ^W : 1000 1110 : 11 sreg reg |
| register to SS | 0100 000B : 1000 1110 : 11 sreg reg |
| memory to segment register | 0100 00XB : 1000 1110 : mod sreg r/m |
| memory64 to segment register (lower 16 bits) | 0100 10XB 1000 1110 : mod sreg r/m |
| memory to SS | 0100 00XB : 1000 1110 : mod sreg r/m |
| segment register to register | 0100 000B : 1000 1100 : 11 sreg reg |
| segment register to qwordregister (zero extended) | 0100 100B 1000 1100 : 11 sreg qwordreg |
| segment register to memory | 0100 00XB : 1000 1100 : mod sreg r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| segment register to memory64 (zero extended) | 0100 10XB 1000 1100 : mod sreg3 r/m |
| MOVBE - Move data after swapping bytes | |
| memory to register | 0100 0RXB : 0000 1111 : 0011 1000:1111 0000 : mod reg r/m |
| memory64 to qwordregister | 0100 1RXB : 0000 1111 : 0011 1000:1111 0000 : mod reg r/m |
| register to memory | 0100 0RXB : 0000 1111 : 0011 1000:1111 0001 : mod reg r/m |
| qwordregister to memory64 | 0100 1RXB : 0000 1111 : 0011 1000:1111 0001 : mod reg r/m |
| MOVS/MOVSb/MOVSsw/MOVSD/MOVSq - Move Data from String to String | |
| Move data from string to string | 1010 010w |
| Move data from string to string (qword) | 0100 1000 1010 0101 |
| MOVsx/MOVsxd - Move with Sign-Extend | |
| register2 to register1 | 0100 0ROB : 0000 1111 : 1011 111w : 11 reg1 reg2 |
| byteregister2 to qwordregister1 (sign-extend) | 0100 1ROB 0000 1111 : 1011 1110 : 11 quadreg1 bytereg2 |
| wordregister2 to qwordregister1 | 0100 1ROB 0000 1111 : 1011 1111 : 11 quadreg1 wordreg2 |
| dwordregister2 to qwordregister1 | 0100 1ROB 0110 0011 : 11 quadreg1 dwordreg2 |
| memory to register | 0100 0RXB : 0000 1111 : 1011 111w : mod reg r/m |
| memory8 to qwordregister (sign-extend) | 0100 1RXB 0000 1111 : 1011 1110 : mod qwordreg r/m |
| memory16 to qwordregister | 0100 1RXB 0000 1111 : 1011 1111 : mod qwordreg r/m |
| memory32 to qwordregister | 0100 1RXB 0110 0011 : mod qwordreg r/m |
| MOVZX - Move with Zero-Extend | |
| register2 to register1 | 0100 0ROB : 0000 1111 : 1011 011w : 11 reg1 reg2 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| dwordregister2 to qwordregister1 | 0100 1R0B 0000 1111 : 1011 0111 : 11 qwordreg1 dwordreg2 |
| memory to register | 0100 0RXB : 0000 1111 : 1011 011w : mod reg r/m |
| memory32 to qwordregister | 0100 1RXB 0000 1111 : 1011 0111 : mod qwordreg r/m |
| MUL - Unsigned Multiply | |
| AL, AX, or EAX with register | 0100 000B : 1111 011w : 11 100 reg |
| RAX with qwordregister (to RDX:RAX) | 0100 100B 1111 0111 : 11 100 qwordreg |
| AL, AX, or EAX with memory | 0100 00XB 1111 011w : mod 100 r/m |
| RAX with memory64 (to RDX:RAX) | 0100 10XB 1111 0111 : mod 100 r/m |
| NEG - Two's Complement Negation | |
| register | 0100 000B : 1111 011w : 11 011 reg |
| qwordregister | 0100 100B 1111 0111 : 11 011 qwordreg |
| memory | 0100 00XB : 1111 011w : mod 011 r/m |
| memory64 | 0100 10XB 1111 0111 : mod 011 r/m |
| NOP - No Operation | 1001 0000 |
| NOT - One's Complement Negation | |
| register | 0100 000B : 1111 011w : 11 010 reg |
| qwordregister | 0100 000B 1111 0111 : 11 010 qwordreg |
| memory | 0100 00XB : 1111 011w : mod 010 r/m |
| memory64 | 0100 1RXB 1111 0111 : mod 010 r/m |
| OR - Logical Inclusive OR | |
| register1 to register2 | 0000 100w : 11 reg1 reg2 |
| byteregister1 to byteregister2 | 0100 0R0B 0000 1000 : 11 bytereg1 bytereg2 |
| qwordregister1 to qwordregister2 | 0100 1R0B 0000 1001 : 11 qwordreg1 qwordreg2 |
| register2 to register1 | 0000 101w : 11 reg1 reg2 |
| byteregister2 to byteregister1 | 0100 0R0B 0000 1010 : 11 bytereg1 bytereg2 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| qwordregister2 to qwordregister1 | 0100 0ROB 0000 1011 : 11 qwordreg1 qwordreg2 |
| memory to register | 0000 101w : mod reg r/m |
| memory8 to byteregister | 0100 0RXB 0000 1010 : mod bytereg r/m |
| memory8 to qwordregister | 0100 0RXB 0000 1011 : mod qwordreg r/m |
| register to memory | 0000 100w : mod reg r/m |
| byteregister to memory8 | 0100 0RXB 0000 1000 : mod bytereg r/m |
| qwordregister to memory64 | 0100 1RXB 0000 1001 : mod qwordreg r/m |
| immediate to register | 1000 00sw : 11 001 reg : imm |
| immediate8 to byteregister | 0100 000B 1000 0000 : 11 001 bytereg : imm8 |
| immediate32 to qwordregister | 0100 000B 1000 0001 : 11 001 qwordreg : imm32 |
| immediate8 to qwordregister | 0100 000B 1000 0011 : 11 001 qwordreg : imm8 |
| immediate to AL, AX, or EAX | 0000 110w : imm |
| immediate64 to RAX | 0100 1000 0000 1101 : imm64 |
| immediate to memory | 1000 00sw : mod 001 r/m : imm |
| immediate8 to memory8 | 0100 00XB 1000 0000 : mod 001 r/m : imm8 |
| immediate32 to memory64 | 0100 00XB 1000 0001 : mod 001 r/m : imm32 |
| immediate8 to memory64 | 0100 00XB 1000 0011 : mod 001 r/m : imm8 |
| OUT - Output to Port | |
| fixed port | 1110 011w : port number |
| variable port | 1110 111w |
| OUTS - Output to DX Port | |
| output to DX Port | 0110 111w |
| POP - Pop a Value from the Stack | |
| wordregister | 0101 0101 : 0100 000B : 1000 1111 : 11 000 reg16 |
| qwordregister | 0100 W00B ^S : 1000 1111 : 11 000 reg64 |
| wordregister (alternate encoding) | 0101 0101 : 0100 000B : 0101 1 reg16 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| qwordregister (alternate encoding) | 0100 W00B : 0101 1 reg64 |
| memory64 | 0100 W0XB ^S : 1000 1111 : mod 000 r/m |
| memory16 | 0101 0101 : 0100 00XB 1000 1111 : mod 000 r/m |
| POP - Pop a Segment Register from the Stack (Note: CS cannot be sreg2 in this usage.) | |
| segment register FS, GS | 0000 1111: 10 sreg3 001 |
| POPF/POPFQ - Pop Stack into FLAGS/RFLAGS Register | |
| pop stack to FLAGS register | 0101 0101 : 1001 1101 |
| pop Stack to RFLAGS register | 0100 1000 1001 1101 |
| PUSH - Push Operand onto the Stack | |
| wordregister | 0101 0101 : 0100 000B : 1111 1111 : 11 110 reg16 |
| qwordregister | 0100 W00B ^S : 1111 1111 : 11 110 reg64 |
| wordregister (alternate encoding) | 0101 0101 : 0100 000B : 0101 0 reg16 |
| qwordregister (alternate encoding) | 0100 W00B ^S : 0101 0 reg64 |
| memory16 | 0101 0101 : 0100 000B : 1111 1111 : mod 110 r/m |
| memory64 | 0100 W00B ^S : 1111 1111 : mod 110 r/m |
| immediate8 | 0110 1010 : imm8 |
| immediate16 | 0101 0101 : 0110 1000 : imm16 |
| immediate64 | 0110 1000 : imm64 |
| PUSH - Push Segment Register onto the Stack | |
| segment register FS,GS | 0000 1111: 10 sreg3 000 |
| PUSHF/PUSHFD - Push Flags Register onto the Stack | 1001 1100 |
| RCL - Rotate thru Carry Left | |
| register by 1 | 0100 000B : 1101 000w : 11 010 reg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 010 qwordreg |
| memory by 1 | 0100 00XB : 1101 000w : mod 010 r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| memory64 by 1 | 0100 10XB 1101 0001 : mod 010 r/m |
| register by CL | 0100 000B : 1101 001w : 11 010 reg |
| qwordregister by CL | 0100 100B 1101 0011 : 11 010 qwordreg |
| memory by CL | 0100 00XB : 1101 001w : mod 010 r/m |
| memory64 by CL | 0100 10XB 1101 0011 : mod 010 r/m |
| register by immediate count | 0100 000B : 1100 000w : 11 010 reg : imm |
| qwordregister by immediate count | 0100 100B 1100 0001 : 11 010 qwordreg : imm8 |
| memory by immediate count | 0100 00XB : 1100 000w : mod 010 r/m : imm |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 010 r/m : imm8 |
| RCR - Rotate thru Carry Right | |
| register by 1 | 0100 000B : 1101 000w : 11 011 reg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 011 qwordreg |
| memory by 1 | 0100 00XB : 1101 000w : mod 011 r/m |
| memory64 by 1 | 0100 10XB 1101 0001 : mod 011 r/m |
| register by CL | 0100 000B : 1101 001w : 11 011 reg |
| qwordregister by CL | 0100 000B 1101 0010 : 11 011 qwordreg |
| memory by CL | 0100 00XB : 1101 001w : mod 011 r/m |
| memory64 by CL | 0100 10XB 1101 0011 : mod 011 r/m |
| register by immediate count | 0100 000B : 1100 000w : 11 011 reg : imm8 |
| qwordregister by immediate count | 0100 100B 1100 0001 : 11 011 qwordreg : imm8 |
| memory by immediate count | 0100 00XB : 1100 000w : mod 011 r/m : imm8 |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 011 r/m : imm8 |
| RDMSR - Read from Model-Specific Register | |
| load ECX-specified register into EDX:EAX | 0000 1111 : 0011 0010 |
| RDPNC - Read Performance Monitoring Counters | |
| load ECX-specified performance counter into EDX:EAX | 0000 1111 : 0011 0011 |
| RDTSR - Read Time-Stamp Counter | |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|---------------------------------------|
| read time-stamp counter into EDX:EAX | 0000 1111 : 0011 0001 |
| REP INS - Input String | |
| REP LODS - Load String | |
| REP MOVS - Move String | |
| REP OUTS - Output String | |
| REP STOS - Store String | |
| REPE CMPS - Compare String | |
| REPE SCAS - Scan String | |
| REPNE CMPS - Compare String | |
| REPNE SCAS - Scan String | |
| RET - Return from Procedure (to same segment) | |
| no argument | 1100 0011 |
| adding immediate to SP | 1100 0010 : 16-bit displacement |
| RET - Return from Procedure (to other segment) | |
| intersegment | 1100 1011 |
| adding immediate to SP | 1100 1010 : 16-bit displacement |
| ROL - Rotate Left | |
| register by 1 | 0100 000B 1101 000w : 11 000 reg |
| byteregister by 1 | 0100 000B 1101 0000 : 11 000 bytereg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 000 qwordreg |
| memory by 1 | 0100 00XB 1101 000w : mod 000 r/m |
| memory8 by 1 | 0100 00XB 1101 0000 : mod 000 r/m |
| memory64 by 1 | 0100 10XB 1101 0001 : mod 000 r/m |
| register by CL | 0100 000B 1101 001w : 11 000 reg |
| byteregister by CL | 0100 000B 1101 0010 : 11 000 bytereg |
| qwordregister by CL | 0100 100B 1101 0011 : 11 000 qwordreg |
| memory by CL | 0100 00XB 1101 001w : mod 000 r/m |
| memory8 by CL | 0100 00XB 1101 0010 : mod 000 r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|----------------------------------|---|
| memory64 by CL | 0100 10XB 1101 0011 : mod 000 r/m |
| register by immediate count | 1100 000w : 11 000 reg : imm8 |
| byteregister by immediate count | 0100 000B 1100 0000 : 11 000 bytereg : imm8 |
| qwordregister by immediate count | 0100 100B 1100 0001 : 11 000 bytereg : imm8 |
| memory by immediate count | 1100 000w : mod 000 r/m : imm8 |
| memory8 by immediate count | 0100 00XB 1100 0000 : mod 000 r/m : imm8 |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 000 r/m : imm8 |
| ROR - Rotate Right | |
| register by 1 | 0100 000B 1101 000w : 11 001 reg |
| byteregister by 1 | 0100 000B 1101 0000 : 11 001 bytereg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 001 qwordreg |
| memory by 1 | 0100 00XB 1101 000w : mod 001 r/m |
| memory8 by 1 | 0100 00XB 1101 0000 : mod 001 r/m |
| memory64 by 1 | 0100 10XB 1101 0001 : mod 001 r/m |
| register by CL | 0100 000B 1101 001w : 11 001 reg |
| byteregister by CL | 0100 000B 1101 0010 : 11 001 bytereg |
| qwordregister by CL | 0100 100B 1101 0011 : 11 001 qwordreg |
| memory by CL | 0100 00XB 1101 001w : mod 001 r/m |
| memory8 by CL | 0100 00XB 1101 0010 : mod 001 r/m |
| memory64 by CL | 0100 10XB 1101 0011 : mod 001 r/m |
| register by immediate count | 0100 000B 1100 000w : 11 001 reg : imm8 |
| byteregister by immediate count | 0100 000B 1100 0000 : 11 001 reg : imm8 |
| qwordregister by immediate count | 0100 100B 1100 0001 : 11 001 qwordreg : imm8 |
| memory by immediate count | 0100 00XB 1100 000w : mod 001 r/m : imm8 |
| memory8 by immediate count | 0100 00XB 1100 0000 : mod 001 r/m : imm8 |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 001 r/m : imm8 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| RSM - Resume from System Management Mode | 0000 1111 : 1010 1010 |
| SAL - Shift Arithmetic Left | same instruction as SHL |
| SAR - Shift Arithmetic Right | |
| register by 1 | 0100 000B 1101 000w : 11 111 reg |
| byteregister by 1 | 0100 000B 1101 0000 : 11 111 bytereg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 111 qwordreg |
| memory by 1 | 0100 00XB 1101 000w : mod 111 r/m |
| memory8 by 1 | 0100 00XB 1101 0000 : mod 111 r/m |
| memory64 by 1 | 0100 10XB 1101 0001 : mod 111 r/m |
| register by CL | 0100 000B 1101 001w : 11 111 reg |
| byteregister by CL | 0100 000B 1101 0010 : 11 111 bytereg |
| qwordregister by CL | 0100 100B 1101 0011 : 11 111 qwordreg |
| memory by CL | 0100 00XB 1101 001w : mod 111 r/m |
| memory8 by CL | 0100 00XB 1101 0010 : mod 111 r/m |
| memory64 by CL | 0100 10XB 1101 0011 : mod 111 r/m |
| register by immediate count | 0100 000B 1100 000w : 11 111 reg : imm8 |
| byteregister by immediate count | 0100 000B 1100 0000 : 11 111 bytereg : imm8 |
| qwordregister by immediate count | 0100 100B 1100 0001 : 11 111 qwordreg : imm8 |
| memory by immediate count | 0100 00XB 1100 000w : mod 111 r/m : imm8 |
| memory8 by immediate count | 0100 00XB 1100 0000 : mod 111 r/m : imm8 |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 111 r/m : imm8 |
| SBB - Integer Subtraction with Borrow | |
| register1 to register2 | 0100 0R0B 0001 100w : 11 reg1 reg2 |
| byteregister1 to byteregister2 | 0100 0R0B 0001 1000 : 11 bytereg1 bytereg2 |
| quadregister1 to quadregister2 | 0100 1R0B 0001 1001 : 11 quadreg1 quadreg2 |
| register2 to register1 | 0100 0R0B 0001 101w : 11 reg1 reg2 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| byteregeister2 to byteregeister1 | 0100 0R0B 0001 1010 : 11 reg1 byteregeister2 |
| byteregeister2 to byteregeister1 | 0100 1R0B 0001 1011 : 11 reg1 byteregeister2 |
| memory to register | 0100 0RXB 0001 101w : mod reg r/m |
| memory8 to byteregeister | 0100 0RXB 0001 1010 : mod byteregeister r/m |
| memory64 to byteregeister | 0100 1RXB 0001 1011 : mod quadreg r/m |
| register to memory | 0100 0RXB 0001 100w : mod reg r/m |
| byteregeister to memory8 | 0100 0RXB 0001 1000 : mod reg r/m |
| quadregister to memory64 | 0100 1RXB 0001 1001 : mod reg r/m |
| immediate to register | 0100 000B 1000 00sw : 11 011 reg : imm |
| immediate8 to byteregeister | 0100 000B 1000 0000 : 11 011 byteregeister : imm8 |
| immediate32 to qwordregister | 0100 100B 1000 0001 : 11 011 qwordreg : imm32 |
| immediate8 to qwordregister | 0100 100B 1000 0011 : 11 011 qwordreg : imm8 |
| immediate to AL, AX, or EAX | 0100 000B 0001 110w : imm |
| immediate32 to RAL | 0100 1000 0001 1101 : imm32 |
| immediate to memory | 0100 00XB 1000 00sw : mod 011 r/m : imm |
| immediate8 to memory8 | 0100 00XB 1000 0000 : mod 011 r/m : imm8 |
| immediate32 to memory64 | 0100 10XB 1000 0001 : mod 011 r/m : imm32 |
| immediate8 to memory64 | 0100 10XB 1000 0011 : mod 011 r/m : imm8 |
| SCAS/SCASB/SCASW/SCASD - Scan String | |
| scan string | 1010 111w |
| scan string (compare AL with byte at RDI) | 0100 1000 1010 1110 |
| scan string (compare RAX with qword at RDI) | 0100 1000 1010 1111 |
| SETcc - Byte Set on Condition | |
| register | 0100 000B 0000 1111 : 1001 tttt : 11 000 reg |
| register | 0100 0000 0000 1111 : 1001 tttt : 11 000 reg |
| memory | 0100 00XB 0000 1111 : 1001 tttt : mod 000 r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| memory | 0100 0000 0000 1111 : 1001 ttn : mod 000 r/m |
| SGDT - Store Global Descriptor Table Register | 0000 1111 : 0000 0001 : mod ^A 000 r/m |
| SHL - Shift Left | |
| register by 1 | 0100 000B 1101 000w : 11 100 reg |
| byteregister by 1 | 0100 000B 1101 0000 : 11 100 bytereg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 100 qwordreg |
| memory by 1 | 0100 00XB 1101 000w : mod 100 r/m |
| memory8 by 1 | 0100 00XB 1101 0000 : mod 100 r/m |
| memory64 by 1 | 0100 10XB 1101 0001 : mod 100 r/m |
| register by CL | 0100 000B 1101 001w : 11 100 reg |
| byteregister by CL | 0100 000B 1101 0010 : 11 100 bytereg |
| qwordregister by CL | 0100 100B 1101 0011 : 11 100 qwordreg |
| memory by CL | 0100 00XB 1101 001w : mod 100 r/m |
| memory8 by CL | 0100 00XB 1101 0010 : mod 100 r/m |
| memory64 by CL | 0100 10XB 1101 0011 : mod 100 r/m |
| register by immediate count | 0100 000B 1100 000w : 11 100 reg : imm8 |
| byteregister by immediate count | 0100 000B 1100 0000 : 11 100 bytereg : imm8 |
| quadregister by immediate count | 0100 100B 1100 0001 : 11 100 quadreg : imm8 |
| memory by immediate count | 0100 00XB 1100 000w : mod 100 r/m : imm8 |
| memory8 by immediate count | 0100 00XB 1100 0000 : mod 100 r/m : imm8 |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 100 r/m : imm8 |
| SHLD - Double Precision Shift Left | |
| register by immediate count | 0100 0R0B 0000 1111 : 1010 0100 : 11 reg2 reg1 : imm8 |
| qwordregister by immediate8 | 0100 1R0B 0000 1111 : 1010 0100 : 11 qwordreg2 qwordreg1 : imm8 |
| memory by immediate count | 0100 0RXB 0000 1111 : 1010 0100 : mod reg r/m : imm8 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| memory64 by immediate8 | 0100 1RxB 0000 1111 : 1010 0100 : mod qwordreg r/m : imm8 |
| register by CL | 0100 0R0B 0000 1111 : 1010 0101 : 11 reg2 reg1 |
| quadregister by CL | 0100 1R0B 0000 1111 : 1010 0101 : 11 quadreg2 quadreg1 |
| memory by CL | 0100 00XB 0000 1111 : 1010 0101 : mod reg r/m |
| memory64 by CL | 0100 1RxB 0000 1111 : 1010 0101 : mod quadreg r/m |
| SHR - Shift Right | |
| register by 1 | 0100 000B 1101 000w : 11 101 reg |
| byteregister by 1 | 0100 000B 1101 0000 : 11 101 bytereg |
| qwordregister by 1 | 0100 100B 1101 0001 : 11 101 qwordreg |
| memory by 1 | 0100 00XB 1101 000w : mod 101 r/m |
| memory8 by 1 | 0100 00XB 1101 0000 : mod 101 r/m |
| memory64 by 1 | 0100 10XB 1101 0001 : mod 101 r/m |
| register by CL | 0100 000B 1101 001w : 11 101 reg |
| byteregister by CL | 0100 000B 1101 0010 : 11 101 bytereg |
| qwordregister by CL | 0100 100B 1101 0011 : 11 101 qwordreg |
| memory by CL | 0100 00XB 1101 001w : mod 101 r/m |
| memory8 by CL | 0100 00XB 1101 0010 : mod 101 r/m |
| memory64 by CL | 0100 10XB 1101 0011 : mod 101 r/m |
| register by immediate count | 0100 000B 1100 000w : 11 101 reg : imm8 |
| byteregister by immediate count | 0100 000B 1100 0000 : 11 101 reg : imm8 |
| qwordregister by immediate count | 0100 100B 1100 0001 : 11 101 reg : imm8 |
| memory by immediate count | 0100 00XB 1100 000w : mod 101 r/m : imm8 |
| memory8 by immediate count | 0100 00XB 1100 0000 : mod 101 r/m : imm8 |
| memory64 by immediate count | 0100 10XB 1100 0001 : mod 101 r/m : imm8 |
| SHRD - Double Precision Shift Right | |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|--|
| register by immediate count | 0100 0ROB 0000 1111 : 1010 1100 : 11 reg2 reg1 : imm8 |
| qwordregister by immediate8 | 0100 1ROB 0000 1111 : 1010 1100 : 11 qwordreg2 qwordreg1 : imm8 |
| memory by immediate count | 0100 00XB 0000 1111 : 1010 1100 : mod reg r/m : imm8 |
| memory64 by immediate8 | 0100 1RXB 0000 1111 : 1010 1100 : mod qwordreg r/m : imm8 |
| register by CL | 0100 000B 0000 1111 : 1010 1101 : 11 reg2 reg1 |
| qwordregister by CL | 0100 1ROB 0000 1111 : 1010 1101 : 11 qwordreg2 qwordreg1 |
| memory by CL | 0000 1111 : 1010 1101 : mod reg r/m |
| memory64 by CL | 0100 1RXB 0000 1111 : 1010 1101 : mod qwordreg r/m |
| SIDT - Store Interrupt Descriptor Table Register | 0000 1111 : 0000 0001 : mod ^A 001 r/m |
| SLDT - Store Local Descriptor Table Register | |
| to register | 0100 000B 0000 1111 : 0000 0000 : 11 000 reg |
| to memory | 0100 00XB 0000 1111 : 0000 0000 : mod 000 r/m |
| SMSW - Store Machine Status Word | |
| to register | 0100 000B 0000 1111 : 0000 0001 : 11 100 reg |
| to memory | 0100 00XB 0000 1111 : 0000 0001 : mod 100 r/m |
| STC - Set Carry Flag | 1111 1001 |
| STD - Set Direction Flag | 1111 1101 |
| STI - Set Interrupt Flag | 1111 1011 |
| STOS/STOSB/STOSW/STOSD/STOSQ - Store String Data | |
| store string data | 1010 101w |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| store string data (RAX at address RDI) | 0100 1000 1010 1011 |
| STR - Store Task Register | |
| to register | 0100 000B 0000 1111 : 0000 0000 : 11 001 reg |
| to memory | 0100 00XB 0000 1111 : 0000 0000 : mod 001 r/m |
| SUB - Integer Subtraction | |
| register1 from register2 | 0100 0ROB 0010 100w : 11 reg1 reg2 |
| byteregister1 from byteregister2 | 0100 0ROB 0010 1000 : 11 bytereg1 bytereg2 |
| qwordregister1 from qwordregister2 | 0100 1ROB 0010 1000 : 11 qwordreg1 qwordreg2 |
| register2 from register1 | 0100 0ROB 0010 101w : 11 reg1 reg2 |
| byteregister2 from byteregister1 | 0100 0ROB 0010 1010 : 11 bytereg1 bytereg2 |
| qwordregister2 from qwordregister1 | 0100 1ROB 0010 1011 : 11 qwordreg1 qwordreg2 |
| memory from register | 0100 00XB 0010 101w : mod reg r/m |
| memory8 from byteregister | 0100 0RXB 0010 1010 : mod bytereg r/m |
| memory64 from qwordregister | 0100 1RXB 0010 1011 : mod qwordreg r/m |
| register from memory | 0100 0RXB 0010 100w : mod reg r/m |
| byteregister from memory8 | 0100 0RXB 0010 1000 : mod bytereg r/m |
| qwordregister from memory8 | 0100 1RXB 0010 1000 : mod qwordreg r/m |
| immediate from register | 0100 000B 1000 00sw : 11 101 reg : imm |
| immediate8 from byteregister | 0100 000B 1000 0000 : 11 101 bytereg : imm8 |
| immediate32 from qwordregister | 0100 100B 1000 0001 : 11 101 qwordreg : imm32 |
| immediate8 from qwordregister | 0100 100B 1000 0011 : 11 101 qwordreg : imm8 |
| immediate from AL, AX, or EAX | 0100 000B 0010 110w : imm |
| immediate32 from RAX | 0100 1000 0010 1101 : imm32 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|---|
| immediate from memory | 0100 00XB 1000 00sw : mod 101 r/m : imm |
| immediate8 from memory8 | 0100 00XB 1000 0000 : mod 101 r/m : imm8 |
| immediate32 from memory64 | 0100 10XB 1000 0001 : mod 101 r/m : imm32 |
| immediate8 from memory64 | 0100 10XB 1000 0011 : mod 101 r/m : imm8 |
| SWAPGS - Swap GS Base Register | |
| GS base register value for value in MSR C0000102H | 0000 1111 0000 0001 [this one incomplete] |
| SYSCALL - Fast System Call | |
| fast call to privilege level 0 system procedures | 0000 1111 0000 0101 |
| SYSRET - Return From Fast System Call | |
| return from fast system call | 0000 1111 0000 0111 |
| TEST - Logical Compare | |
| register1 and register2 | 0100 0R0B 1000 010w : 11 reg1 reg2 |
| byteregister1 and byteregister2 | 0100 0R0B 1000 0100 : 11 bytereg1 bytereg2 |
| qwordregister1 and qwordregister2 | 0100 1R0B 1000 0101 : 11 qwordreg1 qwordreg2 |
| memory and register | 0100 0R0B 1000 010w : mod reg r/m |
| memory8 and byteregister | 0100 0RXB 1000 0100 : mod bytereg r/m |
| memory64 and qwordregister | 0100 1RXB 1000 0101 : mod qwordreg r/m |
| immediate and register | 0100 000B 1111 011w : 11 000 reg : imm |
| immediate8 and byteregister | 0100 000B 1111 0110 : 11 000 bytereg : imm8 |
| immediate32 and qwordregister | 0100 100B 1111 0111 : 11 000 bytereg : imm8 |
| immediate and AL, AX, or EAX | 0100 000B 1010 100w : imm |
| immediate32 and RAX | 0100 1000 1010 1001 : imm32 |
| immediate and memory | 0100 00XB 1111 011w : mod 000 r/m : imm |
| immediate8 and memory8 | 0100 1000 1111 0110 : mod 000 r/m : imm8 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|---|---|
| immediate32 and memory64 | 0100 1000 1111 0111 : mod 000 r/m : imm32 |
| UD2 - Undefined instruction | 0000 FFFF : 0000 1011 |
| VERR - Verify a Segment for Reading | |
| register | 0100 000B 0000 1111 : 0000 0000 : 11 100 reg |
| memory | 0100 00XB 0000 1111 : 0000 0000 : mod 100 r/m |
| VERW - Verify a Segment for Writing | |
| register | 0100 000B 0000 1111 : 0000 0000 : 11 101 reg |
| memory | 0100 00XB 0000 1111 : 0000 0000 : mod 101 r/m |
| WAIT - Wait | 1001 1011 |
| WBINVD - Writeback and Invalidate Data Cache | 0000 1111 : 0000 1001 |
| WRMSR - Write to Model-Specific Register | |
| write EDX:EAX to ECX specified MSR | 0000 1111 : 0011 0000 |
| write RDX[31:0]:RAX[31:0] to RCX specified MSR | 0100 1000 0000 1111 : 0011 0000 |
| XADD - Exchange and Add | |
| register1, register2 | 0100 0R0B 0000 1111 : 1100 000w : 11 reg2 reg1 |
| byteregister1, byteregister2 | 0100 0R0B 0000 1111 : 1100 0000 : 11 bytereg2 bytereg1 |
| qwordregister1, qwordregister2 | 0100 0R0B 0000 1111 : 1100 0001 : 11 qwordreg2 qwordreg1 |
| memory, register | 0100 0RXB 0000 1111 : 1100 000w : mod reg r/m |
| memory8, bytereg | 0100 1RXB 0000 1111 : 1100 0000 : mod bytereg r/m |
| memory64, qwordreg | 0100 1RXB 0000 1111 : 1100 0001 : mod qwordreg r/m |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|--|--|
| XCHG - Exchange Register/Memory with Register | |
| register1 with register2 | 1000 011w : 11 reg1 reg2 |
| AX or EAX with register | 1001 0 reg |
| memory with register | 1000 011w : mod reg r/m |
| XLAT/XLATB - Table Look-up Translation | |
| AL to byte DS:[(E)BX + unsigned AL] | 1101 0111 |
| AL to byte DS:[RBX + unsigned AL] | 0100 1000 1101 0111 |
| XOR - Logical Exclusive OR | |
| register1 to register2 | 0100 0RxB 0011 000w : 11 reg1 reg2 |
| byteregister1 to byteregister2 | 0100 0ROB 0011 0000 : 11 bytereg1 bytereg2 |
| qwordregister1 to qwordregister2 | 0100 1ROB 0011 0001 : 11 qwordreg1 qwordreg2 |
| register2 to register1 | 0100 0ROB 0011 001w : 11 reg1 reg2 |
| byteregister2 to byteregister1 | 0100 0ROB 0011 0010 : 11 bytereg1 bytereg2 |
| qwordregister2 to qwordregister1 | 0100 1ROB 0011 0011 : 11 qwordreg1 qwordreg2 |
| memory to register | 0100 0RxB 0011 001w : mod reg r/m |
| memory8 to byteregister | 0100 0RxB 0011 0010 : mod bytereg r/m |
| memory64 to qwordregister | 0100 1RxB 0011 0011 : mod qwordreg r/m |
| register to memory | 0100 0RxB 0011 000w : mod reg r/m |
| byteregister to memory8 | 0100 0RxB 0011 0000 : mod bytereg r/m |
| qwordregister to memory8 | 0100 1RxB 0011 0001 : mod qwordreg r/m |
| immediate to register | 0100 000B 1000 00sw : 11 110 reg : imm |
| immediate8 to byteregister | 0100 000B 1000 0000 : 11 110 bytereg : imm8 |
| immediate32 to qwordregister | 0100 100B 1000 0001 : 11 110 qwordreg : imm32 |
| immediate8 to qwordregister | 0100 100B 1000 0011 : 11 110 qwordreg : imm8 |

**Table B-15. General Purpose Instruction Formats and Encodings
for 64-Bit Mode (Contd.)**

| Instruction and Format | Encoding |
|-----------------------------|---|
| immediate to AL, AX, or EAX | 0100 000B 0011 010w : imm |
| immediate to RAX | 0100 1000 0011 0101 : immediate data |
| immediate to memory | 0100 00XB 1000 00sw : mod 110 r/m : imm |
| immediate8 to memory8 | 0100 00XB 1000 0000 : mod 110 r/m : imm8 |
| immediate32 to memory64 | 0100 10XB 1000 0001 : mod 110 r/m : imm32 |
| immediate8 to memory64 | 0100 10XB 1000 0011 : mod 110 r/m : imm8 |
| Prefix Bytes | |
| address size | 0110 0111 |
| LOCK | 1111 0000 |
| operand size | 0110 0110 |
| CS segment override | 0010 1110 |
| DS segment override | 0011 1110 |
| ES segment override | 0010 0110 |
| FS segment override | 0110 0100 |
| GS segment override | 0110 0101 |
| SS segment override | 0011 0110 |

B.3 PENTIUM® PROCESSOR FAMILY INSTRUCTION FORMATS AND ENCODINGS

The following table shows formats and encodings introduced by the Pentium processor family.

**Table B-16. Pentium Processor Family Instruction Formats and Encodings,
Non-64-Bit Modes**

| Instruction and Format | Encoding |
|---|-------------------------------------|
| CMPXCHG8B - Compare and Exchange 8 Bytes | |
| EDX:EAX with memory64 | 0000 1111 : 1100 0111 : mod 001 r/m |

Table B-17. Pentium Processor Family Instruction Formats and Encodings, 64-Bit Mode

| Instruction and Format | Encoding |
|--|---|
| CMPXCHG8B/CMPXCHG16B - Compare and Exchange Bytes | |
| EDX:EAX with memory64 | 0000 1111 : 1100 0111 : mod 001 r/m |
| RDX:RAX with memory128 | 0100 10XB 0000 1111 : 1100 0111 : mod 001 r/m |

B.4 64-BIT MODE INSTRUCTION ENCODINGS FOR SIMD INSTRUCTION EXTENSIONS

Non-64-bit mode instruction encodings for MMX Technology, SSE, SSE2, and SSE3 are covered by applying these rules to Table B-19 through Table B-31. Table B-33 lists special encodings (instructions that do not follow the rules below).

- The REX instruction has no effect:
 - On immediates
 - If both operands are MMX registers
 - On MMX registers and XMM registers
 - If an MMX register is encoded in the reg field of the ModR/M byte
- If a memory operand is encoded in the r/m field of the ModR/M byte, REX.X and REX.B may be used for encoding the memory operand.
- If a general-purpose register is encoded in the r/m field of the ModR/M byte, REX.B may be used for register encoding and REX.W may be used to encode the 64-bit operand size.
- If an XMM register operand is encoded in the reg field of the ModR/M byte, REX.R may be used for register encoding. If an XMM register operand is encoded in the r/m field of the ModR/M byte, REX.B may be used for register encoding.

B.5 MMX INSTRUCTION FORMATS AND ENCODINGS

MMX instructions, except the EMMS instruction, use a format similar to the 2-byte Intel Architecture integer format. Details of subfield encodings within these formats are presented below.

B.5.1 Granularity Field (gg)

The granularity field (gg) indicates the size of the packed operands that the instruction is operating on. When this field is used, it is located in bits 1 and 0 of the second opcode byte. Table B-18 shows the encoding of the gg field.

Table B-18. Encoding of Granularity of Data Field (gg)

| gg | Granularity of Data |
|----|---------------------|
| 00 | Packed Bytes |
| 01 | Packed Words |
| 10 | Packed Doublewords |
| 11 | Quadword |

B.5.2 MMX Technology and General-Purpose Register Fields (mmxreg and reg)

When MMX technology registers (mmxreg) are used as operands, they are encoded in the ModR/M byte in the reg field (bits 5, 4, and 3) and/or the R/M field (bits 2, 1, and 0).

If an MMX instruction operates on a general-purpose register (reg), the register is encoded in the R/M field of the ModR/M byte.

B.5.3 MMX Instruction Formats and Encodings Table

Table B-19 shows the formats and encodings of the integer instructions.

Table B-19. MMX Instruction Formats and Encodings

| Instruction and Format | Encoding |
|--|---|
| EMMS - Empty MMX technology state | 0000 1111:01110111 |
| MOVD - Move doubleword | |
| reg to mmxreg | 0000 1111:0110 1110: 11 mmxreg reg |
| reg from mmxreg | 0000 1111:0111 1110: 11 mmxreg reg |
| mem to mmxreg | 0000 1111:0110 1110: mod mmxreg r/m |
| mem from mmxreg | 0000 1111:0111 1110: mod mmxreg r/m |
| MOVQ - Move quadword | |
| mmxreg2 to mmxreg1 | 0000 1111:0110 1111: 11 mmxreg1 mmxreg2 |
| mmxreg2 from mmxreg1 | 0000 1111:0111 1111: 11 mmxreg1 mmxreg2 |
| mem to mmxreg | 0000 1111:0110 1111: mod mmxreg r/m |

Table B-19. MMX Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|---|--|
| mem from mmxreg | 0000 1111:0111 1111: mod mmxreg r/m |
| PACKSSDW¹ - Pack dword to word data (signed with saturation) | |
| mmxreg2 to mmxreg1 | 0000 1111:0110 1011: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:0110 1011: mod mmxreg r/m |
| PACKSSWB¹ - Pack word to byte data (signed with saturation) | |
| mmxreg2 to mmxreg1 | 0000 1111:0110 0011: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:0110 0011: mod mmxreg r/m |
| PACKUSWB¹ - Pack word to byte data (unsigned with saturation) | |
| mmxreg2 to mmxreg1 | 0000 1111:0110 0111: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:0110 0111: mod mmxreg r/m |
| PADD - Add with wrap-around | |
| mmxreg2 to mmxreg1 | 0000 1111: 1111 11gg: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111: 1111 11gg: mod mmxreg r/m |
| PADDs - Add signed with saturation | |
| mmxreg2 to mmxreg1 | 0000 1111: 1110 11gg: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111: 1110 11gg: mod mmxreg r/m |
| PADDUS - Add unsigned with saturation | |
| mmxreg2 to mmxreg1 | 0000 1111: 1101 11gg: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111: 1101 11gg: mod mmxreg r/m |
| PAND - Bitwise And | |
| mmxreg2 to mmxreg1 | 0000 1111:1101 1011: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1101 1011: mod mmxreg r/m |
| PANDN - Bitwise AndNot | |
| mmxreg2 to mmxreg1 | 0000 1111:1101 1111: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1101 1111: mod mmxreg r/m |
| PCMPEQ - Packed compare for equality | |
| mmxreg1 with mmxreg2 | 0000 1111:0111 01gg: 11 mmxreg1 mmxreg2 |
| mmxreg with memory | 0000 1111:0111 01gg: mod mmxreg r/m |

Table B-19. MMX Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|--|---|
| PCMPGT - Packed compare greater (signed) | |
| mmxreg1 with mmxreg2 | 0000 1111:0110 01gg: 11 mmxreg1 mmxreg2 |
| mmxreg with memory | 0000 1111:0110 01gg: mod mmxreg r/m |
| PMADDWD - Packed multiply add | |
| mmxreg2 to mmxreg1 | 0000 1111:1111 0101: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1111 0101: mod mmxreg r/m |
| PMULHUW - Packed multiplication, store high word (unsigned) | |
| mmxreg2 to mmxreg1 | 0000 1111: 1110 0100: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111: 1110 0100: mod mmxreg r/m |
| PMULHW - Packed multiplication, store high word | |
| mmxreg2 to mmxreg1 | 0000 1111:1110 0101: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1110 0101: mod mmxreg r/m |
| PMULLW - Packed multiplication, store low word | |
| mmxreg2 to mmxreg1 | 0000 1111:1101 0101: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1101 0101: mod mmxreg r/m |
| POR - Bitwise Or | |
| mmxreg2 to mmxreg1 | 0000 1111:1110 1011: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1110 1011: mod mmxreg r/m |
| PSLL² - Packed shift left logical | |
| mmxreg1 by mmxreg2 | 0000 1111:1111 00gg: 11 mmxreg1 mmxreg2 |
| mmxreg by memory | 0000 1111:1111 00gg: mod mmxreg r/m |
| mmxreg by immediate | 0000 1111:0111 00gg: 11 110 mmxreg: imm8 data |
| PSRA² - Packed shift right arithmetic | |
| mmxreg1 by mmxreg2 | 0000 1111:1110 00gg: 11 mmxreg1 mmxreg2 |
| mmxreg by memory | 0000 1111:1110 00gg: mod mmxreg r/m |
| mmxreg by immediate | 0000 1111:0111 00gg: 11 100 mmxreg: imm8 data |

Table B-19. MMX Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|---|---|
| PSRL² - Packed shift right logical | |
| mmxreg1 by mmxreg2 | 0000 1111:1101 00gg: 11 mmxreg1 mmxreg2 |
| mmxreg by memory | 0000 1111:1101 00gg: mod mmxreg r/m |
| mmxreg by immediate | 0000 1111:0111 00gg: 11 010 mmxreg: imm8 data |
| PSUB - Subtract with wrap-around | |
| mmxreg2 from mmxreg1 | 0000 1111:1111 10gg: 11 mmxreg1 mmxreg2 |
| memory from mmxreg | 0000 1111:1111 10gg: mod mmxreg r/m |
| PSUBS - Subtract signed with saturation | |
| mmxreg2 from mmxreg1 | 0000 1111:1110 10gg: 11 mmxreg1 mmxreg2 |
| memory from mmxreg | 0000 1111:1110 10gg: mod mmxreg r/m |
| PSUBUS - Subtract unsigned with saturation | |
| mmxreg2 from mmxreg1 | 0000 1111:1101 10gg: 11 mmxreg1 mmxreg2 |
| memory from mmxreg | 0000 1111:1101 10gg: mod mmxreg r/m |
| PUNPCKH - Unpack high data to next larger type | |
| mmxreg2 to mmxreg1 | 0000 1111:0110 10gg: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:0110 10gg: mod mmxreg r/m |
| PUNPCKL - Unpack low data to next larger type | |
| mmxreg2 to mmxreg1 | 0000 1111:0110 00gg: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:0110 00gg: mod mmxreg r/m |
| PXOR - Bitwise Xor | |
| mmxreg2 to mmxreg1 | 0000 1111:1110 1111: 11 mmxreg1 mmxreg2 |
| memory to mmxreg | 0000 1111:1110 1111: mod mmxreg r/m |

NOTES:

1. The pack instructions perform saturation from signed packed data of one type to signed or unsigned data of the next smaller type.
2. The format of the shift instructions has one additional format to support shifting by immediate shift-counts. The shift operations are not supported equally for all data types.

B.6 PROCESSOR EXTENDED STATE INSTRUCTION FORMATS AND ENCODINGS

Table B-20 shows the formats and encodings for several instructions that relate to processor extended state management.

Table B-20. Formats and Encodings of XSAVE/XRSTOR/XGETBV/XSETBV Instructions

| Instruction and Format | Encoding |
|---|---|
| XGETBV – Get Value of Extended Control Register | 0000 1111:0000 0001: 1101 0000 |
| XRSTOR – Restore Processor Extended States¹ | 0000 1111:1010 1110: mod ^A 101 r/m |
| XSAVE – Save Processor Extended States¹ | 0000 1111:1010 1110: mod ^A 100 r/m |
| XSETBV – Set Extended Control Register | 0000 1111:0000 0001: 1101 0001 |

NOTES:

1. For XSAVE and XRSTOR, “mod = 11” is reserved.

B.7 P6 FAMILY INSTRUCTION FORMATS AND ENCODINGS

Table B-20 shows the formats and encodings for several instructions that were introduced into the IA-32 architecture in the P6 family processors.

Table B-21. Formats and Encodings of P6 Family Instructions

| Instruction and Format | Encoding |
|---|------------------------------------|
| CMOVcc – Conditional Move | |
| register2 to register1 | 0000 1111: 0100 ttn : 11 reg1 reg2 |
| memory to register | 0000 1111 : 0100 ttn : mod reg r/m |
| FCMOVcc – Conditional Move on EFLAG Register Condition Codes | |
| move if below (B) | 11011 010 : 11 000 ST(i) |
| move if equal (E) | 11011 010 : 11 001 ST(i) |
| move if below or equal (BE) | 11011 010 : 11 010 ST(i) |
| move if unordered (U) | 11011 010 : 11 011 ST(i) |
| move if not below (NB) | 11011 011 : 11 000 ST(i) |
| move if not equal (NE) | 11011 011 : 11 001 ST(i) |

Table B-21. Formats and Encodings of P6 Family Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| move if not below or equal (NBE) | 11011 011 : 11 010 ST(i) |
| move if not unordered (NU) | 11011 011 : 11 011 ST(i) |
| FCOMI - Compare Real and Set EFLAGS | 11011 011 : 11 110 ST(i) |
| FXRSTOR - Restore x87 FPU, MMX, SSE, and SSE2 State⁷ | 0000 1111:1010 1110: mod ^A 001 r/m |
| FXSAVE - Save x87 FPU, MMX, SSE, and SSE2 State⁷ | 0000 1111:1010 1110: mod ^A 000 r/m |
| SYSENTER - Fast System Call | 0000 1111:0011 0100 |
| SYSEXIT - Fast Return from Fast System Call | 0000 1111:0011 0101 |

NOTES:

1. For FXSAVE and FXRSTOR, "mod = 11" is reserved.

B.8 SSE INSTRUCTION FORMATS AND ENCODINGS

The SSE instructions use the ModR/M format and are preceded by the 0FH prefix byte. In general, operations are not duplicated to provide two directions (that is, separate load and store variants).

The following three tables (Tables B-22, B-23, and B-24) show the formats and encodings for the SSE SIMD floating-point, SIMD integer, and cacheability and memory ordering instructions, respectively. Some SSE instructions require a mandatory prefix (66H, F2H, F3H) as part of the two-byte opcode. Mandatory prefixes are included in the tables.

Table B-22. Formats and Encodings of SSE Floating-Point Instructions

| Instruction and Format | Encoding |
|--|--|
| ADDPS—Add Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1000: mod xmmreg r/m |
| ADDSS—Add Scalar Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0011:0000 1111:01011000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:01011000: mod xmmreg r/m |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| ANDNPS—Bitwise Logical AND NOT of Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 0101: mod xmmreg r/m |
| ANDPS—Bitwise Logical AND of Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 0100: mod xmmreg r/m |
| CMPPS—Compare Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg, imm8 | 0000 1111:1100 0010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0000 1111:1100 0010: mod xmmreg r/m: imm8 |
| CMPSS—Compare Scalar Single-Precision Floating-Point Values | |
| xmmreg to xmmreg, imm8 | 1111 0011:0000 1111:1100 0010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 1111 0011:0000 1111:1100 0010: mod xmmreg r/m: imm8 |
| COMISS—Compare Scalar Ordered Single-Precision Floating-Point Values and Set EFLAGS | |
| xmmreg to xmmreg | 0000 1111:0010 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0010 1111: mod xmmreg r/m |
| CVTPI2PS—Convert Packed Doubleword Integers to Packed Single-Precision Floating-Point Values | |
| mmreg to xmmreg | 0000 1111:0010 1010:11 xmmreg1 mmreg1 |
| mem to xmmreg | 0000 1111:0010 1010: mod xmmreg r/m |
| CVTPS2PI—Convert Packed Single-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to mmreg | 0000 1111:0010 1101:11 mmreg1 xmmreg1 |
| mem to mmreg | 0000 1111:0010 1101: mod mmreg r/m |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| CVTSI2SS—Convert Doubleword Integer to Scalar Single-Precision Floating-Point Value | |
| r32 to xmmreg1 | 1111 0011:0000 1111:00101010:11 xmmreg r32 |
| mem to xmmreg | 1111 0011:0000 1111:00101010: mod xmmreg r/m |
| CVTSS2SI—Convert Scalar Single-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 1111 0011:0000 1111:0010 1101:11 r32 xmmreg |
| mem to r32 | 1111 0011:0000 1111:0010 1101: mod r32 r/m |
| CVTTPS2PI—Convert with Truncation Packed Single-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to mmreg | 0000 1111:0010 1100:11 mmreg1 xmmreg1 |
| mem to mmreg | 0000 1111:0010 1100: mod mmreg r/m |
| CVTTSS2SI—Convert with Truncation Scalar Single-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 1111 0011:0000 1111:0010 1100:11 r32 xmmreg1 |
| mem to r32 | 1111 0011:0000 1111:0010 1100: mod r32 r/m |
| DIVPS—Divide Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1110: mod xmmreg r/m |
| DIVSS—Divide Scalar Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 1110: mod xmmreg r/m |
| LDMXCSR—Load MXCSR Register State | |
| m32 to MXCSR | 0000 1111:1010 1110:mod ^A 010 mem |
| MAXPS—Return Maximum Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1111:11 xmmreg1 xmmreg2 |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| mem to xmmreg | 0000 1111:0101 1111: mod xmmreg r/m |
| MAXSS—Return Maximum Scalar Double-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 1111: mod xmmreg r/m |
| MINPS—Return Minimum Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1101: mod xmmreg r/m |
| MINSS—Return Minimum Scalar Double-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 1101: mod xmmreg r/m |
| MOVAPS—Move Aligned Packed Single-Precision Floating-Point Values | |
| xmmreg2 to xmmreg1 | 0000 1111:0010 1000:11 xmmreg2 xmmreg1 |
| mem to xmmreg1 | 0000 1111:0010 1000: mod xmmreg r/m |
| xmmreg1 to xmmreg2 | 0000 1111:0010 1001:11 xmmreg1 xmmreg2 |
| xmmreg1 to mem | 0000 1111:0010 1001: mod xmmreg r/m |
| MOVHLPS—Move Packed Single-Precision Floating-Point Values High to Low | |
| xmmreg to xmmreg | 0000 1111:0001 0010:11 xmmreg1 xmmreg2 |
| MOVHPS—Move High Packed Single-Precision Floating-Point Values | |
| mem to xmmreg | 0000 1111:0001 0110: mod xmmreg r/m |
| xmmreg to mem | 0000 1111:0001 0111: mod xmmreg r/m |
| MOVLHPS—Move Packed Single-Precision Floating-Point Values Low to High | |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| xmmreg to xmmreg | 0000 1111:00010110:11 xmmreg1 xmmreg2 |
| MOVLPS—Move Low Packed Single-Precision Floating-Point Values | |
| mem to xmmreg | 0000 1111:0001 0010: mod xmmreg r/m |
| xmmreg to mem | 0000 1111:0001 0011: mod xmmreg r/m |
| MOVMSKPS—Extract Packed Single-Precision Floating-Point Sign Mask | |
| xmmreg to r32 | 0000 1111:0101 0000:11 r32 xmmreg |
| MOVSS—Move Scalar Single-Precision Floating-Point Values | |
| xmmreg2 to xmmreg1 | 1111 0011:0000 1111:0001 0000:11 xmmreg2 xmmreg1 |
| mem to xmmreg1 | 1111 0011:0000 1111:0001 0000: mod xmmreg r/m |
| xmmreg1 to xmmreg2 | 1111 0011:0000 1111:0001 0001:11 xmmreg1 xmmreg2 |
| xmmreg1 to mem | 1111 0011:0000 1111:0001 0001: mod xmmreg r/m |
| MOVUPS—Move Unaligned Packed Single-Precision Floating-Point Values | |
| xmmreg2 to xmmreg1 | 0000 1111:0001 0000:11 xmmreg2 xmmreg1 |
| mem to xmmreg1 | 0000 1111:0001 0000: mod xmmreg r/m |
| xmmreg1 to xmmreg2 | 0000 1111:0001 0001:11 xmmreg1 xmmreg2 |
| xmmreg1 to mem | 0000 1111:0001 0001: mod xmmreg r/m |
| MULPS—Multiply Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1001: mod xmmreg rm |
| MULSS—Multiply Scalar Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 1001: mod xmmreg r/m |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| ORPS—Bitwise Logical OR of Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 0110 mod xmmreg r/m |
| RCPPS—Compute Reciprocals of Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 0011: mod xmmreg r/m |
| RCPS—Compute Reciprocals of Scalar Single-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0011:0000 1111:01010011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:01010011: mod xmmreg r/m |
| RSQRTPS—Compute Reciprocals of Square Roots of Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 0010 mode xmmreg r/m |
| RSQRTSS—Compute Reciprocals of Square Roots of Scalar Single-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 0010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 0010 mod xmmreg r/m |
| SHUFPS—Shuffle Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg, imm8 | 0000 1111:1100 0110:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0000 1111:1100 0110: mod xmmreg r/m: imm8 |
| SQRTPS—Compute Square Roots of Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0001:11 xmmreg1 xmmreg 2 |
| mem to xmmreg | 0000 1111:0101 0001 mod xmmreg r/m |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|--|
| SQRTSS—Compute Square Root of Scalar Single-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 0001:11 xmmreg1 xmmreg 2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 0001:mod xmmreg r/m |
| STMXCSR—Store MXCSR Register State | |
| MXCSR to mem | 0000 1111:1010 1110:mod ^A 011 mem |
| SUBPS—Subtract Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1100:mod xmmreg r/m |
| SUBSS—Subtract Scalar Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 1100:mod xmmreg r/m |
| UCOMISS—Unordered Compare Scalar Ordered Single-Precision Floating-Point Values and Set EFLAGS | |
| xmmreg to xmmreg | 0000 1111:0010 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0010 1110 mod xmmreg r/m |
| UNPCKHPS—Unpack and Interleave High Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0001 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0001 0101 mod xmmreg r/m |
| UNPCKLPS—Unpack and Interleave Low Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0001 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0001 0100 mod xmmreg r/m |
| XORPS—Bitwise Logical XOR of Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 0111:11 xmmreg1 xmmreg2 |

Table B-22. Formats and Encodings of SSE Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|------------------------|------------------------------------|
| mem to xmmreg | 0000 1111:0101 0111 mod xmmreg r/m |

Table B-23. Formats and Encodings of SSE Integer Instructions

| Instruction and Format | Encoding |
|--|--|
| PAVGB/PAVGW—Average Packed Integers | |
| mmreg to mmreg | 0000 1111:1110 0000:11 mmreg1 mmreg2 |
| | 0000 1111:1110 0011:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1110 0000 mod mmreg r/m |
| | 0000 1111:1110 0011 mod mmreg r/m |
| PEXTRW—Extract Word | |
| mmreg to reg32, imm8 | 0000 1111:1100 0101:11 r32 mmreg; imm8 |
| PINSRW—Insert Word | |
| reg32 to mmreg, imm8 | 0000 1111:1100 0100:11 mmreg r32; imm8 |
| m16 to mmreg, imm8 | 0000 1111:1100 0100 mod mmreg r/m; imm8 |
| PMAXSW—Maximum of Packed Signed Word Integers | |
| mmreg to mmreg | 0000 1111:1110 1110:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1110 1110 mod mmreg r/m |
| PMAXUB—Maximum of Packed Unsigned Byte Integers | |
| mmreg to mmreg | 0000 1111:1101 1110:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1101 1110 mod mmreg r/m |
| PMINSW—Minimum of Packed Signed Word Integers | |
| mmreg to mmreg | 0000 1111:1110 1010:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1110 1010 mod mmreg r/m |
| PMINUB—Minimum of Packed Unsigned Byte Integers | |
| mmreg to mmreg | 0000 1111:1101 1010:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1101 1010 mod mmreg r/m |
| PMOVMASKB—Move Byte Mask To Integer | |

Table B-23. Formats and Encodings of SSE Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| mmreg to reg32 | 0000 1111:1101 0111:11 r32 mmreg |
| PMULHUW—Multiply Packed Unsigned Integers and Store High Result | |
| mmreg to mmreg | 0000 1111:1110 0100:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1110 0100 mod mmreg r/m |
| PSADBW—Compute Sum of Absolute Differences | |
| mmreg to mmreg | 0000 1111:1111 0110:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1111 0110 mod mmreg r/m |
| PSHUFW—Shuffle Packed Words | |
| mmreg to mmreg, imm8 | 0000 1111:0111 0000:11 mmreg1 mmreg2: imm8 |
| mem to mmreg, imm8 | 0000 1111:0111 0000:11 mod mmreg r/m: imm8 |

Table B-24. Format and Encoding of SSE Cacheability & Memory Ordering Instructions

| Instruction and Format | Encoding |
|--|--|
| MASKMOVQ—Store Selected Bytes of Quadword | |
| mmreg to mmreg | 0000 1111:1111 0111:11 mmreg1 mmreg2 |
| MOVNTPS—Store Packed Single-Precision Floating-Point Values Using Non-Temporal Hint | |
| xmmreg to mem | 0000 1111:0010 1011: mod xmmreg r/m |
| MOVNTQ—Store Quadword Using Non-Temporal Hint | |
| mmreg to mem | 0000 1111:1110 0111: mod mmreg r/m |
| PREFETCHT0—Prefetch Temporal to All Cache Levels | 0000 1111:0001 1000:mod ^A 001 mem |
| PREFETCHT1—Prefetch Temporal to First Level Cache | 0000 1111:0001 1000:mod ^A 010 mem |
| PREFETCHT2—Prefetch Temporal to Second Level Cache | 0000 1111:0001 1000:mod ^A 011 mem |

Table B-24. Format and Encoding of SSE Cacheability & Memory Ordering Instructions (Contd.)

| Instruction and Format | Encoding |
|--|--|
| PREFETCHNTA—Prefetch Non-Temporal to All Cache Levels | 0000 1111:0001 1000:mod ^A 000 mem |
| SFENCE—Store Fence | 0000 1111:1010 1110:11 111 000 |

B.9 SSE2 INSTRUCTION FORMATS AND ENCODINGS

The SSE2 instructions use the ModR/M format and are preceded by the 0FH prefix byte. In general, operations are not duplicated to provide two directions (that is, separate load and store variants).

The following three tables show the formats and encodings for the SSE2 SIMD floating-point, SIMD integer, and cacheability instructions, respectively. Some SSE2 instructions require a mandatory prefix (66H, F2H, F3H) as part of the two-byte opcode. These prefixes are included in the tables.

B.9.1 Granularity Field (gg)

The granularity field (gg) indicates the size of the packed operands that the instruction is operating on. When this field is used, it is located in bits 1 and 0 of the second opcode byte. Table B-25 shows the encoding of this gg field.

Table B-25. Encoding of Granularity of Data Field (gg)

| gg | Granularity of Data |
|----|---------------------|
| 00 | Packed Bytes |
| 01 | Packed Words |
| 10 | Packed Doublewords |
| 11 | Quadword |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions

| Instruction and Format | Encoding |
|---|---|
| ADDPPD—Add Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1000: mod xmmreg r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| ADDSD—Add Scalar Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 1000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 1000: mod xmmreg r/m |
| ANDNPD—Bitwise Logical AND NOT of Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 0101: mod xmmreg r/m |
| ANDPD—Bitwise Logical AND of Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 0100: mod xmmreg r/m |
| CMPPD—Compare Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:1100 0010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:1100 0010: mod xmmreg r/m: imm8 |
| CMPSD—Compare Scalar Double-Precision Floating-Point Values | |
| xmmreg to xmmreg, imm8 | 1111 0010:0000 1111:1100 0010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 1111 010:0000 1111:1100 0010: mod xmmreg r/m: imm8 |
| COMISD—Compare Scalar Ordered Double-Precision Floating-Point Values and Set EFLAGS | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0010 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0010 1111: mod xmmreg r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|--|
| CVTPI2PD—Convert Packed Doubleword Integers to Packed Double-Precision Floating-Point Values | |
| mmreg to xmmreg | 0110 0110:0000 1111:0010 1010:11 xmmreg1 mmreg1 |
| mem to xmmreg | 0110 0110:0000 1111:0010 1010: mod xmmreg r/m |
| CVTPD2PI—Convert Packed Double-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to mmreg | 0110 0110:0000 1111:0010 1101:11 mmreg1 xmmreg1 |
| mem to mmreg | 0110 0110:0000 1111:0010 1101: mod mmreg r/m |
| CVTSI2SD—Convert Doubleword Integer to Scalar Double-Precision Floating-Point Value | |
| r32 to xmmreg1 | 1111 0010:0000 1111:0010 1010:11 xmmreg r32 |
| mem to xmmreg | 1111 0010:0000 1111:0010 1010: mod xmmreg r/m |
| CVTSD2SI—Convert Scalar Double-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 1111 0010:0000 1111:0010 1101:11 r32 xmmreg |
| mem to r32 | 1111 0010:0000 1111:0010 1101: mod r32 r/m |
| CVTTPD2PI—Convert with Truncation Packed Double-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to mmreg | 0110 0110:0000 1111:0010 1100:11 mmreg xmmreg |
| mem to mmreg | 0110 0110:0000 1111:0010 1100: mod mmreg r/m |
| CVTTSD2SI—Convert with Truncation Scalar Double-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 1111 0010:0000 1111:0010 1100:11 r32 xmmreg |
| mem to r32 | 1111 0010:0000 1111:0010 1100: mod r32 r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| CVTPD2PS—Covert Packed Double-Precision Floating-Point Values to Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1010: mod xmmreg r/m |
| CVTPS2PD—Covert Packed Single-Precision Floating-Point Values to Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1010: mod xmmreg r/m |
| CVTSD2SS—Covert Scalar Double-Precision Floating-Point Value to Scalar Single-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 1010: mod xmmreg r/m |
| CVTSS2SD—Covert Scalar Single-Precision Floating-Point Value to Scalar Double-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:00001 111:0101 1010: mod xmmreg r/m |
| CVTPD2DQ—Convert Packed Double-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to xmmreg | 1111 0010:0000 1111:1110 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:1110 0110: mod xmmreg r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| CVTTPD2DQ—Convert With Truncation Packed Double-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1110 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1110 0110: mod xmmreg r/m |
| CVTDQ2PD—Convert Packed Doubleword Integers to Packed Single-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0011:0000 1111:1110 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:1110 0110: mod xmmreg r/m |
| CVTPS2DQ—Convert Packed Single-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1011: mod xmmreg r/m |
| CVTTPS2DQ—Convert With Truncation Packed Single-Precision Floating-Point Values to Packed Doubleword Integers | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0101 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0101 1011: mod xmmreg r/m |
| CVTDQ2PS—Convert Packed Doubleword Integers to Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0000 1111:0101 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0000 1111:0101 1011: mod xmmreg r/m |
| DIVPD—Divide Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1110: mod xmmreg r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| DIVSD—Divide Scalar Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 1110: mod xmmreg r/m |
| MAXPD—Return Maximum Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1111: mod xmmreg r/m |
| MAXSD—Return Maximum Scalar Double-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 1111: mod xmmreg r/m |
| MINPD—Return Minimum Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1101: mod xmmreg r/m |
| MINSD—Return Minimum Scalar Double-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 1101: mod xmmreg r/m |
| MOVAPD—Move Aligned Packed Double-Precision Floating-Point Values | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:0010 1001:11 xmmreg2 xmmreg1 |
| mem to xmmreg1 | 0110 0110:0000 1111:0010 1001: mod xmmreg r/m |
| xmmreg1 to xmmreg2 | 0110 0110:0000 1111:0010 1000:11 xmmreg1 xmmreg2 |
| xmmreg1 to mem | 0110 0110:0000 1111:0010 1000: mod xmmreg r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| MOVHPD—Move High Packed Double-Precision Floating-Point Values | |
| mem to xmmreg | 0110 0110:0000 1111:0001 0111: mod xmmreg r/m |
| xmmreg to mem | 0110 0110:0000 1111:0001 0110: mod xmmreg r/m |
| MOVLPD—Move Low Packed Double-Precision Floating-Point Values | |
| mem to xmmreg | 0110 0110:0000 1111:0001 0011: mod xmmreg r/m |
| xmmreg to mem | 0110 0110:0000 1111:0001 0010: mod xmmreg r/m |
| MOVMSKPD—Extract Packed Double-Precision Floating-Point Sign Mask | |
| xmmreg to r32 | 0110 0110:0000 1111:0101 0000:11 r32 xmmreg |
| MOVSD—Move Scalar Double-Precision Floating-Point Values | |
| xmmreg2 to xmmreg1 | 1111 0010:0000 1111:0001 0001:11 xmmreg2 xmmreg1 |
| mem to xmmreg1 | 1111 0010:0000 1111:0001 0001: mod xmmreg r/m |
| xmmreg1 to xmmreg2 | 1111 0010:0000 1111:0001 0000:11 xmmreg1 xmmreg2 |
| xmmreg1 to mem | 1111 0010:0000 1111:0001 0000: mod xmmreg r/m |
| MOVUPD—Move Unaligned Packed Double-Precision Floating-Point Values | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:0001 0001:11 xmmreg2 xmmreg1 |
| mem to xmmreg1 | 0110 0110:0000 1111:0001 0001: mod xmmreg r/m |
| xmmreg1 to xmmreg2 | 0110 0110:0000 1111:0001 0000:11 xmmreg1 xmmreg2 |
| xmmreg1 to mem | 0110 0110:0000 1111:0001 0000: mod xmmreg r/m |
| MULPD—Multiply Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1001: mod xmmreg rm |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| MULSD—Multiply Scalar Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0010:00001111:01011001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:00001111:01011001: mod xmmreg r/m |
| ORPD—Bitwise Logical OR of Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 0110: mod xmmreg r/m |
| SHUFPD—Shuffle Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:1100 0110:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:1100 0110: mod xmmreg r/m: imm8 |
| SQRTPD—Compute Square Roots of Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 0001:11 xmmreg1 xmmreg 2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 0001: mod xmmreg r/m |
| SQRTSD—Compute Square Root of Scalar Double-Precision Floating-Point Value | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 0001:11 xmmreg1 xmmreg 2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 0001: mod xmmreg r/m |
| SUBPD—Subtract Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 1100: mod xmmreg r/m |

Table B-26. Formats and Encodings of SSE2 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| SUBSD—Subtract Scalar Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 1111 0010:0000 1111:0101 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0010:0000 1111:0101 1100: mod xmmreg r/m |
| UCOMISD—Unordered Compare Scalar Ordered Double-Precision Floating-Point Values and Set EFLAGS | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0010 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0010 1110: mod xmmreg r/m |
| UNPCKHPD—Unpack and Interleave High Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0001 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0001 0101: mod xmmreg r/m |
| UNPCKLPD—Unpack and Interleave Low Packed Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0001 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0001 0100: mod xmmreg r/m |
| XORPD—Bitwise Logical OR of Double-Precision Floating-Point Values | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0101 0111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0101 0111: mod xmmreg r/m |

Table B-27. Formats and Encodings of SSE2 Integer Instructions

| Instruction and Format | Encoding |
|---|--|
| MOVD—Move Doubleword | |
| reg to xmmreg | 0110 0110:0000 1111:0110 1110: 11 xmmreg reg |
| reg from xmmreg | 0110 0110:0000 1111:0111 1110: 11 xmmreg reg |
| mem to xmmreg | 0110 0110:0000 1111:0110 1110: mod xmmreg r/m |
| mem from xmmreg | 0110 0110:0000 1111:0111 1110: mod xmmreg r/m |
| MOVDQA—Move Aligned Double Quadword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0110 1111:11 xmmreg1 xmmreg2 |
| | 0110 0110:0000 1111:0111 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0110 1111: mod xmmreg r/m |
| mem from xmmreg | 0110 0110:0000 1111:0111 1111: mod xmmreg r/m |
| MOVDQU—Move Unaligned Double Quadword | |
| xmmreg to xmmreg | 1111 0011:0000 1111:0110 1111:11 xmmreg1 xmmreg2 |
| | 1111 0011:0000 1111:0111 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0110 1111: mod xmmreg r/m |
| mem from xmmreg | 1111 0011:0000 1111:0111 1111: mod xmmreg r/m |
| MOVQ2DQ—Move Quadword from MMX to XMM Register | |
| mmreg to xmmreg | 1111 0011:0000 1111:1101 0110:11 mmreg1 mmreg2 |
| MOVQ2Q—Move Quadword from XMM to MMX Register | |
| xmmreg to mmreg | 1111 0010:0000 1111:1101 0110:11 mmreg1 mmreg2 |
| MOVQ—Move Quadword | |
| xmmreg2 to xmmreg1 | 1111 0011:0000 1111:0111 1110: 11 xmmreg1 xmmreg2 |
| xmmreg2 from xmmreg1 | 0110 0110:0000 1111:1101 0110: 11 xmmreg1 xmmreg2 |
| mem to xmmreg | 1111 0011:0000 1111:0111 1110: mod xmmreg r/m |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| mem from xmmreg | 0110 0110:0000 1111:1101 0110: mod xmmreg r/m |
| PACKSSDW¹—Pack Dword To Word Data (signed with saturation) | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:0110 1011: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:0110 1011: mod xmmreg r/m |
| PACKSSWB—Pack Word To Byte Data (signed with saturation) | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:0110 0011: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:0110 0011: mod xmmreg r/m |
| PACKUSWB—Pack Word To Byte Data (unsigned with saturation) | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:0110 0111: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:0110 0111: mod xmmreg r/m |
| PADDQ—Add Packed Quadword Integers | |
| mmreg to mmreg | 0000 1111:1101 0100:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1101 0100: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:1101 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1101 0100: mod xmmreg r/m |
| PADD—Add With Wrap-around | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111: 1111 11gg: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111: 1111 11gg: mod xmmreg r/m |
| PADDSS—Add Signed With Saturation | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111: 1110 11gg: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111: 1110 11gg: mod xmmreg r/m |
| PADDUS—Add Unsigned With Saturation | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111: 1101 11gg: 11 xmmreg1 xmmreg2 |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|---|--|
| memory to xmmreg | 0110 0110:0000 1111: 1101 11gg: mod xmmreg r/m |
| PAND—Bitwise And | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1101 1011: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1101 1011: mod xmmreg r/m |
| PANDN—Bitwise AndNot | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1101 1111: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1101 1111: mod xmmreg r/m |
| PAVGB—Average Packed Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:11100 000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 01100110:00001111:11100000 mod xmmreg r/m |
| PAVGW—Average Packed Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1110 0011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1110 0011 mod xmmreg r/m |
| PCMPEQ—Packed Compare For Equality | |
| xmmreg1 with xmmreg2 | 0110 0110:0000 1111:0111 01gg: 11 xmmreg1 xmmreg2 |
| xmmreg with memory | 0110 0110:0000 1111:0111 01gg: mod xmmreg r/m |
| PCMPGT—Packed Compare Greater (signed) | |
| xmmreg1 with xmmreg2 | 0110 0110:0000 1111:0110 01gg: 11 xmmreg1 xmmreg2 |
| xmmreg with memory | 0110 0110:0000 1111:0110 01gg: mod xmmreg r/m |
| PEXTRW—Extract Word | |
| xmmreg to reg32, imm8 | 0110 0110:0000 1111:1100 0101:11 r32 xmmreg: imm8 |
| PINSRW—Insert Word | |
| reg32 to xmmreg, imm8 | 0110 0110:0000 1111:1100 0100:11 xmmreg r32: imm8 |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|--|---|
| m16 to xmmreg, imm8 | 0110 0110:0000 1111:1100 0100 mod xmmreg r/m: imm8 |
| PMADDWD—Packed Multiply Add | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1111 0101: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1111 0101: mod xmmreg r/m |
| PMAxSW—Maximum of Packed Signed Word Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1110 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 01100110:00001111:11101110 mod xmmreg r/m |
| PMAxUB—Maximum of Packed Unsigned Byte Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1101 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1101 1110 mod xmmreg r/m |
| PMINSW—Minimum of Packed Signed Word Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1110 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1110 1010 mod xmmreg r/m |
| PMINUB—Minimum of Packed Unsigned Byte Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1101 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1101 1010 mod xmmreg r/m |
| PMOVMskB—Move Byte Mask To Integer | |
| xmmreg to reg32 | 0110 0110:0000 1111:1101 0111:11 r32 xmmreg |
| PMULHUW—Packed multiplication, store high word (unsigned) | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1110 0100: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1110 0100: mod xmmreg r/m |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| PMULHW—Packed Multiplication, store high word | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1110 0101: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1110 0101: mod xmmreg r/m |
| PMULLW—Packed Multiplication, store low word | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1101 0101: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1101 0101: mod xmmreg r/m |
| PMULUDQ—Multiply Packed Unsigned Doubleword Integers | |
| mmreg to mmreg | 0000 1111:1111 0100:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1111 0100: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:00001111:1111 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:00001111:1111 0100: mod xmmreg r/m |
| POR—Bitwise Or | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1110 1011: 11 xmmreg1 xmmreg2 |
| xmemory to xmmreg | 0110 0110:0000 1111:1110 1011: mod xmmreg r/m |
| PSADBW—Compute Sum of Absolute Differences | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1111 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1111 0110: mod xmmreg r/m |
| PSHUFLW—Shuffle Packed Low Words | |
| xmmreg to xmmreg, imm8 | 1111 0010:0000 1111:0111 0000:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 1111 0010:0000 1111:0111 0000:11 mod xmmreg r/m: imm8 |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|---|---|
| PSHUFHW—Shuffle Packed High Words | |
| xmmreg to xmmreg, imm8 | 1111 0011:0000 1111:0111 0000:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 1111 0011:0000 1111:0111 0000:11 mod xmmreg r/m: imm8 |
| PSHUFD—Shuffle Packed Doublewords | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0111 0000:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0111 0000:11 mod xmmreg r/m: imm8 |
| PSLLDQ—Shift Double Quadword Left Logical | |
| xmmreg, imm8 | 0110 0110:0000 1111:0111 0011:11 111 xmmreg: imm8 |
| PSLL—Packed Shift Left Logical | |
| xmmreg1 by xmmreg2 | 0110 0110:0000 1111:1111 00gg: 11 xmmreg1 xmmreg2 |
| xmmreg by memory | 0110 0110:0000 1111:1111 00gg: mod xmmreg r/m |
| xmmreg by immediate | 0110 0110:0000 1111:0111 00gg: 11 110 xmmreg: imm8 |
| PSRA—Packed Shift Right Arithmetic | |
| xmmreg1 by xmmreg2 | 0110 0110:0000 1111:1110 00gg: 11 xmmreg1 xmmreg2 |
| xmmreg by memory | 0110 0110:0000 1111:1110 00gg: mod xmmreg r/m |
| xmmreg by immediate | 0110 0110:0000 1111:0111 00gg: 11 100 xmmreg: imm8 |
| PSRLDQ—Shift Double Quadword Right Logical | |
| xmmreg, imm8 | 0110 0110:00001111:01110011:11 011 xmmreg: imm8 |
| PSRL—Packed Shift Right Logical | |
| xmmxreg1 by xmmxreg2 | 0110 0110:0000 1111:1101 00gg: 11 xmmreg1 xmmreg2 |
| xmmxreg by memory | 0110 0110:0000 1111:1101 00gg: mod xmmreg r/m |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|---|--|
| xmmreg by immediate | 0110 0110:0000 1111:0111 00gg: 11 010 xmmreg: imm8 |
| PSUBQ—Subtract Packed Quadword Integers | |
| mmreg to mmreg | 0000 1111:11111 011:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:1111 1011: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:1111 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:1111 1011: mod xmmreg r/m |
| PSUB—Subtract With Wrap-around | |
| xmmreg2 from xmmreg1 | 0110 0110:0000 1111:1111 10gg: 11 xmmreg1 xmmreg2 |
| memory from xmmreg | 0110 0110:0000 1111:1111 10gg: mod xmmreg r/m |
| PSUBS—Subtract Signed With Saturation | |
| xmmreg2 from xmmreg1 | 0110 0110:0000 1111:1110 10gg: 11 xmmreg1 xmmreg2 |
| memory from xmmreg | 0110 0110:0000 1111:1110 10gg: mod xmmreg r/m |
| PSUBUS—Subtract Unsigned With Saturation | |
| xmmreg2 from xmmreg1 | 0000 1111:1101 10gg: 11 xmmreg1 xmmreg2 |
| memory from xmmreg | 0000 1111:1101 10gg: mod xmmreg r/m |
| PUNPCKH—Unpack High Data To Next Larger Type | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0110 10gg:11 xmmreg1 Xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0110 10gg: mod xmmreg r/m |
| PUNPCKHQDQ—Unpack High Data | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0110 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0110 1101: mod xmmreg r/m |
| PUNPCKL—Unpack Low Data To Next Larger Type | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0110 00gg:11 xmmreg1 xmmreg2 |

Table B-27. Formats and Encodings of SSE2 Integer Instructions (Contd.)

| Instruction and Format | Encoding |
|-----------------------------------|--|
| mem to xmmreg | 0110 0110:0000 1111:0110 00gg: mod xmmreg r/m |
| PUNPCKLQDQ—Unpack Low Data | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0110 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0110 1100: mod xmmreg r/m |
| PXOR—Bitwise Xor | |
| xmmreg2 to xmmreg1 | 0110 0110:0000 1111:1110 1111: 11 xmmreg1 xmmreg2 |
| memory to xmmreg | 0110 0110:0000 1111:1110 1111: mod xmmreg r/m |

Table B-28. Format and Encoding of SSE2 Cacheability Instructions

| Instruction and Format | Encoding |
|--|---|
| MASKMOVDQU—Store Selected Bytes of Double Quadword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:1111 0111:11 xmmreg1 xmmreg2 |
| CLFLUSH—Flush Cache Line | |
| mem | 0000 1111:1010 1110:mod r/m |
| MOVNTPD—Store Packed Double-Precision Floating-Point Values Using Non-Temporal Hint | |
| xmmreg to mem | 0110 0110:0000 1111:0010 1011: mod xmmreg r/m |
| MOVNTDQ—Store Double Quadword Using Non-Temporal Hint | |
| xmmreg to mem | 0110 0110:0000 1111:1110 0111: mod xmmreg r/m |
| MOVNTI—Store Doubleword Using Non-Temporal Hint | |
| reg to mem | 0000 1111:1100 0011: mod reg r/m |
| PAUSE—Spin Loop Hint | 1111 0011:1001 0000 |
| LFENCE—Load Fence | 0000 1111:1010 1110: 11 101 000 |
| MFENCE—Memory Fence | 0000 1111:1010 1110: 11 110 000 |

B.10 SSE3 FORMATS AND ENCODINGS TABLE

The tables in this section provide SSE3 formats and encodings. Some SSE3 instructions require a mandatory prefix (66H, F2H, F3H) as part of the two-byte opcode. These prefixes are included in the tables.

When in IA-32e mode, use of the REX.R prefix permits instructions that use general purpose and XMM registers to access additional registers. Some instructions require the REX.W prefix to promote the instruction to 64-bit operation. Instructions that require the REX.W prefix are listed (with their opcodes) in Section B.12.

Table B-29. Formats and Encodings of SSE3 Floating-Point Instructions

| Instruction and Format | Encoding |
|--|--|
| ADDSD—Add /Sub packed DP FP numbers from XMM2/Mem to XMM1 | |
| xmmreg2 to xmmreg1 | 01100110:00001111:11010000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 01100110:00001111:11010000: mod xmmreg r/m |
| ADDSS—Add /Sub packed SP FP numbers from XMM2/Mem to XMM1 | |
| xmmreg2 to xmmreg1 | 11110010:00001111:11010000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 11110010:00001111:11010000: mod xmmreg r/m |
| HADDSD—Add horizontally packed DP FP numbers XMM2/Mem to XMM1 | |
| xmmreg2 to xmmreg1 | 01100110:00001111:01111100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 01100110:00001111:01111100: mod xmmreg r/m |
| HADDSS—Add horizontally packed SP FP numbers XMM2/Mem to XMM1 | |
| xmmreg2 to xmmreg1 | 11110010:00001111:01111100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 11110010:00001111:01111100: mod xmmreg r/m |
| HSUBSD—Sub horizontally packed DP FP numbers XMM2/Mem to XMM1 | |
| xmmreg2 to xmmreg1 | 01100110:00001111:01111101:11 xmmreg1 xmmreg2 |

Table B-29. Formats and Encodings of SSE3 Floating-Point Instructions (Contd.)

| Instruction and Format | Encoding |
|--|--|
| mem to xmmreg | 01100110:00001111:01111101: mod xmmreg r/m |
| HSUBPS—Sub horizontally packed SP FP numbers XMM2/Mem to XMM1 | |
| xmmreg2 to xmmreg1 | 11110010:00001111:01111101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 11110010:00001111:01111101: mod xmmreg r/m |

Table B-30. Formats and Encodings for SSE3 Event Management Instructions

| Instruction and Format | Encoding |
|--|----------------------------------|
| MONITOR—Set up a linear address range to be monitored by hardware | |
| eax, ecx, edx | 0000 1111 : 0000 0001:11 001 000 |
| MWAIT—Wait until write-back store performed within the range specified by the instruction MONITOR | |
| eax, ecx | 0000 1111 : 0000 0001:11 001 001 |

Table B-31. Formats and Encodings for SSE3 Integer and Move Instructions

| Instruction and Format | Encoding |
|--|--|
| FISTTP—Store ST in int16 (chop) and pop | |
| m16int | 11011 111 : mod ^A 001 r/m |
| FISTTP—Store ST in int32 (chop) and pop | |
| m32int | 11011 011 : mod ^A 001 r/m |
| FISTTP—Store ST in int64 (chop) and pop | |
| m64int | 11011 101 : mod ^A 001 r/m |
| LDDQU—Load unaligned integer 128-bit | |
| xmm, m128 | 11110010:00001111:11110000: mod ^A xmmreg r/m |
| MOVDDUP—Move 64 bits representing one DP data from XMM2/Mem to XMM1 and duplicate | |
| xmmreg2 to xmmreg1 | 11110010:00001111:00010010:11 xmmreg1 xmmreg2 |

Table B-31. Formats and Encodings for SSE3 Integer and Move Instructions (Contd.)

| Instruction and Format | Encoding |
|---|--|
| mem to xmmreg | 11110010:00001111:00010010: mod xmmreg r/m |
| MOVSHDUP—Move 128 bits representing 4 SP data from XMM2/Mem to XMM1 and duplicate high | |
| xmmreg2 to xmmreg1 | 11110011:00001111:00010110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 11110011:00001111:00010110: mod xmmreg r/m |
| MOVSLDUP—Move 128 bits representing 4 SP data from XMM2/Mem to XMM1 and duplicate low | |
| xmmreg2 to xmmreg1 | 11110011:00001111:00010010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 11110011:00001111:00010010: mod xmmreg r/m |

B.11 SSSE3 FORMATS AND ENCODING TABLE

The tables in this section provide SSSE3 formats and encodings. Some SSSE3 instructions require a mandatory prefix (66H) as part of the three-byte opcode. These prefixes are included in the table below.

Table B-32. Formats and Encodings for SSSE3 Instructions

| Instruction and Format | Encoding |
|---|--|
| PABSB—Packed Absolute Value Bytes | |
| mmreg to mmreg | 0000 1111:0011 1000: 0001 1100:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0001 1100: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 1100: mod xmmreg r/m |
| PABSD—Packed Absolute Value Double Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0001 1110:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0001 1110: mod mmreg r/m |

Table B-32. Formats and Encodings for SSSE3 Instructions (Contd.)

| Instruction and Format | Encoding |
|---|--|
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 1110: mod xmmreg r/m |
| PABSW—Packed Absolute Value Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0001 1101:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0001 1101: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 1101: mod xmmreg r/m |
| PALIGNR—Packed Align Right | |
| mmreg to mmreg | 0000 1111:0011 1010: 0000 1111:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1010: 0000 1111: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1010: 0000 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0000 1111: mod xmmreg r/m |
| PHADDD—Packed Horizontal Add Double Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0010:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0010: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0010: mod xmmreg r/m |
| PHADDSW—Packed Horizontal Add and Saturate | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0011:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0011: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0011: mod xmmreg r/m |

Table B-32. Formats and Encodings for SSE3 Instructions (Contd.)

| Instruction and Format | Encoding |
|--|--|
| PHADDW—Packed Horizontal Add Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0001:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0001: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0001: mod xmmreg r/m |
| PHSUBD—Packed Horizontal Subtract Double Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0110:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0110: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0110: mod xmmreg r/m |
| PHSUBSW—Packed Horizontal Subtract and Saturate | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0111:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0111: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0111: mod xmmreg r/m |
| PHSUBW—Packed Horizontal Subtract Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0101:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0101: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0101: mod xmmreg r/m |
| PMADDUBSW—Multiply and Add Packed Signed and Unsigned Bytes | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0100:11 mmreg1 mmreg2 |

Table B-32. Formats and Encodings for SSSE3 Instructions (Contd.)

| Instruction and Format | Encoding |
|--|--|
| mem to mmreg | 0000 1111:0011 1000: 0000 0100: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0100: mod xmmreg r/m |
| PMULHRW—Packed Multiply Hlgn with Round and Scale | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 1011:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 1011: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1011: mod xmmreg r/m |
| PSHUFB—Packed Shuffle Bytes | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 0000:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 0000: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 0000: mod xmmreg r/m |
| PSIGNB—Packed Sign Bytes | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 1000:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 1000: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1000: mod xmmreg r/m |
| PSIGND—Packed Sign Double Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 1010:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 1010: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1010: mod xmmreg r/m |

Table B-32. Formats and Encodings for SSE3 Instructions (Contd.)

| Instruction and Format | Encoding |
|---------------------------------|--|
| PSIGNW—Packed Sign Words | |
| mmreg to mmreg | 0000 1111:0011 1000: 0000 1001:11 mmreg1 mmreg2 |
| mem to mmreg | 0000 1111:0011 1000: 0000 1001: mod mmreg r/m |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0000 1001: mod xmmreg r/m |

B.12 SPECIAL ENCODINGS FOR 64-BIT MODE

The following Pentium, P6, MMX, SSE, SSE2, SSE3 instructions are promoted to 64-bit operation in IA-32e mode by using REX.W. However, these entries are special cases that do not follow the general rules (specified in Section B.4).

Table B-33. Special Case Instructions Promoted Using REX.W

| Instruction and Format | Encoding |
|--|---|
| CMOVcc—Conditional Move | |
| register2 to register1 | 0100 0ROB 0000 1111: 0100 ttn : 11 reg1 reg2 |
| qwordregister2 to qwordregister1 | 0100 1ROB 0000 1111: 0100 ttn : 11 qwordreg1 qwordreg2 |
| memory to register | 0100 0RXB 0000 1111 : 0100 ttn : mod reg r/m |
| memory64 to qwordregister | 0100 1RXB 0000 1111 : 0100 ttn : mod qwordreg r/m |
| CVTSD2SI—Convert Scalar Double-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 0100 0ROB 1111 0010:0000 1111:0010 1101:11 r32 xmmreg |
| xmmreg to r64 | 0100 1ROB 1111 0010:0000 1111:0010 1101:11 r64 xmmreg |
| mem64 to r32 | 0100 0ROXB 1111 0010:0000 1111:0010 1101: mod r32 r/m |
| mem64 to r64 | 0100 1RXB 1111 0010:0000 1111:0010 1101: mod r64 r/m |

Table B-33. Special Case Instructions Promoted Using REX.W (Contd.)

| Instruction and Format | Encoding |
|---|--|
| CVTSI2SS—Convert Doubleword Integer to Scalar Single-Precision Floating-Point Value | |
| r32 to xmmreg1 | 0100 0ROB 1111 0011:0000 1111:0010 1010:11 xmmreg r32 |
| r64 to xmmreg1 | 0100 1ROB 1111 0011:0000 1111:0010 1010:11 xmmreg r64 |
| mem to xmmreg | 0100 0RXB 1111 0011:0000 1111:0010 1010: mod xmmreg r/m |
| mem64 to xmmreg | 0100 1RXB 1111 0011:0000 1111:0010 1010: mod xmmreg r/m |
| CVTSI2SD—Convert Doubleword Integer to Scalar Double-Precision Floating-Point Value | |
| r32 to xmmreg1 | 0100 0ROB 1111 0010:0000 1111:0010 1010:11 xmmreg r32 |
| r64 to xmmreg1 | 0100 1ROB 1111 0010:0000 1111:0010 1010:11 xmmreg r64 |
| mem to xmmreg | 0100 0RXB 1111 0010:0000 1111:00101 010: mod xmmreg r/m |
| mem64 to xmmreg | 0100 1RXB 1111 0010:0000 1111:0010 1010: mod xmmreg r/m |
| CVTSS2SI—Convert Scalar Single-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 0100 0ROB 1111 0011:0000 1111:0010 1101:11 r32 xmmreg |
| xmmreg to r64 | 0100 1ROB 1111 0011:0000 1111:0010 1101:11 r64 xmmreg |
| mem to r32 | 0100 0RXB 11110011:00001111:00101101: mod r32 r/m |
| mem32 to r64 | 0100 1RXB 1111 0011:0000 1111:0010 1101: mod r64 r/m |
| CVTTSD2SI—Convert with Truncation Scalar Double-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 0100 0ROB 11110010:00001111:00101100:11 r32 xmmreg |

Table B-33. Special Case Instructions Promoted Using REX.W (Contd.)

| Instruction and Format | Encoding |
|---|---|
| xmmreg to r64 | 0100 1ROB 1111 0010:0000 1111:0010 1100:11 r64 xmmreg |
| mem64 to r32 | 0100 0RXB 1111 0010:0000 1111:0010 1100: mod r32 r/m |
| mem64 to r64 | 0100 1RXB 1111 0010:0000 1111:0010 1100: mod r64 r/m |
| CVTTSS2SI—Convert with Truncation Scalar Single-Precision Floating-Point Value to Doubleword Integer | |
| xmmreg to r32 | 0100 0ROB 1111 0011:0000 1111:0010 1100:11 r32 xmmreg1 |
| xmmreg to r64 | 0100 1ROB 1111 0011:0000 1111:0010 1100:11 r64 xmmreg1 |
| mem to r32 | 0100 0RXB 1111 0011:0000 1111:0010 1100: mod r32 r/m |
| mem32 to r64 | 0100 1RXB 1111 0011:0000 1111:0010 1100: mod r64 r/m |
| MOVD/MOVQ—Move doubleword | |
| reg to mmxreg | 0100 0ROB 0000 1111:0110 1110: 11 mmxreg reg |
| qwordreg to mmxreg | 0100 1ROB 0000 1111:0110 1110: 11 mmxreg qwordreg |
| reg from mmxreg | 0100 0ROB 0000 1111:0111 1110: 11 mmxreg reg |
| qwordreg from mmxreg | 0100 1ROB 0000 1111:0111 1110: 11 mmxreg qwordreg |
| mem to mmxreg | 0100 0RXB 0000 1111:0110 1110: mod mmxreg r/m |
| mem64 to mmxreg | 0100 1RXB 0000 1111:0110 1110: mod mmxreg r/m |
| mem from mmxreg | 0100 0RXB 0000 1111:0111 1110: mod mmxreg r/m |
| mem64 from mmxreg | 0100 1RXB 0000 1111:0111 1110: mod mmxreg r/m |
| mmxreg with memory | 0100 0RXB 0000 1111:0110 01gg: mod mmxreg r/m |

Table B-33. Special Case Instructions Promoted Using REX.W (Contd.)

| Instruction and Format | Encoding |
|--|---|
| MOVMSKPS—Extract Packed Single-Precision Floating-Point Sign Mask | |
| xmmreg to r32 | 0100 0ROB 0000 1111:0101 0000:11 r32 xmmreg |
| xmmreg to r64 | 0100 1ROB 00001111:01010000:11 r64 xmmreg |
| PEXTRW—Extract Word | |
| mmreg to reg32, imm8 | 0100 0ROB 0000 1111:1100 0101:11 r32 mmreg: imm8 |
| mmreg to reg64, imm8 | 0100 1ROB 0000 1111:1100 0101:11 r64 mmreg: imm8 |
| xmmreg to reg32, imm8 | 0100 0ROB 0110 0110 0000 1111:1100 0101:11 r32 xmmreg: imm8 |
| xmmreg to reg64, imm8 | 0100 1ROB 0110 0110 0000 1111:1100 0101:11 r64 xmmreg: imm8 |
| PINSRW—Insert Word | |
| reg32 to mmreg, imm8 | 0100 0ROB 0000 1111:1100 0100:11 mmreg r32: imm8 |
| reg64 to mmreg, imm8 | 0100 1ROB 0000 1111:1100 0100:11 mmreg r64: imm8 |
| m16 to mmreg, imm8 | 0100 0ROB 0000 1111:1100 0100 mod mmreg r/m: imm8 |
| m16 to mmreg, imm8 | 0100 1RXB 0000 1111:11000100 mod mmreg r/m: imm8 |
| reg32 to xmmreg, imm8 | 0100 0RXB 0110 0110 0000 1111:1100 0100:11 xmmreg r32: imm8 |
| reg64 to xmmreg, imm8 | 0100 0RXB 0110 0110 0000 1111:1100 0100:11 xmmreg r64: imm8 |
| m16 to xmmreg, imm8 | 0100 0RXB 0110 0110 0000 1111:1100 0100 mod xmmreg r/m: imm8 |
| m16 to xmmreg, imm8 | 0100 1RXB 0110 0110 0000 1111:1100 0100 mod xmmreg r/m: imm8 |
| PMOVMASKB—Move Byte Mask To Integer | |
| mmreg to reg32 | 0100 0RXB 0000 1111:1101 0111:11 r32 mmreg |

Table B-33. Special Case Instructions Promoted Using REX.W (Contd.)

| Instruction and Format | Encoding |
|------------------------|---|
| mmreg to reg64 | 0100 1ROB 0000 1111:1101 0111:11 r64 mmreg |
| xmmreg to reg32 | 0100 0RXB 0110 0110 0000 1111:1101 0111:11 r32 mmreg |
| xmmreg to reg64 | 0110 0110 0000 1111:1101 0111:11 r64 xmmreg |

B.13 SSE4.1 FORMATS AND ENCODING TABLE

The tables in this section provide SSE4.1 formats and encodings. Some SSE4.1 instructions require a mandatory prefix (66H, F2H, F3H) as part of the three-byte opcode. These prefixes are included in the tables.

In 64-bit mode, some instructions requires REX.W, the byte sequence of REX.W prefix in the opcode sequence is shown.

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|---|--|
| BLENDPD — Blend Packed Double-Precision Floats | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1010: 0000 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0000 1101: mod xmmreg r/m |
| BLENDPS — Blend Packed Single-Precision Floats | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1010: 0000 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0000 1100: mod xmmreg r/m |
| BLENDVPD — Variable Blend Packed Double-Precision Floats | |
| xmmreg to xmmreg <xmm0> | 0110 0110:0000 1111:0011 1000: 0001 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg <xmm0> | 0110 0110:0000 1111:0011 1000: 0001 0101: mod xmmreg r/m |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|---|--|
| BLENDVPS – Variable Blend Packed Single-Precision Floats | |
| xmmreg to xmmreg <ymm0> | 0110 0110:0000 1111:0011 1000: 0001 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg <ymm0> | 0110 0110:0000 1111:0011 1000: 0001 0100: mod xmmreg r/m |
| DPPD – Packed Double-Precision Dot Products | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0100 0001:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0100 0001: mod xmmreg r/m: imm8 |
| DPPS – Packed Single-Precision Dot Products | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0100 0000:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0100 0000: mod xmmreg r/m: imm8 |
| EXTRACTPS – Extract From Packed Single-Precision Floats | |
| reg from xmmreg , imm8 | 0110 0110:0000 1111:0011 1010: 0001 0111:11 reg xmmreg: imm8 |
| mem from xmmreg , imm8 | 0110 0110:0000 1111:0011 1010: 0001 0111: mod r/m xmmreg: imm8 |
| INSERTPS – Insert Into Packed Single-Precision Floats | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0010 0001:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0010 0001: mod xmmreg r/m: imm8 |
| MOVNTDQA – Load Double Quadword Non-temporal Aligned | |
| m128 to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1010:11 r/m xmmreg2 |
| MPSADBW – Multiple Packed Sums of Absolute Difference | |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|---|--|
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0100 0010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0100 0010: mod xmmreg r/m: imm8 |
| PACKUSDW — Pack with Unsigned Saturation | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1011: mod xmmreg r/m |
| PBLENDVB — Variable Blend Packed Bytes | |
| xmmreg to xmmreg <ymm0> | 0110 0110:0000 1111:0011 1000: 0001 0000:11 xmmreg1 xmmreg2 |
| mem to xmmreg <ymm0> | 0110 0110:0000 1111:0011 1000: 0001 0000: mod xmmreg r/m |
| PBLENDW — Blend Packed Words | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0001 1110:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1110: mod xmmreg r/m: imm8 |
| PCMPEQQ — Compare Packed Qword Data of Equal | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1001: mod xmmreg r/m |
| PEXTRB — Extract Byte | |
| reg from xmmreg , imm8 | 0110 0110:0000 1111:0011 1010: 0001 0100:11 reg xmmreg: imm8 |
| xmmreg to mem, imm8 | 0110 0110:0000 1111:0011 1010: 0001 0100: mod xmmreg r/m: imm8 |
| PEXTRD — Extract DWord | |
| reg from xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0001 0110:11 reg xmmreg: imm8 |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|--|---|
| xmmreg to mem, imm8 | 0110 0110:0000 1111:0011 1010: 0001 0110: mod xmmreg r/m: imm8 |
| PEXTRQ — Extract QWord | |
| r64 from xmmreg, imm8 | 0110 0110:REX.W:0000 1111:0011 1010: 0001 0110:11 reg xmmreg: imm8 |
| m64 from xmmreg, imm8 | 0110 0110:REX.W:0000 1111:0011 1010: 0001 0110: mod xmmreg r/m: imm8 |
| PEXTRW — Extract Word | |
| reg from xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0001 0101:11 reg xmmreg: imm8 |
| mem from xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0001 0101: mod xmmreg r/m: imm8 |
| PHMINPOSUW — Packed Horizontal Word Minimum | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0100 0001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0100 0001: mod xmmreg r/m |
| PINSRB — Extract Byte | |
| reg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0010 0000:11 xmmreg reg: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0010 0000: mod xmmreg r/m: imm8 |
| PINSRD — Extract DWord | |
| reg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0010 0010:11 xmmreg reg: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0010 0010: mod xmmreg r/m: imm8 |
| PINSRQ — Extract QWord | |
| r64 to xmmreg, imm8 | 0110 0110:REX.W:0000 1111:0011 1010: 0010 0010:11 xmmreg reg: imm8 |
| m64 to xmmreg, imm8 | 0110 0110:REX.W:0000 1111:0011 1010: 0010 0010: mod xmmreg r/m: imm8 |
| PMAXSB — Maximum of Packed Signed Byte Integers | |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|---|--|
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1100: mod xmmreg r/m |
| PMAXSD – Maximum of Packed Signed Dword Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1101: mod xmmreg r/m |
| PMAXUD – Maximum of Packed Unsigned Dword Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1111: mod xmmreg r/m |
| PMAXUW – Maximum of Packed Unsigned Word Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1110:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1110: mod xmmreg r/m |
| PMINSB – Minimum of Packed Signed Byte Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1000: mod xmmreg r/m |
| PMINSD – Minimum of Packed Signed Dword Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1001: mod xmmreg r/m |
| PMINUD – Minimum of Packed Unsigned Dword Integers | |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|---|--|
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1011: mod xmmreg r/m |
| PMINUW – Minimum of Packed Unsigned Word Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 1010: mod xmmreg r/m |
| PMOVSXBD – Packed Move Sign Extend - Byte to Dword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0001: mod xmmreg r/m |
| PMOVSXBQ – Packed Move Sign Extend - Byte to Qword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0010: mod xmmreg r/m |
| PMOVSXBW – Packed Move Sign Extend - Byte to Word | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0000: mod xmmreg r/m |
| PMOVSXWD – Packed Move Sign Extend - Word to Dword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0011: mod xmmreg r/m |
| PMOVSXWQ – Packed Move Sign Extend - Word to Qword | |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|--|--|
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0100: mod xmmreg r/m |
| PMOVSXDQ – Packed Move Sign Extend - Dword to Qword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 0101: mod xmmreg r/m |
| PMOVZXBQ – Packed Move Zero Extend - Byte to Dword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0001:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0001: mod xmmreg r/m |
| PMOVZXBQ – Packed Move Zero Extend - Byte to Qword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0010:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0010: mod xmmreg r/m |
| PMOVZXBW – Packed Move Zero Extend - Byte to Word | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0000: mod xmmreg r/m |
| PMOVZXWD – Packed Move Zero Extend - Word to Dword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0011:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0011: mod xmmreg r/m |
| PMOVZXWQ – Packed Move Zero Extend - Word to Qword | |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|---|--|
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0100:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0100: mod xmmreg r/m |
| PMOVZXDQ – Packed Move Zero Extend - Dword to Qword | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0101:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0101: mod xmmreg r/m |
| PMULDQ – Multiply Packed Signed Dword Integers | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0010 1000: mod xmmreg r/m |
| PMULLD – Multiply Packed Signed Dword Integers, Store low Result | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0100 0000:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0100 0000: mod xmmreg r/m |
| PTEST – Logical Compare | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 0111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0001 0111: mod xmmreg r/m |
| ROUNDPD – Round Packed Double-Precision Values | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1001:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1001: mod xmmreg r/m: imm8 |
| ROUNDPS – Round Packed Single-Precision Values | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1000:11 xmmreg1 xmmreg2: imm8 |

Table B-34. Encodings of SSE4.1 instructions

| Instruction and Format | Encoding |
|--|--|
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1000: mod xmmreg r/m: imm8 |
| ROUNDSD — Round Scalar Double-Precision Value | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1011:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1011: mod xmmreg r/m: imm8 |
| ROUNDSS — Round Scalar Single-Precision Value | |
| xmmreg to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg, imm8 | 0110 0110:0000 1111:0011 1010: 0000 1010: mod xmmreg r/m: imm8 |

B.14 SSE4.2 FORMATS AND ENCODING TABLE

The tables in this section provide SSE4.2 formats and encodings. Some SSE4.2 instructions require a mandatory prefix (66H, F2H, F3H) as part of the three-byte opcode. These prefixes are included in the tables. In 64-bit mode, some instructions requires REX.W, the byte sequence of REX.W prefix in the opcode sequence is shown.

Table B-35. Encodings of SSE4.2 instructions

| Instruction and Format | Encoding |
|--------------------------|---|
| CRC32 — Accumulate CRC32 | |
| reg2 to reg1 | 1111 0010:0000 1111:0011 1000: 1111 000w :11 reg1 reg2 |
| mem to reg | 1111 0010:0000 1111:0011 1000: 1111 000w : mod reg r/m |
| bytereg2 to reg1 | 1111 0010:0100 WROB:0000 1111:0011 1000: 1111 0000 :11 reg1 bytereg2 |
| m8 to reg | 1111 0010:0100 WROB:0000 1111:0011 1000: 1111 0000 : mod reg r/m |
| qwreg2 to qwreg1 | 1111 0010:0100 1ROB:0000 1111:0011 1000: 1111 0000 :11 qwreg1 qwreg2 |

Table B-35. Encodings of SSE4.2 instructions

| Instruction and Format | Encoding |
|--|--|
| mem64 to qwreg | 1111 0010:0100 1R0B:0000 1111:0011 1000: 1111 0000 : mod qwreg r/m |
| PCMPESTRI— Packed Compare Explicit-Length Strings To Index | |
| xmmreg2 to xmmreg1, imm8 | 0110 0110:0000 1111:0011 1010: 0110 0001:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0110 0001: mod xmmreg r/m |
| PCMPESTRM— Packed Compare Explicit-Length Strings To Mask | |
| xmmreg2 to xmmreg1, imm8 | 0110 0110:0000 1111:0011 1010: 0110 0000:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0110 0000: mod xmmreg r/m |
| PCMPISTRI— Packed Compare Implicit-Length String To Index | |
| xmmreg2 to xmmreg1, imm8 | 0110 0110:0000 1111:0011 1010: 0110 0011:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0110 0011: mod xmmreg r/m |
| PCMPISTRM— Packed Compare Implicit-Length Strings To Mask | |
| xmmreg2 to xmmreg1, imm8 | 0110 0110:0000 1111:0011 1010: 0110 0010:11 xmmreg1 xmmreg2: imm8 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1010: 0110 0010: mod xmmreg r/m |
| PCMPGTQ— Packed Compare Greater Than | |
| xmmreg to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0111:11 xmmreg1 xmmreg2 |
| mem to xmmreg | 0110 0110:0000 1111:0011 1000: 0011 0111: mod xmmreg r/m |
| POPCNT— Return Number of Bits Set to 1 | |
| reg2 to reg1 | 1111 0011:0000 1111:1011 1000:11 reg1 reg2 |
| mem to reg1 | 1111 0011:0000 1111:1011 1000:mod reg1 r/m |

Table B-35. Encodings of SSE4.2 instructions

| Instruction and Format | Encoding |
|------------------------|---|
| qwrreg2 to qwrreg1 | 1111 0011:0100 1ROB:0000 1111:1011 1000:11 reg1 reg2 |
| mem64 to qwrreg1 | 1111 0011:0100 1ROB:0000 1111:1011 1000:mod reg1 r/m |

B.15 FLOATING-POINT INSTRUCTION FORMATS AND ENCODINGS

Table B-35 shows the five different formats used for floating-point instructions. In all cases, instructions are at least two bytes long and begin with the bit pattern 11011.

Table B-36. General Floating-Point Instruction Formats

| | Instruction | | | | | | | | | Optional Fields | | |
|---|-------------|-----|---|-------------|-----|---|-----|-----|-------|-----------------|-------|------|
| | First Byte | | | Second Byte | | | | | | | | |
| 1 | 11011 | OPA | | 1 | mod | | 1 | OPB | r/m | | s-i-b | disp |
| 2 | 11011 | MF | | OPA | mod | | OPB | | r/m | | s-i-b | disp |
| 3 | 11011 | d | P | OPA | 1 | 1 | OPB | R | ST(i) | | | |
| 4 | 11011 | 0 | 0 | 1 | 1 | 1 | 1 | OP | | | | |
| 5 | 11011 | 0 | 1 | 1 | 1 | 1 | 1 | OP | | | | |
| | 15–11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

MF = Memory Format

00 – 32-bit real

01 – 32-bit integer

10 – 64-bit real

11 – 16-bit integer

P = Pop

0 – Do not pop stack

1 – Pop stack after operation

d = Destination

0 – Destination is ST(0)

1 – Destination is ST(i)

R XOR d = 0 – Destination OP Source

R XOR d = 1 – Source OP Destination

ST(i) = Register stack element *i*

000 = Stack Top

001 = Second stack element

.

.

.

111 = Eighth stack element

The Mod and R/M fields of the ModR/M byte have the same interpretation as the corresponding fields of the integer instructions. The SIB byte and disp (displacement) are optionally present in instructions that have Mod and R/M fields. Their presence depends on the values of Mod and R/M, as for integer instructions.

Table B-36 shows the formats and encodings of the floating-point instructions.

Table B-37. Floating-Point Instruction Formats and Encodings

| Instruction and Format | Encoding |
|--|--------------------------|
| F2XM1 - Compute $2^{\text{ST}(0)} - 1$ | 11011 001 : 1111 0000 |
| FABS - Absolute Value | 11011 001 : 1110 0001 |
| FADD - Add | |
| ST(0) \leftarrow ST(0) + 32-bit memory | 11011 000 : mod 000 r/m |
| ST(0) \leftarrow ST(0) + 64-bit memory | 11011 100 : mod 000 r/m |
| ST(d) \leftarrow ST(0) + ST(i) | 11011 d00 : 11 000 ST(i) |
| FADDP - Add and Pop | |
| ST(0) \leftarrow ST(0) + ST(i) | 11011 110 : 11 000 ST(i) |
| FBLD - Load Binary Coded Decimal | 11011 111 : mod 100 r/m |
| FBSTP - Store Binary Coded Decimal and Pop | 11011 111 : mod 110 r/m |
| FCFS - Change Sign | 11011 001 : 1110 0000 |
| FCLEX - Clear Exceptions | 11011 011 : 1110 0010 |
| FCOM - Compare Real | |
| 32-bit memory | 11011 000 : mod 010 r/m |
| 64-bit memory | 11011 100 : mod 010 r/m |
| ST(i) | 11011 000 : 11 010 ST(i) |
| FCOMP - Compare Real and Pop | |
| 32-bit memory | 11011 000 : mod 011 r/m |
| 64-bit memory | 11011 100 : mod 011 r/m |
| ST(i) | 11011 000 : 11 011 ST(i) |
| FCOMPP - Compare Real and Pop Twice | 11011 110 : 11 011 001 |
| FCOMIP - Compare Real, Set EFLAGS, and Pop | 11011 111 : 11 110 ST(i) |
| FCOS - Cosine of ST(0) | 11011 001 : 1111 1111 |
| FDECSTP - Decrement Stack-Top Pointer | 11011 001 : 1111 0110 |
| FDIV - Divide | |
| ST(0) \leftarrow ST(0) \div 32-bit memory | 11011 000 : mod 110 r/m |
| ST(0) \leftarrow ST(0) \div 64-bit memory | 11011 100 : mod 110 r/m |
| ST(d) \leftarrow ST(0) \div ST(i) | 11011 d00 : 1111 R ST(i) |

Table B-37. Floating-Point Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|--|--------------------------|
| FDIVP - Divide and Pop | |
| $ST(0) \leftarrow ST(0) \div ST(i)$ | 11011 110 : 1111 1 ST(i) |
| FDIVR - Reverse Divide | |
| $ST(0) \leftarrow 32\text{-bit memory} \div ST(0)$ | 11011 000 : mod 111 r/m |
| $ST(0) \leftarrow 64\text{-bit memory} \div ST(0)$ | 11011 100 : mod 111 r/m |
| $ST(d) \leftarrow ST(i) \div ST(0)$ | 11011 d00 : 1111 R ST(i) |
| FDIVRP - Reverse Divide and Pop | |
| $ST(0) \leftarrow ST(i) \div ST(0)$ | 11011 110 : 1111 0 ST(i) |
| FFREE - Free ST(i) Register | 11011 101 : 1100 0 ST(i) |
| FIADD - Add Integer | |
| $ST(0) \leftarrow ST(0) + 16\text{-bit memory}$ | 11011 110 : mod 000 r/m |
| $ST(0) \leftarrow ST(0) + 32\text{-bit memory}$ | 11011 010 : mod 000 r/m |
| FICOM - Compare Integer | |
| 16-bit memory | 11011 110 : mod 010 r/m |
| 32-bit memory | 11011 010 : mod 010 r/m |
| FICOMP - Compare Integer and Pop | |
| 16-bit memory | 11011 110 : mod 011 r/m |
| 32-bit memory | 11011 010 : mod 011 r/m |
| FIDIV | |
| $ST(0) \leftarrow ST(0) \div 16\text{-bit memory}$ | 11011 110 : mod 110 r/m |
| $ST(0) \leftarrow ST(0) \div 32\text{-bit memory}$ | 11011 010 : mod 110 r/m |
| FIDIVR | |
| $ST(0) \leftarrow 16\text{-bit memory} \div ST(0)$ | 11011 110 : mod 111 r/m |
| $ST(0) \leftarrow 32\text{-bit memory} \div ST(0)$ | 11011 010 : mod 111 r/m |
| FILD - Load Integer | |
| 16-bit memory | 11011 111 : mod 000 r/m |
| 32-bit memory | 11011 011 : mod 000 r/m |
| 64-bit memory | 11011 111 : mod 101 r/m |
| FIMUL | |
| $ST(0) \leftarrow ST(0) \times 16\text{-bit memory}$ | 11011 110 : mod 001 r/m |

Table B-37. Floating-Point Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|--|----------------------------|
| $ST(0) \leftarrow ST(0) \times$ 32-bit memory | 11011 010 : mod 001 r/m |
| FINCSTP - Increment Stack Pointer | 11011 001 : 1111 0111 |
| FINIT - Initialize Floating-Point Unit | |
| FIST - Store Integer | |
| 16-bit memory | 11011 111 : mod 010 r/m |
| 32-bit memory | 11011 011 : mod 010 r/m |
| FISTP - Store Integer and Pop | |
| 16-bit memory | 11011 111 : mod 011 r/m |
| 32-bit memory | 11011 011 : mod 011 r/m |
| 64-bit memory | 11011 111 : mod 111 r/m |
| FISUB | |
| $ST(0) \leftarrow ST(0) -$ 16-bit memory | 11011 110 : mod 100 r/m |
| $ST(0) \leftarrow ST(0) -$ 32-bit memory | 11011 010 : mod 100 r/m |
| FISUBR | |
| $ST(0) \leftarrow$ 16-bit memory – $ST(0)$ | 11011 110 : mod 101 r/m |
| $ST(0) \leftarrow$ 32-bit memory – $ST(0)$ | 11011 010 : mod 101 r/m |
| FLD - Load Real | |
| 32-bit memory | 11011 001 : mod 000 r/m |
| 64-bit memory | 11011 101 : mod 000 r/m |
| 80-bit memory | 11011 011 : mod 101 r/m |
| $ST(i)$ | 11011 001 : 11 000 $ST(i)$ |
| FLD1 - Load +1.0 into $ST(0)$ | 11011 001 : 1110 1000 |
| FLDCW - Load Control Word | 11011 001 : mod 101 r/m |
| FLDENV - Load FPU Environment | 11011 001 : mod 100 r/m |
| FLDL2E - Load $\log_2(\epsilon)$ into $ST(0)$ | 11011 001 : 1110 1010 |
| FLDL2T - Load $\log_2(10)$ into $ST(0)$ | 11011 001 : 1110 1001 |
| FLDLG2 - Load $\log_{10}(2)$ into $ST(0)$ | 11011 001 : 1110 1100 |
| FLDLN2 - Load $\log_e(2)$ into $ST(0)$ | 11011 001 : 1110 1101 |
| FLDPI - Load π into $ST(0)$ | 11011 001 : 1110 1011 |
| FLDZ - Load +0.0 into $ST(0)$ | 11011 001 : 1110 1110 |
| FMUL - Multiply | |

Table B-37. Floating-Point Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|--|--------------------------|
| $ST(0) \leftarrow ST(0) \times 32\text{-bit memory}$ | 11011 000 : mod 001 r/m |
| $ST(0) \leftarrow ST(0) \times 64\text{-bit memory}$ | 11011 100 : mod 001 r/m |
| $ST(d) \leftarrow ST(0) \times ST(i)$ | 11011 d00 : 1100 1 ST(i) |
| FMULP - Multiply | |
| $ST(i) \leftarrow ST(0) \times ST(i)$ | 11011 110 : 1100 1 ST(i) |
| FNOP - No Operation | 11011 001 : 1101 0000 |
| FPATAN - Partial Arctangent | 11011 001 : 1111 0011 |
| FPREM - Partial Remainder | 11011 001 : 1111 1000 |
| FPREM1 - Partial Remainder (IEEE) | 11011 001 : 1111 0101 |
| FPTAN - Partial Tangent | 11011 001 : 1111 0010 |
| FRNDINT - Round to Integer | 11011 001 : 1111 1100 |
| FRSTOR - Restore FPU State | 11011 101 : mod 100 r/m |
| FSAVE - Store FPU State | 11011 101 : mod 110 r/m |
| FSCALE - Scale | 11011 001 : 1111 1101 |
| FSIN - Sine | 11011 001 : 1111 1110 |
| FSINCOS - Sine and Cosine | 11011 001 : 1111 1011 |
| FSQRT - Square Root | 11011 001 : 1111 1010 |
| FST - Store Real | |
| 32-bit memory | 11011 001 : mod 010 r/m |
| 64-bit memory | 11011 101 : mod 010 r/m |
| ST(i) | 11011 101 : 11 010 ST(i) |
| FSTCW - Store Control Word | 11011 001 : mod 111 r/m |
| FSTENV - Store FPU Environment | 11011 001 : mod 110 r/m |
| FSTP - Store Real and Pop | |
| 32-bit memory | 11011 001 : mod 011 r/m |
| 64-bit memory | 11011 101 : mod 011 r/m |
| 80-bit memory | 11011 011 : mod 111 r/m |
| ST(i) | 11011 101 : 11 011 ST(i) |
| FSTSW - Store Status Word into AX | 11011 111 : 1110 0000 |
| FSTSW - Store Status Word into Memory | 11011 101 : mod 111 r/m |
| FSUB - Subtract | |

Table B-37. Floating-Point Instruction Formats and Encodings (Contd.)

| Instruction and Format | Encoding |
|---|--------------------------|
| ST(0) ← ST(0) - 32-bit memory | 11011 000 : mod 100 r/m |
| ST(0) ← ST(0) - 64-bit memory | 11011 100 : mod 100 r/m |
| ST(d) ← ST(0) - ST(i) | 11011 d00 : 1110 R ST(i) |
| FSUBP - Subtract and Pop | |
| ST(0) ← ST(0) - ST(i) | 11011 110 : 1110 1 ST(i) |
| FSUBR - Reverse Subtract | |
| ST(0) ← 32-bit memory - ST(0) | 11011 000 : mod 101 r/m |
| ST(0) ← 64-bit memory - ST(0) | 11011 100 : mod 101 r/m |
| ST(d) ← ST(i) - ST(0) | 11011 d00 : 1110 R ST(i) |
| FSUBRP - Reverse Subtract and Pop | |
| ST(i) ← ST(i) - ST(0) | 11011 110 : 1110 0 ST(i) |
| FTST - Test | 11011 001 : 1110 0100 |
| FUCOM - Unordered Compare Real | 11011 101 : 1110 0 ST(i) |
| FUCOMP - Unordered Compare Real and Pop | 11011 101 : 1110 1 ST(i) |
| FUCOMPP - Unordered Compare Real and Pop Twice | 11011 010 : 1110 1001 |
| FUCOMI - Unorderd Compare Real and Set EFLAGS | 11011 011 : 11 101 ST(i) |
| FUCOMIP - Unorderd Compare Real, Set EFLAGS, and Pop | 11011 111 : 11 101 ST(i) |
| FXAM - Examine | 11011 001 : 1110 0101 |
| FXCH - Exchange ST(0) and ST(i) | 11011 001 : 1100 1 ST(i) |
| FXTRACT - Extract Exponent and Significand | 11011 001 : 1111 0100 |
| FYL2X - ST(1) × log₂(ST(0)) | 11011 001 : 1111 0001 |
| FYL2XP1 - ST(1) × log₂(ST(0) + 1.0) | 11011 001 : 1111 1001 |
| FWAIT - Wait until FPU Ready | 1001 1011 |

B.16 VMX INSTRUCTIONS

Table B-37 describes virtual-machine extensions (VMX).

Table B-38. Encodings for VMX Instructions

| Instruction and Format | Encoding |
|---|---|
| INVEPT—Invalidate Cached EPT Mappings | |
| Descriptor m128 according to reg | 01100110 00001111 00111000 10000000: mod reg r/m |
| INVVPID—Invalidate Cached VPID Mappings | |
| Descriptor m128 according to reg | 01100110 00001111 00111000 10000001: mod reg r/m |
| VMCALL—Call to VM Monitor | |
| Call VMM: causes VM exit. | 00001111 00000001 11000001 |
| VMCLEAR—Clear Virtual-Machine Control Structure | |
| mem32:VMCS_data_ptr | 01100110 00001111 11000111: mod 110 r/m |
| mem64:VMCS_data_ptr | 01100110 00001111 11000111: mod 110 r/m |
| VMLAUNCH—Launch Virtual Machine | |
| Launch VM managed by Current_VMCS | 00001111 00000001 11000010 |
| VMRESUME—Resume Virtual Machine | |
| Resume VM managed by Current_VMCS | 00001111 00000001 11000011 |
| VMPTRLD—Load Pointer to Virtual-Machine Control Structure | |
| mem32 to Current_VMCS_ptr | 00001111 11000111: mod 110 r/m |
| mem64 to Current_VMCS_ptr | 00001111 11000111: mod 110 r/m |
| VMPTRST—Store Pointer to Virtual-Machine Control Structure | |
| Current_VMCS_ptr to mem32 | 00001111 11000111: mod 111 r/m |
| Current_VMCS_ptr to mem64 | 00001111 11000111: mod 111 r/m |
| VMREAD—Read Field from Virtual-Machine Control Structure | |
| r32 (VMCS_fieldn) to r32 | 00001111 01111000: 11 reg2 reg1 |
| r32 (VMCS_fieldn) to mem32 | 00001111 01111000: mod r32 r/m |
| r64 (VMCS_fieldn) to r64 | 00001111 01111000: 11 reg2 reg1 |
| r64 (VMCS_fieldn) to mem64 | 00001111 01111000: mod r64 r/m |

Table B-38. Encodings for VMX Instructions

| Instruction and Format | Encoding |
|--|--|
| VMWRITE—Write Field to Virtual-Machine Control Structure | |
| r32 to r32 (<i>VMCS_fieldn</i>) mem32 to r32 (<i>VMCS_fieldn</i>) r64 to r64 (<i>VMCS_fieldn</i>) mem64 to r64 (<i>VMCS_fieldn</i>) | 00001111 01111001: 11 reg1 reg2 00001111 01111001: mod r32 r/m 00001111 01111001: 11 reg1 reg2 00001111 01111001: mod r64 r/m |
| VMXOFF—Leave VMX Operation | |
| Leave VMX. | 00001111 00000001 11000100 |
| VMXON—Enter VMX Operation | |
| Enter VMX. | 11110011 00001111 11000111: mod 110 r/m |

B.17 SMX INSTRUCTIONS

Table B-38 describes Safer Mode extensions (VMX). **GETSEC leaf functions are selected by a valid value in EAX on input.**

Table B-39. Encodings for SMX Instructions

| Instruction and Format | Encoding |
|---|----------------------------|
| GETSEC—GETSEC leaf functions are selected by the value in EAX on input | |
| <i>GETSEC[CAPABILITIES].</i> | 00001111 00110111 (EAX= 0) |
| <i>GETSEC[ENTERACCS].</i> | 00001111 00110111 (EAX= 2) |
| <i>GETSEC[EXITAC].</i> | 00001111 00110111 (EAX= 3) |
| <i>GETSEC[SENER].</i> | 00001111 00110111 (EAX= 4) |
| <i>GETSEC[SEXIT].</i> | 00001111 00110111 (EAX= 5) |
| <i>GETSEC[PARAMETERS].</i> | 00001111 00110111 (EAX= 6) |
| <i>GETSEC[SMCTRL].</i> | 00001111 00110111 (EAX= 7) |
| <i>GETSEC[WAKEUP].</i> | 00001111 00110111 (EAX= 8) |

APPENDIX C

INTEL® C/C++ COMPILER INTRINSICS AND FUNCTIONAL EQUIVALENTS

The two tables in this appendix itemize the Intel C/C++ compiler intrinsics and functional equivalents for the Intel MMX technology, SSE, SSE2, SSE3, and SSSE3 instructions.

There may be additional intrinsics that do not have an instruction equivalent. It is strongly recommended that the reader reference the compiler documentation for the complete list of supported intrinsics. Please refer to <http://www.intel.com/support/performancetools/>.

Table C-1 presents simple intrinsics and Table C-2 presents composite intrinsics. Some intrinsics are “composites” because they require more than one instruction to implement them.

Intel C/C++ Compiler intrinsic names reflect the following naming conventions:

`_mm_<intrin_op>_<suffix>`

where:

| | |
|--------------------------------|---|
| <code><intrin_op></code> | Indicates the intrinsics basic operation; for example, add for addition and sub for subtraction |
| <code><suffix></code> | Denotes the type of data operated on by the instruction. The first one or two letters of each suffix denotes whether the data is packed (p), extended packed (ep), or scalar (s). |

The remaining letters denote the type:

| | |
|------|---------------------------------|
| s | single-precision floating point |
| d | double-precision floating point |
| i128 | signed 128-bit integer |
| i64 | signed 64-bit integer |
| u64 | unsigned 64-bit integer |
| i32 | signed 32-bit integer |
| u32 | unsigned 32-bit integer |
| i16 | signed 16-bit integer |
| u16 | unsigned 16-bit integer |
| i8 | signed 8-bit integer |
| u8 | unsigned 8-bit integer |

The variable `r` is generally used for the intrinsic's return value. A number appended to a variable name indicates the element of a packed object. For example, `r0` is the lowest word of `r`.

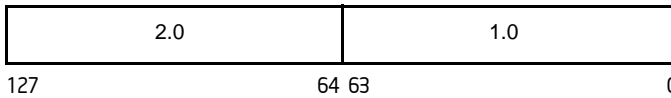
The packed values are represented in right-to-left order, with the lowest value being used for scalar operations. Consider the following example operation:

```
double a[2] = {1.0, 2.0};
__m128d t = _mm_load_pd(a);
```

The result is the same as either of the following:

```
__m128d t = _mm_set_pd(2.0, 1.0);
__m128d t = _mm_setr_pd(1.0, 2.0);
```

In other words, the XMM register that holds the value t will look as follows:



The “scalar” element is 1.0. Due to the nature of the instruction, some intrinsics require their arguments to be immediates (constant integer literals).

To use an intrinsic in your code, insert a line with the following syntax:

```
data_type intrinsic_name (parameters)
```

Where:

- data_type
Is the return data type, which can be either void, int, __m64, __m128, __m128d, or __m128i. Only the __mm_empty intrinsic returns void.
- intrinsic_name
Is the name of the intrinsic, which behaves like a function that you can use in your C/C++ code instead of in-lining the actual instruction.
- parameters
Represents the parameters required by each intrinsic.

C.1 SIMPLE INTRINSICS

NOTE

For detailed descriptions of the intrinsics in Table C-1, see the corresponding mnemonic in Chapter 3 in the “Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2A”, or Chapter 4, “Instruction Set Reference, N-Z” in the “Intel® 64 and IA-32 Architectures Software Developer’s Manual, Volume 2B”.

Table C-1. Simple Intrinsics

| Mnemonic | Intrinsic |
|----------|---|
| ADDPD | <code>__m128d _mm_add_pd(__m128d a, __m128d b)</code> |
| ADDPS | <code>__m128 _mm_add_ps(__m128 a, __m128 b)</code> |
| ADDSD | <code>__m128d _mm_add_sd(__m128d a, __m128d b)</code> |
| ADDSS | <code>__m128 _mm_add_ss(__m128 a, __m128 b)</code> |
| ADDSUBPD | <code>__m128d _mm_addsub_pd(__m128d a, __m128d b)</code> |
| ADDSUBPS | <code>__m128 _mm_addsub_ps(__m128 a, __m128 b)</code> |
| ANDNPD | <code>__m128d _mm_andnot_pd(__m128d a, __m128d b)</code> |
| ANDNPS | <code>__m128 _mm_andnot_ps(__m128 a, __m128 b)</code> |
| ANDPD | <code>__m128d _mm_and_pd(__m128d a, __m128d b)</code> |
| ANDPS | <code>__m128 _mm_and_ps(__m128 a, __m128 b)</code> |
| BLENDDPD | <code>__m128d _mm_blend_pd(__m128d v1, __m128d v2, const int mask)</code> |
| BLENDPS | <code>__m128 _mm_blend_ps(__m128 v1, __m128 v2, const int mask)</code> |
| BLENDVPD | <code>__m128d _mm_blendv_pd(__m128d v1, __m128d v2, __m128d v3)</code> |
| BLENDVPS | <code>__m128 _mm_blendv_ps(__m128 v1, __m128 v2, __m128 v3)</code> |
| CLFLUSH | <code>void _mm_clflush(void const *p)</code> |
| CMPPD | <code>__m128d _mm_cmpeq_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmplt_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmple_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpgt_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpge_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpneq_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpnlt_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpngt_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpnge_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpord_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpunord_pd(__m128d a, __m128d b)</code> |
| | <code>__m128d _mm_cmpnle_pd(__m128d a, __m128d b)</code> |
| CMPPS | <code>__m128 _mm_cmpeq_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmplt_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmple_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmpgt_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmpge_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmpneq_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmpnlt_ps(__m128 a, __m128 b)</code> |
| | <code>__m128 _mm_cmpngt_ps(__m128 a, __m128 b)</code> |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|--|
| | __m128_mm_cmpnge_ps(__m128 a, __m128 b) |
| | __m128_mm_cmpord_ps(__m128 a, __m128 b) |
| | __m128_mm_cmpunord_ps(__m128 a, __m128 b) |
| | __m128_mm_cmpnle_ps(__m128 a, __m128 b) |
| CMPSD | __m128d_mm_cmpeq_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmplt_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmple_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpgt_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpge_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpneq_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpnlt_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpnle_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpngt_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpnge_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpord_sd(__m128d a, __m128d b) |
| | __m128d_mm_cmpunord_sd(__m128d a, __m128d b) |
| CMPSS | __m128_mm_cmpeq_ss(__m128 a, __m128 b) |
| | __m128_mm_cmplt_ss(__m128 a, __m128 b) |
| | __m128_mm_cmple_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpgt_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpge_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpneq_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpnlt_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpnle_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpngt_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpnge_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpord_ss(__m128 a, __m128 b) |
| | __m128_mm_cmpunord_ss(__m128 a, __m128 b) |
| COMISD | int_mm_comieq_sd(__m128d a, __m128d b) |
| | int_mm_comilt_sd(__m128d a, __m128d b) |
| | int_mm_comile_sd(__m128d a, __m128d b) |
| | int_mm_comigt_sd(__m128d a, __m128d b) |
| | int_mm_comige_sd(__m128d a, __m128d b) |
| | int_mm_comineq_sd(__m128d a, __m128d b) |
| COMISS | int_mm_comieq_ss(__m128 a, __m128 b) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------|--|
| | int __mm_comilt_ss(__m128 a, __m128 b) |
| | int __mm_comile_ss(__m128 a, __m128 b) |
| | int __mm_comigt_ss(__m128 a, __m128 b) |
| | int __mm_comige_ss(__m128 a, __m128 b) |
| | int __mm_comineq_ss(__m128 a, __m128 b) |
| CRC32 | unsigned int __mm_crc32_u8(unsigned int crc, unsigned char data) |
| | unsigned int __mm_crc32_u16(unsigned int crc, unsigned short data) |
| | unsigned int __mm_crc32_u32(unsigned int crc, unsigned int data) |
| | unsigned __int64 __mm_crc32_u64(unsigned __int64 crc, unsigned __int64 data) |
| CVTDQ2PD | __m128d __mm_cvtepi32_pd(__m128i a) |
| CVTDQ2PS | __m128 __mm_cvtepi32_ps(__m128i a) |
| CVTPD2DQ | __m128i __mm_cvtpd_epi32(__m128d a) |
| CVTPD2PI | __m64 __mm_cvtpd_pi32(__m128d a) |
| CVTPD2PS | __m128 __mm_cvtpd_ps(__m128d a) |
| CVTPI2PD | __m128d __mm_cvtpi32_pd(__m64 a) |
| CVTPI2PS | __m128 __mm_cvt_pi2ps(__m128 a, __m64 b) __m128 __mm_cvtpi32_ps(__m128 a, __m64 b) |
| CVTPS2DQ | __m128i __mm_cvtps_epi32(__m128 a) |
| CVTPS2PD | __m128d __mm_cvtps_pd(__m128 a) |
| CVTPS2PI | __m64 __mm_cvt_ps2pi(__m128 a) __m64 __mm_cvtps_pi32(__m128 a) |
| CVTSD2SI | int __mm_cvtsd_si32(__m128d a) |
| CVTSD2SS | __m128 __mm_cvtsd_ss(__m128 a, __m128d b) |
| CVTSI2SD | __m128d __mm_cvtsi32_sd(__m128d a, int b) |
| CVTSI2SS | __m128 __mm_cvt_si2ss(__m128 a, int b) __m128 __mm_cvtsi32_ss(__m128 a, int b) |
| CVTSS2SD | __m128d __mm_cvtsd_ss(__m128d a, __m128 b) |
| CVTSS2SI | int __mm_cvt_ss2si(__m128 a) int __mm_cvtss_si32(__m128 a) |
| CVTTPD2DQ | __m128i __mm_cvttpd_epi32(__m128d a) |
| CVTTPD2PI | __m64 __mm_cvttpd_pi32(__m128d a) |
| CVTTPS2DQ | __m128i __mm_cvttps_epi32(__m128 a) |
| CVTTPS2PI | __m64 __mm_cvt_t_ps2pi(__m128 a) __m64 __mm_cvttps_pi32(__m128 a) |
| CVTTSD2SI | int __mm_cvttss_si32(__m128d a) |
| CVTTSS2SI | int __mm_cvt_t_ss2si(__m128 a) int __mm_cvttss_si32(__m128 a) __m64 __mm_cvtsi32_si64(int i) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|------------|--|
| | |
| DIVPD | __m128d _mm_div_pd(__m128d a, __m128d b) |
| DIVPS | __m128 _mm_div_ps(__m128 a, __m128 b) |
| DIVSD | __m128d _mm_div_sd(__m128d a, __m128d b) |
| DIVSS | __m128 _mm_div_ss(__m128 a, __m128 b) |
| DPPD | __m128d _mm_dp_pd(__m128d a, __m128d b, const int mask) |
| DPPS | __m128 _mm_dp_ps(__m128 a, __m128 b, const int mask) |
| EMMS | void _mm_empty() |
| EXTRACTPS | int_mm_extract_ps(__m128 src, const int ndx) |
| HADDPD | __m128d _mm_hadd_pd(__m128d a, __m128d b) |
| HADDPS | __m128 _mm_hadd_ps(__m128 a, __m128 b) |
| HSUBPD | __m128d _mm_hsub_pd(__m128d a, __m128d b) |
| HSUBPS | __m128 _mm_hsub_ps(__m128 a, __m128 b) |
| INSERTPS | __m128 _mm_insert_ps(__m128 dst, __m128 src, const int ndx) |
| LDDQU | __m128i _mm_lddqu_si128(__m128i const *p) |
| LDMXCSR | __mm_setcsr(unsigned int i) |
| LFENCE | void _mm_lfence(void) |
| MASKMOVDQU | void _mm_maskmoveu_si128(__m128i d, __m128i n, char *p) |
| MASKMOVQ | void _mm_maskmove_si64(__m64 d, __m64 n, char *p) |
| MAXPD | __m128d _mm_max_pd(__m128d a, __m128d b) |
| MAXPS | __m128 _mm_max_ps(__m128 a, __m128 b) |
| MAXSD | __m128d _mm_max_sd(__m128d a, __m128d b) |
| MAXSS | __m128 _mm_max_ss(__m128 a, __m128 b) |
| MFENCE | void _mm_mfence(void) |
| MINPD | __m128d _mm_min_pd(__m128d a, __m128d b) |
| MINPS | __m128 _mm_min_ps(__m128 a, __m128 b) |
| MINSD | __m128d _mm_min_sd(__m128d a, __m128d b) |
| MINSS | __m128 _mm_min_ss(__m128 a, __m128 b) |
| MONITOR | void _mm_monitor(void const *p, unsigned extensions, unsigned hints) |
| MOVAPD | __m128d _mm_load_pd(double * p) |
| | void_mm_store_pd(double *p, __m128d a) |
| MOVAPS | __m128 _mm_load_ps(float * p) |
| | void_mm_store_ps(float *p, __m128 a) |
| MOVD | __m128i _mm_cvtsi32_si128(int a) |
| | int_mm_cvtsi128_si32(__m128i a) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|----------|--|
| | |
| | int __mm_cvtsi64_si32(__m64 a) |
| MOVDDUP | __m128d __mm_movedup_pd(__m128d a) |
| | __m128d __mm_loaddup_pd(double const * dp) |
| MOVDDQA | __m128i __mm_load_si128(__m128i * p) |
| | void __mm_store_si128(__m128i *p, __m128i a) |
| MOVDDQU | __m128i __mm_loadu_si128(__m128i * p) |
| | void __mm_storeu_si128(__m128i *p, __m128i a) |
| MOVDDQ2Q | __m64 __mm_movepi64_pi64(__m128i a) |
| MOVHLPS | __m128 __mm_movehl_ps(__m128 a, __m128 b) |
| MOVHPD | __m128d __mm_loadh_pd(__m128d a, double * p) |
| | void __mm_storeh_pd(double * p, __m128d a) |
| MOVHPS | __m128 __mm_loadh_pi(__m128 a, __m64 * p) |
| | void __mm_storeh_pi(__m64 * p, __m128 a) |
| MOVLPD | __m128d __mm_loadl_pd(__m128d a, double * p) |
| | void __mm_storel_pd(double * p, __m128d a) |
| MOVLPS | __m128 __mm_loadl_pi(__m128 a, __m64 * p) |
| | void __mm_storel_pi(__m64 * p, __m128 a) |
| MOVLHPS | __m128 __mm_movelh_ps(__m128 a, __m128 b) |
| MOVMSKPD | int __mm_movemask_pd(__m128d a) |
| MOVMSKPS | int __mm_movemask_ps(__m128 a) |
| MOVNTDQA | __m128i __mm_stream_load_si128(__m128i *p) |
| MOVNTDQ | void __mm_stream_si128(__m128i * p, __m128i a) |
| MOVNTPD | void __mm_stream_pd(double * p, __m128d a) |
| MOVNTPS | void __mm_stream_ps(float * p, __m128 a) |
| MOVNTI | void __mm_stream_si32(int * p, int a) |
| MOVNTQ | void __mm_stream_pi(__m64 * p, __m64 a) |
| MOVQ | __m128i __mm_loadl_epi64(__m128i * p) |
| | void __mm_storel_epi64(__m128i * p, __m128i a) |
| | __m128i __mm_move_epi64(__m128i a) |
| MOVQ2DQ | __m128i __mm_movpi64_epi64(__m64 a) |
| MOVSD | __m128d __mm_load_sd(double * p) |
| | void __mm_store_sd(double * p, __m128d a) |
| | __m128d __mm_move_sd(__m128d a, __m128d b) |
| MOVSHDUP | __m128 __mm_movehdup_ps(__m128 a) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|--|
| MOVSLDUP | __m128 _mm_moveldup_ps(__m128 a) |
| MOVSS | __m128 _mm_load_ss(float * p) |
| | void _mm_store_ss(float * p, __m128 a) |
| | __m128 _mm_move_ss(__m128 a, __m128 b) |
| MOVUPD | __m128d _mm_loadu_pd(double * p) |
| | void _mm_storeu_pd(double *p, __m128d a) |
| MOVUPS | __m128 _mm_loadu_ps(float * p) |
| | void _mm_storeu_ps(float *p, __m128 a) |
| MPSADBW | __m128i _mm_mpsadbw_epu8(__m128i s1, __m128i s2, const int mask) |
| MULPD | __m128d _mm_mul_pd(__m128d a, __m128d b) |
| MULPS | __m128 _mm_mul_ss(__m128 a, __m128 b) |
| MULSD | __m128d _mm_mul_sd(__m128d a, __m128d b) |
| MULSS | __m128 _mm_mul_ss(__m128 a, __m128 b) |
| MWAIT | void _mm_mwait(unsigned extensions, unsigned hints) |
| ORPD | __m128d _mm_or_pd(__m128d a, __m128d b) |
| ORPS | __m128 _mm_or_ps(__m128 a, __m128 b) |
| PABSB | __m64 _mm_abs_pi8 (__m64 a) |
| | __m128i _mm_abs_epi8 (__m128i a) |
| PABSD | __m64 _mm_abs_pi32 (__m64 a) |
| | __m128i _mm_abs_epi32 (__m128i a) |
| PABSW | __m64 _mm_abs_pi16 (__m64 a) |
| | __m128i _mm_abs_epi16 (__m128i a) |
| PACKSSWB | __m128i _mm_packs_epi16(__m128i m1, __m128i m2) |
| PACKSSWB | __m64 _mm_packs_pi16(__m64 m1, __m64 m2) |
| PACKSSDW | __m128i _mm_packs_epi32 (__m128i m1, __m128i m2) |
| PACKSSDW | __m64 _mm_packs_pi32 (__m64 m1, __m64 m2) |
| PACKUSDW | __m128i _mm_packus_epi32(__m128i m1, __m128i m2) |
| PACKUSWB | __m128i _mm_packus_epi16(__m128i m1, __m128i m2) |
| PACKUSWB | __m64 _mm_packs_pu16(__m64 m1, __m64 m2) |
| PADDB | __m128i _mm_add_epi8(__m128i m1, __m128i m2) |
| PADDB | __m64 _mm_add_pi8(__m64 m1, __m64 m2) |
| PADDW | __m128i _mm_add_epi16(__m128i m1, __m128i m2) |
| PADDW | __m64 _mm_add_pi16(__m64 m1, __m64 m2) |
| PADDD | __m128i _mm_add_epi32(__m128i m1, __m128i m2) |
| PADDD | __m64 _mm_add_pi32(__m64 m1, __m64 m2) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------|--|
| PADDQ | <code>__m128i _mm_add_epi64(__m128i m1, __m128i m2)</code> |
| PADDQ | <code>__m64 _mm_add_si64(__m64 m1, __m64 m2)</code> |
| PADDSB | <code>__m128i _mm_adds_epi8(__m128i m1, __m128i m2)</code> |
| PADDSB | <code>__m64 _mm_adds_pi8(__m64 m1, __m64 m2)</code> |
| PADDSW | <code>__m128i _mm_adds_epi16(__m128i m1, __m128i m2)</code> |
| PADDSW | <code>__m64 _mm_adds_pi16(__m64 m1, __m64 m2)</code> |
| PADDUSB | <code>__m128i _mm_adds_epu8(__m128i m1, __m128i m2)</code> |
| PADDUSB | <code>__m64 _mm_adds_pu8(__m64 m1, __m64 m2)</code> |
| PADDUSW | <code>__m128i _mm_adds_epu16(__m128i m1, __m128i m2)</code> |
| PADDUSW | <code>__m64 _mm_adds_pu16(__m64 m1, __m64 m2)</code> |
| PALIGNR | <code>__m64 _mm_alignr_pi8 (__m64 a, __m64 b, int n)</code> |
| | <code>__m128i _mm_alignr_epi8 (__m128i a, __m128i b, int n)</code> |
| PAND | <code>__m128i _mm_and_si128(__m128i m1, __m128i m2)</code> |
| PAND | <code>__m64 _mm_and_si64(__m64 m1, __m64 m2)</code> |
| PANDN | <code>__m128i _mm_andnot_si128(__m128i m1, __m128i m2)</code> |
| PANDN | <code>__m64 _mm_andnot_si64(__m64 m1, __m64 m2)</code> |
| PAUSE | <code>void _mm_pause(void)</code> |
| PAVGB | <code>__m128i _mm_avg_epu8(__m128i a, __m128i b)</code> |
| PAVGB | <code>__m64 _mm_avg_pu8(__m64 a, __m64 b)</code> |
| PAVGW | <code>__m128i _mm_avg_epu16(__m128i a, __m128i b)</code> |
| PAVGW | <code>__m64 _mm_avg_pu16(__m64 a, __m64 b)</code> |
| PBLENDVB | <code>__m128i _mm_blendv_epi (__m128i v1, __m128i v2, __m128i mask)</code> |
| PBLENDW | <code>__m128i _mm_blend_epi16(__m128i v1, __m128i v2, const int mask)</code> |
| PCMPEQB | <code>__m128i _mm_cmpeq_epi8(__m128i m1, __m128i m2)</code> |
| PCMPEQB | <code>__m64 _mm_cmpeq_pi8(__m64 m1, __m64 m2)</code> |
| PCMPEQQ | <code>__m128i _mm_cmpeq_epi64(__m128i a, __m128i b)</code> |
| PCMPEQW | <code>__m128i _mm_cmpeq_epi16 (__m128i m1, __m128i m2)</code> |
| PCMPEQW | <code>__m64 _mm_cmpeq_pi16 (__m64 m1, __m64 m2)</code> |
| PCMPEQD | <code>__m128i _mm_cmpeq_epi32(__m128i m1, __m128i m2)</code> |
| PCMPEQD | <code>__m64 _mm_cmpeq_pi32(__m64 m1, __m64 m2)</code> |
| PCMPESTRI | <code>int _mm_cmpestri (__m128i a, int la, __m128i b, int lb, const int mode)</code> |
| | <code>int _mm_cmpestra (__m128i a, int la, __m128i b, int lb, const int mode)</code> |
| | <code>int _mm_cmpestrc (__m128i a, int la, __m128i b, int lb, const int mode)</code> |
| | <code>int _mm_cmpestro (__m128i a, int la, __m128i b, int lb, const int mode)</code> |
| | <code>int _mm_cmpestrs (__m128i a, int la, __m128i b, int lb, const int mode)</code> |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|--|
| | int_mm_cmpestrz (__m128i a, int la, __m128i b, int lb, const int mode) |
| PCMPSTRM | __m128i_mm_cmpestrm (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestra (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestrc (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestro (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestrs (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestrz (__m128i a, int la, __m128i b, int lb, const int mode) |
| PCMPGTB | __m128i_mm_cmpgt_epi8 (__m128i m1, __m128i m2) |
| PCMPGTB | __m64_mm_cmpgt_pi8 (__m64 m1, __m64 m2) |
| PCMPGTW | __m128i_mm_cmpgt_epi16 (__m128i m1, __m128i m2) |
| PCMPGTW | __m64_mm_cmpgt_pi16 (__m64 m1, __m64 m2) |
| PCMPGTD | __m128i_mm_cmpgt_epi32 (__m128i m1, __m128i m2) |
| PCMPGTD | __m64_mm_cmpgt_pi32 (__m64 m1, __m64 m2) |
| PCMPISTRI | __m128i_mm_cmpestrm (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestra (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestrc (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestro (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpestrs (__m128i a, int la, __m128i b, int lb, const int mode) |
| | int_mm_cmpistrz (__m128i a, __m128i b, const int mode) |
| PCMPISTRM | __m128i_mm_cmpistrm (__m128i a, __m128i b, const int mode) |
| | int_mm_cmpistra (__m128i a, __m128i b, const int mode) |
| | int_mm_cmpistrc (__m128i a, __m128i b, const int mode) |
| | int_mm_cmpistro (__m128i a, __m128i b, const int mode) |
| | int_mm_cmpistrs (__m128i a, __m128i b, const int mode) |
| | int_mm_cmpistrz (__m128i a, __m128i b, const int mode) |
| PCMPGTQ | __m128i_mm_cmpgt_epi64 (__m128i a, __m128i b) |
| PEXTRB | int_mm_extract_epi8 (__m128i src, const int ndx) |
| PEXTRD | int_mm_extract_epi32 (__m128i src, const int ndx) |
| PEXTRQ | __int64_mm_extract_epi64 (__m128i src, const int ndx) |
| PEXTRW | int_mm_extract_epi16 (__m128i a, int n) |
| PEXTRW | int_mm_extract_pi16 (__m64 a, int n) |
| | int_mm_extract_epi16 (__m128i src, int ndx) |
| PHADDD | __m64_mm_hadd_pi32 (__m64 a, __m64 b) |
| | __m128i_mm_hadd_epi32 (__m128i a, __m128i b) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|---|
| PHADDSW | <code>__m64 __mm_hadds_pi16 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_hadds_epi16 (__m128i a, __m128i b)</code> |
| PHADDW | <code>__m64 __mm_hadd_pi16 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_hadd_epi16 (__m128i a, __m128i b)</code> |
| PHMINPOSUW | <code>__m128i __mm_minpos_epu16 (__m128i packed_words)</code> |
| PHSUBD | <code>__m64 __mm_hsub_pi32 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_hsub_epi32 (__m128i a, __m128i b)</code> |
| PHSUBSW | <code>__m64 __mm_hsubs_pi16 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_hsubs_epi16 (__m128i a, __m128i b)</code> |
| PHSUBW | <code>__m64 __mm_hsub_pi16 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_hsub_epi16 (__m128i a, __m128i b)</code> |
| PINSRB | <code>__m128i __mm_insert_epi8 (__m128i s1, int s2, const int ndx)</code> |
| PINSRD | <code>__m128i __mm_insert_epi32 (__m128i s2, int s, const int ndx)</code> |
| PINSRQ | <code>__m128i __mm_insert_epi64 (__m128i s2, __int64 s, const int ndx)</code> |
| PINSRW | <code>__m128i __mm_insert_epi16 (__m128i a, int d, int n)</code> |
| PINSRW | <code>__m64 __mm_insert_pi16 (__m64 a, int d, int n)</code> |
| PMADDUBSW | <code>__m64 __mm_maddubs_pi16 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_maddubs_epi16 (__m128i a, __m128i b)</code> |
| PMADDWD | <code>__m128i __mm_madd_epi16 (__m128i m1, __m128i m2)</code> |
| PMADDWD | <code>__m64 __mm_madd_pi16 (__m64 m1, __m64 m2)</code> |
| PMASB | <code>__m128i __mm_max_epi8 (__m128i a, __m128i b)</code> |
| PMASD | <code>__m128i __mm_max_epi32 (__m128i a, __m128i b)</code> |
| PMASW | <code>__m128i __mm_max_epi16 (__m128i a, __m128i b)</code> |
| PMASW | <code>__m64 __mm_max_pi16 (__m64 a, __m64 b)</code> |
| PMAXUB | <code>__m128i __mm_max_epu8 (__m128i a, __m128i b)</code> |
| PMAXUB | <code>__m64 __mm_max_pu8 (__m64 a, __m64 b)</code> |
| PMAXUD | <code>__m128i __mm_max_epu32 (__m128i a, __m128i b)</code> |
| PMAXUW | <code>__m128i __mm_max_epu16 (__m128i a, __m128i b)</code> |
| PMINSB | <code>__m128i __mm_min_epi8 (__m128i a, __m128i b)</code> |
| PMINSD | <code>__m128i __mm_min_epi32 (__m128i a, __m128i b)</code> |
| PMINSW | <code>__m128i __mm_min_epi16 (__m128i a, __m128i b)</code> |
| PMINSW | <code>__m64 __mm_min_pi16 (__m64 a, __m64 b)</code> |
| PMINUB | <code>__m128i __mm_min_epu8 (__m128i a, __m128i b)</code> |
| PMINUB | <code>__m64 __mm_min_pu8 (__m64 a, __m64 b)</code> |
| PMINUD | <code>__m128i __mm_min_epu32 (__m128i a, __m128i b)</code> |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|---|
| PMINUW | __m128i _mm_min_epu16(__m128i a, __m128i b) |
| PMOVMSKB | int _mm_movemask_epi8(__m128i a) |
| PMOVMSKB | int _mm_movemask_pi8(__m64 a) |
| PMOVXSBW | __m128i _mm_cvtepi8_epi16(__m128i a) |
| PMOVXSBQ | __m128i _mm_cvtepi8_epi32(__m128i a) |
| PMOVXSBQ | __m128i _mm_cvtepi8_epi64(__m128i a) |
| PMOVXSWD | __m128i _mm_cvtepi16_epi32(__m128i a) |
| PMOVXSWQ | __m128i _mm_cvtepi16_epi64(__m128i a) |
| PMOVXDQ | __m128i _mm_cvtepi32_epi64(__m128i a) |
| PMOVZXBW | __m128i _mm_cvtepu8_epi16(__m128i a) |
| PMOVZXBQ | __m128i _mm_cvtepu8_epi32(__m128i a) |
| PMOVZXBQ | __m128i _mm_cvtepu8_epi64(__m128i a) |
| PMOVZSWD | __m128i _mm_cvtepu16_epi32(__m128i a) |
| PMOVZSWQ | __m128i _mm_cvtepu16_epi64(__m128i a) |
| PMOVZXDQ | __m128i _mm_cvtepu32_epi64(__m128i a) |
| PMULDQ | __m128i _mm_mul_epi32(__m128i a, __m128i b) |
| PMULHRSW | __m64 _mm_mulhrs_pi16(__m64 a, __m64 b) |
| | __m128i _mm_mulhrs_epi16(__m128i a, __m128i b) |
| PMULHUW | __m128i _mm_mulhi_epu16(__m128i a, __m128i b) |
| PMULHUW | __m64 _mm_mulhi_pu16(__m64 a, __m64 b) |
| PMULHW | __m128i _mm_mulhi_epi16(__m128i m1, __m128i m2) |
| PMULHW | __m64 _mm_mulhi_pi16(__m64 m1, __m64 m2) |
| PMULLUD | __m128i _mm_mullo_epi32(__m128i a, __m128i b) |
| PMULLW | __m128i _mm_mullo_epi16(__m128i m1, __m128i m2) |
| PMULLW | __m64 _mm_mullo_pi16(__m64 m1, __m64 m2) |
| PMULUDQ | __m64 _mm_mul_su32(__m64 m1, __m64 m2) |
| | __m128i _mm_mul_epu32(__m128i m1, __m128i m2) |
| POPCNT | int _mm_popcnt_u32(unsigned int a) |
| | int64_t _mm_popcnt_u64(unsigned __int64 a) |
| POR | __m64 _mm_or_si64(__m64 m1, __m64 m2) |
| POR | __m128i _mm_or_si128(__m128i m1, __m128i m2) |
| PREFETCHh | void _mm_prefetch(char *a, int sel) |
| PSADBQ | __m128i _mm_sad_epu8(__m128i a, __m128i b) |
| PSADBQ | __m64 _mm_sad_pu8(__m64 a, __m64 b) |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|--|
| PSHUFB | <code>__m64 __mm_shuffle_pi8 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_shuffle_epi8 (__m128i a, __m128i b)</code> |
| PSHUFD | <code>__m128i __mm_shuffle_epi32(__m128i a, int n)</code> |
| PSHUFHW | <code>__m128i __mm_shufflehi_epi16(__m128i a, int n)</code> |
| PSHUFLW | <code>__m128i __mm_shufflelo_epi16(__m128i a, int n)</code> |
| PSHUFW | <code>__m64 __mm_shuffle_pi16(__m64 a, int n)</code> |
| PSIGNB | <code>__m64 __mm_sign_pi8 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_sign_epi8 (__m128i a, __m128i b)</code> |
| PSIGND | <code>__m64 __mm_sign_pi32 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_sign_epi32 (__m128i a, __m128i b)</code> |
| PSIGNW | <code>__m64 __mm_sign_pi16 (__m64 a, __m64 b)</code> |
| | <code>__m128i __mm_sign_epi16 (__m128i a, __m128i b)</code> |
| PSLLW | <code>__m128i __mm_sll_epi16(__m128i m, __m128i count)</code> |
| PSLLW | <code>__m128i __mm_slli_epi16(__m128i m, int count)</code> |
| PSLLW | <code>__m64 __mm_sll_pi16(__m64 m, __m64 count)</code> |
| | <code>__m64 __mm_slli_pi16(__m64 m, int count)</code> |
| PSLLD | <code>__m128i __mm_slli_epi32(__m128i m, int count)</code> |
| | <code>__m128i __mm_sll_epi32(__m128i m, __m128i count)</code> |
| PSLLD | <code>__m64 __mm_slli_pi32(__m64 m, int count)</code> |
| | <code>__m64 __mm_sll_pi32(__m64 m, __m64 count)</code> |
| PSLLQ | <code>__m64 __mm_sll_si64(__m64 m, __m64 count)</code> |
| | <code>__m64 __mm_slli_si64(__m64 m, int count)</code> |
| PSLLQ | <code>__m128i __mm_sll_epi64(__m128i m, __m128i count)</code> |
| | <code>__m128i __mm_slli_epi64(__m128i m, int count)</code> |
| PSLLDQ | <code>__m128i __mm_slli_si128(__m128i m, int imm)</code> |
| PSRAW | <code>__m128i __mm_sra_epi16(__m128i m, __m128i count)</code> |
| | <code>__m128i __mm_srai_epi16(__m128i m, int count)</code> |
| PSRAW | <code>__m64 __mm_sra_pi16(__m64 m, __m64 count)</code> |
| | <code>__m64 __mm_srai_pi16(__m64 m, int count)</code> |
| PSRAD | <code>__m128i __mm_sra_epi32 (__m128i m, __m128i count)</code> |
| | <code>__m128i __mm_srai_epi32 (__m128i m, int count)</code> |
| PSRAD | <code>__m64 __mm_sra_pi32 (__m64 m, __m64 count)</code> |
| | <code>__m64 __mm_srai_pi32 (__m64 m, int count)</code> |
| PSRLW | <code>__m128i __mm_srl_epi16 (__m128i m, __m128i count)</code> |
| | <code>__m128i __mm_slli_epi16 (__m128i m, int count)</code> |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------|--|
| | |
| | <code>__m64 __mm_srl_pi16(__m64 m, int count)</code> |
| PSRLD | <code>__m128i __mm_srl_epi32 (__m128i m, __m128i count)</code> |
| | <code>__m128i __mm_srl_epi32 (__m128i m, int count)</code> |
| PSRLD | <code>__m64 __mm_srl_pi32 (__m64 m, __m64 count)</code> |
| | <code>__m64 __mm_srl_pi32 (__m64 m, int count)</code> |
| PSRLQ | <code>__m128i __mm_srl_epi64 (__m128i m, __m128i count)</code> |
| | <code>__m128i __mm_srl_epi64 (__m128i m, int count)</code> |
| PSRLQ | <code>__m64 __mm_srl_si64 (__m64 m, __m64 count)</code> |
| | <code>__m64 __mm_srl_si64 (__m64 m, int count)</code> |
| PSRLDQ | <code>__m128i __mm_srl_si128(__m128i m, int imm)</code> |
| PSUBB | <code>__m128i __mm_sub_epi8(__m128i m1, __m128i m2)</code> |
| PSUBB | <code>__m64 __mm_sub_pi8(__m64 m1, __m64 m2)</code> |
| PSUBW | <code>__m128i __mm_sub_epi16(__m128i m1, __m128i m2)</code> |
| PSUBW | <code>__m64 __mm_sub_pi16(__m64 m1, __m64 m2)</code> |
| PSUBD | <code>__m128i __mm_sub_epi32(__m128i m1, __m128i m2)</code> |
| PSUBD | <code>__m64 __mm_sub_pi32(__m64 m1, __m64 m2)</code> |
| PSUBQ | <code>__m128i __mm_sub_epi64(__m128i m1, __m128i m2)</code> |
| PSUBQ | <code>__m64 __mm_sub_si64(__m64 m1, __m64 m2)</code> |
| PSUBSB | <code>__m128i __mm_subs_epi8(__m128i m1, __m128i m2)</code> |
| PSUBSB | <code>__m64 __mm_subs_pi8(__m64 m1, __m64 m2)</code> |
| PSUBSW | <code>__m128i __mm_subs_epi16(__m128i m1, __m128i m2)</code> |
| PSUBSW | <code>__m64 __mm_subs_pi16(__m64 m1, __m64 m2)</code> |
| PSUBUSB | <code>__m128i __mm_subs_epu8(__m128i m1, __m128i m2)</code> |
| PSUBUSB | <code>__m64 __mm_subs_pu8(__m64 m1, __m64 m2)</code> |
| PSUBUSW | <code>__m128i __mm_subs_epu16(__m128i m1, __m128i m2)</code> |
| PSUBUSW | <code>__m64 __mm_subs_pu16(__m64 m1, __m64 m2)</code> |
| PTEST | <code>int __mm_testz_si128(__m128i s1, __m128i s2)</code> |
| | <code>int __mm_testc_si128(__m128i s1, __m128i s2)</code> |
| | <code>int __mm_testnzc_si128(__m128i s1, __m128i s2)</code> |
| PUNPCKHBW | <code>__m64 __mm_unpackhi_pi8(__m64 m1, __m64 m2)</code> |
| PUNPCKHBW | <code>__m128i __mm_unpackhi_epi8(__m128i m1, __m128i m2)</code> |
| PUNPCKHWD | <code>__m64 __mm_unpackhi_pi16(__m64 m1, __m64 m2)</code> |
| PUNPCKHWD | <code>__m128i __mm_unpackhi_epi16(__m128i m1, __m128i m2)</code> |
| PUNPCKHDQ | <code>__m64 __mm_unpackhi_pi32(__m64 m1, __m64 m2)</code> |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|--|
| PUNPCKHDQ | <code>__m128i _mm_unpackhi_epi32(__m128i m1, __m128i m2)</code> |
| PUNPCKHQDQ | <code>__m128i _mm_unpackhi_epi64(__m128i m1, __m128i m2)</code> |
| PUNPCKLBW | <code>__m64 _mm_unpacklo_pi8 (__m64 m1, __m64 m2)</code> |
| PUNPCKLBW | <code>__m128i _mm_unpacklo_epi8 (__m128i m1, __m128i m2)</code> |
| PUNPCKLWD | <code>__m64 _mm_unpacklo_pi16(__m64 m1, __m64 m2)</code> |
| PUNPCKLWD | <code>__m128i _mm_unpacklo_epi16(__m128i m1, __m128i m2)</code> |
| PUNPCKLDQ | <code>__m64 _mm_unpacklo_pi32(__m64 m1, __m64 m2)</code> |
| PUNPCKLDQ | <code>__m128i _mm_unpacklo_epi32(__m128i m1, __m128i m2)</code> |
| PUNPCKLDQ | <code>__m128i _mm_unpacklo_epi64(__m128i m1, __m128i m2)</code> |
| PXOR | <code>__m64 _mm_xor_si64(__m64 m1, __m64 m2)</code> |
| PXOR | <code>__m128i _mm_xor_si128(__m128i m1, __m128i m2)</code> |
| RCPPS | <code>__m128 _mm_rcp_ps(__m128 a)</code> |
| RCPSS | <code>__m128 _mm_rcp_ss(__m128 a)</code> |
| ROUNDPD | <code>__m128 mm_round_pd(__m128d s1, int iRoundMode)</code> |
| | <code>__m128 mm_floor_pd(__m128d s1)</code> |
| | <code>__m128 mm_ceil_pd(__m128d s1)</code> |
| ROUNDPS | <code>__m128 mm_round_ps(__m128 s1, int iRoundMode)</code> |
| | <code>__m128 mm_floor_ps(__m128 s1)</code> |
| | <code>__m128 mm_ceil_ps(__m128 s1)</code> |
| ROUNDSD | <code>__m128d mm_round_sd(__m128d dst, __m128d s1, int iRoundMode)</code> |
| | <code>__m128d mm_floor_sd(__m128d dst, __m128d s1)</code> |
| | <code>__m128d mm_ceil_sd(__m128d dst, __m128d s1)</code> |
| ROUNDSS | <code>__m128 mm_round_ss(__m128 dst, __m128 s1, int iRoundMode)</code> |
| | <code>__m128 mm_floor_ss(__m128 dst, __m128 s1)</code> |
| | <code>__m128 mm_ceil_ss(__m128 dst, __m128 s1)</code> |
| RSQRTPS | <code>__m128 _mm_rsqrtps(__m128 a)</code> |
| RSQRTSS | <code>__m128 _mm_rsqrtss(__m128 a)</code> |
| SFENCE | <code>void mm_sfence(void)</code> |
| SHUFFPD | <code>__m128d _mm_shuffle_pd(__m128d a, __m128d b, unsigned int imm8)</code> |
| SHUFFPS | <code>__m128 _mm_shuffle_ps(__m128 a, __m128 b, unsigned int imm8)</code> |
| SQRTPD | <code>__m128d _mm_sqrtps(__m128d a)</code> |
| SQRTPS | <code>__m128 _mm_sqrtps(__m128 a)</code> |
| SQRTSD | <code>__m128d _mm_sqrt_sd(__m128d a)</code> |
| SQRTSS | <code>__m128 _mm_sqrt_ss(__m128 a)</code> |
| STMXCSR | <code>_mm_getcsr(void)</code> |

Table C-1. Simple Intrinsics (Contd.)

| Mnemonic | Intrinsic |
|-----------------|--|
| SUBPD | __m128d_mm_sub_pd(__m128d a, __m128d b) |
| SUBPS | __m128_mm_sub_ps(__m128 a, __m128 b) |
| SUBSD | __m128d_mm_sub_sd(__m128d a, __m128d b) |
| SUBSS | __m128_mm_sub_ss(__m128 a, __m128 b) |
| UCOMISD | int_mm_ucomieq_sd(__m128d a, __m128d b) |
| | int_mm_ucomilt_sd(__m128d a, __m128d b) |
| | int_mm_ucomile_sd(__m128d a, __m128d b) |
| | int_mm_ucomigt_sd(__m128d a, __m128d b) |
| | int_mm_ucomige_sd(__m128d a, __m128d b) |
| | int_mm_ucomineq_sd(__m128d a, __m128d b) |
| UCOMISS | int_mm_ucomieq_ss(__m128 a, __m128 b) |
| | int_mm_ucomilt_ss(__m128 a, __m128 b) |
| | int_mm_ucomile_ss(__m128 a, __m128 b) |
| | int_mm_ucomigt_ss(__m128 a, __m128 b) |
| | int_mm_ucomige_ss(__m128 a, __m128 b) |
| | int_mm_ucomineq_ss(__m128 a, __m128 b) |
| UNPCKHPD | __m128d_mm_unpackhi_pd(__m128d a, __m128d b) |
| UNPCKHPS | __m128_mm_unpackhi_ps(__m128 a, __m128 b) |
| UNPCKLPD | __m128d_mm_unpacklo_pd(__m128d a, __m128d b) |
| UNPCKLPS | __m128_mm_unpacklo_ps(__m128 a, __m128 b) |
| XORPD | __m128d_mm_xor_pd(__m128d a, __m128d b) |
| XORPS | __m128_mm_xor_ps(__m128 a, __m128 b) |

C.2 COMPOSITE INTRINSICS

Table C-2. Composite Intrinsics

| Mnemonic | Intrinsic |
|-----------------|---|
| (composite) | __m128i_mm_set_epi64(__m64 q1, __m64 q0) |
| (composite) | __m128i_mm_set_epi32(int i3, int i2, int i1, int i0) |
| (composite) | __m128i_mm_set_epi16(short w7, short w6, short w5, short w4, short w3, short w2, short w1, short w0) |
| (composite) | __m128i_mm_set_epi8(char w15, char w14, char w13, char w12, char w11, char w10, char w9, char w8, char w7, char w6, char w5, char w4, char w3, char w2, char w1, char w0) |
| (composite) | __m128i_mm_set1_epi64(__m64 q) |

Table C-2. Composite Intrinsic (Contd.)

| Mnemonic | Intrinsic |
|---------------------|--|
| (composite) | __m128i_mm_set1_epi32(int a) |
| (composite) | __m128i_mm_set1_epi16(short a) |
| (composite) | __m128i_mm_set1_epi8(char a) |
| (composite) | __m128i_mm_setr_epi64(__m64 q1, __m64 q0) |
| (composite) | __m128i_mm_setr_epi32(int i3, int i2, int i1, int i0) |
| (composite) | __m128i_mm_setr_epi16(short w7, short w6, short w5, short w4, short w3, short w2, short w, short w0) |
| (composite) | __m128i_mm_setr_epi8(char w15, char w14, char w13, char w12, char w11, char w10, char w9, char w8, char w7, char w6, char w5, char w4, char w3, char w2, char w1, char w0) |
| (composite) | __m128i_mm_setzero_si128() |
| (composite) | __m128_mm_set_ps1(float w) __m128_mm_set1_ps(float w) |
| (composite) | __m128cmm_set1_pd(double w) |
| (composite) | __m128d_mm_set_sd(double w) |
| (composite) | __m128d_mm_set_pd(double z, double y) |
| (composite) | __m128_mm_set_ps(float z, float y, float x, float w) |
| (composite) | __m128d_mm_setr_pd(double z, double y) |
| (composite) | __m128_mm_setr_ps(float z, float y, float x, float w) |
| (composite) | __m128d_mm_setzero_pd(void) |
| (composite) | __m128_mm_setzero_ps(void) |
| MOVSD + shuffle | __m128d_mm_load_pd(double * p) __m128d_mm_load1_pd(double * p) |
| MOVSS + shuffle | __m128_mm_load_ps1(float * p) __m128_mm_load1_ps(float * p) |
| MOVAPD + shuffle | __m128d_mm_loadr_pd(double * p) |
| MOVAPS + shuffle | __m128_mm_loadr_ps(float * p) |
| MOVSD + shuffle | void __mm_store1_pd(double * p, __m128d a) |
| MOVSS + shuffle | void __mm_store_ps1(float * p, __m128 a) void __mm_store1_ps(float * p, __m128 a) |
| MOVAPD + shuffle | __mm_storer_pd(double * p, __m128d a) |
| MOVAPS + shuffle | __mm_storer_ps(float * p, __m128 a) |

Numerics

- 0000, B-59
- 64-bit mode
 - control and debug registers, 2-15
 - default operand size, 2-15
 - direct memory-offset MOVs, 2-13
 - general purpose encodings, B-24
 - immediates, 2-14
 - introduction, 2-9
 - machine instructions, B-1
 - reg (reg) field, B-4
 - REX prefixes, 2-9, B-2
 - RIP-relative addressing, 2-14
 - SIMD encodings, B-54
 - special instruction encodings, B-92
 - summary table notation, 3-7

A

- AAA instruction, 3-26
- AAD instruction, 3-28
- AAM instruction, 3-30
- AAS instruction, 3-32
- Access rights, segment descriptor, 3-560
- ADC instruction, 3-34, 3-589
- ADD instruction, 3-26, 3-37, 3-284, 3-589
- ADDPD instruction, 3-40
- ADDPS instruction, 3-43
- Addressing methods
 - RIP-relative, 2-14
- Addressing, segments, 1-6
- ADDSI instruction, 3-46
- ADDSS instruction, 3-49
- ADDSUBPD instruction, 3-52
- ADDSUBPS instruction, 3-56
- AND instruction, 3-60, 3-589
- ANDNPD instruction, 3-67
- ANDNPS instruction, 3-69
- ANDPD instruction, 3-63
- ANDPS instruction, 3-65
- Arctangent, x87 FPU operation, 3-393
- ARPL instruction, 3-71
- authenticated code execution mode, 6-4

B

- B (default stack size) flag, segment descriptor, 4-296
- Base (operand addressing), 2-4
- BCD integers
 - packed, 3-284, 3-286, 3-331, 3-333
 - unpacked, 3-26, 3-28, 3-30, 3-32
- Binary numbers, 1-6
- Bit order, 1-4
- bootstrap processor, 6-21
- bootstrap processor, 6-28, 6-37, 6-39, 6-40
- BOUND instruction, 3-84
- BOUND range exceeded exception (#BR), 3-84
- Branch hints, 2-2

- Brand information, 3-204
 - processor brand index, 3-207
 - processor brand string, 3-205
- BSF instruction, 3-87
- BSR instruction, 3-89
- BSWAP instruction, 3-91
- BT instruction, 3-93
- BTC instruction, 3-96, 3-589
- BTR instruction, 3-99, 3-589
- BTS instruction, 3-102, 3-589
- Byte order, 1-4

C

- Cache and TLB information, 3-199
- Cache Inclusiveness, 3-183
- Caches, invalidating (flushing), 3-526, 4-497
- CALL instruction, 3-105
- GETSEC, 6-3
- CBW instruction, 3-123
- CDQ instruction, 3-282
- CDQE instruction, 3-123
- CF (carry) flag, EFLAGS register, 3-37, 3-93, 3-96, 3-99, 3-102, 3-124, 3-133, 3-288, 3-495, 3-501, 3-745, 4-312, 4-379, 4-396, 4-399, 4-428, 4-442
- CLC instruction, 3-124
- CLD instruction, 3-125
- CLFLUSH instruction, 3-126
 - CPUID flag, 3-198
- CLI instruction, 3-128
- CLTS instruction, 3-131
- CMC instruction, 3-133
- CMOVcc flag, 3-198
- CMOVcc instructions, 3-134
 - CPUID flag, 3-198
- CMP instruction, 3-141
- CMPPD instruction, 3-144
- CMPPS instruction, 3-149
- CMPS instruction, 3-154, 4-333
- CMPSB instruction, 3-154
- CMPSD instruction, 3-154, 3-160
- CMPSQ instruction, 3-154
- CMPSI instruction, 3-164
- CMPSW instruction, 3-154
- CMPXCHG instruction, 3-168, 3-589
- CMPXCHG16B instruction, 3-171
 - CPUID bit, 3-194
- CMPXCHG8B instruction, 3-171
 - CPUID flag, 3-197
- COMISD instruction, 3-174
- COMISS instruction, 3-177
- Compatibility mode
 - introduction, 2-9
 - see 64-bit mode
 - summary table notation, 3-7
- Compatibility, software, 1-4
- compilers

INDEX

- documentation, 1-9
 - Condition code flags, EFLAGS register, 3-134
 - Condition code flags, x87 FPU status word
 - flags affected by instructions, 3-14
 - setting, 3-443, 3-445, 3-448
 - Conditional jump, 3-541
 - Conforming code segment, 3-561
 - Constants (floating point), loading, 3-381
 - Control registers, moving values to and from, 3-645
 - Cosine, x87 FPU operation, 3-349, 3-418
 - CPL, 3-128, 4-492
 - CPUID instruction, 3-180, 3-198
 - 36-bit page size extension, 3-198
 - AP-485, 1-9
 - APIC on-chip, 3-197
 - basic CPUID information, 3-181
 - cache and TLB characteristics, 3-181
 - CLFLUSH flag, 3-198
 - CLFLUSH instruction cache line size, 3-192
 - CMPXCHG16B flag, 3-194
 - CMPXCHG8B flag, 3-197
 - CPL qualified debug store, 3-193
 - debug extensions, CR4.DE, 3-197
 - debug store supported, 3-198
 - deterministic cache parameters leaf, 3-182, 3-185, 3-186, 3-187
 - extended function information, 3-187
 - feature information, 3-196
 - FPU on-chip, 3-197
 - FSAVE flag, 3-198
 - FXRSTOR flag, 3-198
 - HT technology flag, 3-199
 - IA-32e mode available, 3-187
 - input limits for EAX, 3-189
 - L1 Context ID, 3-194
 - local APIC physical ID, 3-192
 - machine check architecture, 3-198
 - machine check exception, 3-197
 - memory type range registers, 3-197
 - MONITOR feature information, 3-203
 - MONITOR/MWAIT flag, 3-193
 - MONITOR/MWAIT leaf, 3-183, 3-184, 3-185
 - MWAIT feature information, 3-203
 - page attribute table, 3-198
 - page size extension, 3-197
 - performance monitoring features, 3-204
 - physical address bits, 3-188
 - physical address extension, 3-197
 - power management, 3-203, 3-204
 - processor brand index, 3-192, 3-205
 - processor brand string, 3-188, 3-204
 - processor serial number, 3-181, 3-198
 - processor type field, 3-191
 - PTE global bit, 3-198
 - RDMSR flag, 3-197
 - returned in EBX, 3-192
 - returned in ECX & EDX, 3-192
 - self snoop, 3-199
 - SpeedStep technology, 3-194
 - SS2 extensions flag, 3-199
 - SSE extensions flag, 3-199
 - SSE3 extensions flag, 3-193
 - SSSE3 extensions flag, 3-194
 - SYSENTER flag, 3-197
 - SYSEXIT flag, 3-197
 - thermal management, 3-203, 3-204
 - thermal monitor, 3-194, 3-198, 3-199
 - time stamp counter, 3-197
 - using CPUID, 3-180
 - vendor ID string, 3-189
 - version information, 3-181, 3-203
 - virtual 8086 Mode flag, 3-197
 - virtual address bits, 3-188
 - WRMSR flag, 3-197
 - CQO instruction, 3-282
 - CRO control register, 4-413
 - CS register, 3-106, 3-511, 3-530, 3-549, 3-640, 4-204
 - CVTDQ2PD instruction, 3-213
 - CVTDQ2PS instruction, 3-219
 - CVTPD2DQ instruction, 3-222
 - CVTPD2PI instruction, 3-225
 - CVTPD2PS instruction, 3-228
 - CVTPI2PD instruction, 3-231
 - CVTPI2PS instruction, 3-234
 - CVTPS2DQ instruction, 3-237
 - CVTPS2PD instruction, 3-240
 - CVTPS2PI instruction, 3-243
 - CVTSD2SI instruction, 3-246
 - CVTSD2SS instruction, 3-249
 - CVTSI2SD instruction, 3-252
 - CVTSI2SS instruction, 3-255
 - CVTSS2SD instruction, 3-258
 - CVTSS2SI instruction, 3-261
 - CVTTPD2DQ instruction, 3-264
 - CVTTPD2PI instruction, 3-264, 3-267
 - CVTTPS2DQ instruction, 3-270
 - CVTTPS2PI instruction, 3-273
 - CVTTSD2SI instruction, 3-276
 - CVTTSS2SI instruction, 3-279
 - CWD instruction, 3-282
 - CWDE instruction, 3-123
 - C/C++ compiler intrinsics
 - compiler functional equivalents, C-1
 - composite, C-16
 - description of, 3-11
 - lists of, C-1
 - simple, C-2
- ## D
- D (default operation size) flag, segment descriptor, 4-204, 4-210, 4-296
 - DAA instruction, 3-284
 - DAS instruction, 3-286
 - Debug registers, moving value to and from, 3-648

DEC instruction, 3-288, 3-589
 Denormalized finite number, 3-448
 Detecting and Enabling SMX
 level 2, 6-2
 DF (direction) flag, EFLAGS register, 3-125, 3-156,
 3-505, 3-592, 3-715, 4-19, 4-383, 4-429
 Displacement (operand addressing), 2-4
 DIV instruction, 3-291
 Divide error exception (#DE), 3-291
 DIVPD instruction, 3-295
 DIVPS instruction, 3-298
 DIVSD instruction, 3-301
 DIVSS instruction, 3-304
 DS register, 3-155, 3-569, 3-591, 3-714, 4-18

E

EDI register, 4-382, 4-429, 4-435
 Effective address, 3-575
 EFLAGS register
 condition codes, 3-138, 3-340, 3-346
 flags affected by instructions, 3-14
 popping, 4-214
 popping on return from interrupt, 3-530
 pushing, 4-303
 pushing on interrupts, 3-511
 saving, 4-369
 status flags, 3-141, 3-545, 4-389, 4-471
 EIP register, 3-106, 3-511, 3-530, 3-549
 EMMS instruction, 3-314
 Encodings
 See machine instructions, opcodes
 ENTER instruction, 3-316
 GETSEC, 6-4, 6-12
 Error numbers
 VM-instruction error field, 5-38
 ES register, 3-569, 4-18, 4-382, 4-435
 ESI register, 3-155, 3-591, 3-592, 3-714, 4-18, 4-429
 ESP register, 3-106, 4-204
 Exceptions
 BOUND range exceeded (#BR), 3-84
 notation, 1-6
 overflow exception (#OF), 3-511
 returning from, 3-530
 GETSEC, 6-4, 6-6
 Exponent, extracting from floating-point number,
 3-466
 Extract exponent and significand, x87 FPU operation
 , 3-466

F

F2XM1 instruction, 3-323, 3-466
 FABS instruction, 3-325
 FADD instruction, 3-327
 FADDP instruction, 3-327
 Far pointer, loading, 3-569
 Far return, RET instruction, 4-336

FBLD instruction, 3-331
 FBSTP instruction, 3-333
 FCHS instruction, 3-336
 FCLEX instruction, 3-338
 FCMOVcc instructions, 3-340
 FCOM instruction, 3-342
 FCOMI instruction, 3-346
 FCOMIP instruction, 3-346
 FCOMP instruction, 3-342
 FCOMPP instruction, 3-342
 FCOS instruction, 3-349
 FDECSTP instruction, 3-351
 FDIV instruction, 3-353
 FDIVP instruction, 3-353
 FDIVR instruction, 3-357
 FDIVRP instruction, 3-357
 Feature information, processor, 3-180
 FFREE instruction, 3-361
 FIADD instruction, 3-327
 FICOM instruction, 3-362
 FICOMP instruction, 3-362
 FIDIV instruction, 3-353
 FIDIVR instruction, 3-357
 FILD instruction, 3-365
 FIMUL instruction, 3-388
 FINCSTP instruction, 3-367
 FINIT instruction, 3-369
 FINIT/FNINIT instructions, 3-410
 FIST instruction, 3-371
 FISTP instruction, 3-371
 FISTTP instruction, 3-375
 FISUB instruction, 3-435
 FISUBR instruction, 3-439
 FLD instruction, 3-378
 FLD1 instruction, 3-381
 FLDcw instruction, 3-383
 FLDENv instruction, 3-385
 FLDL2E instruction, 3-381
 FLDL2T instruction, 3-381
 FLDLG2 instruction, 3-381
 FLDLN2 instruction, 3-381
 FLDPI instruction, 3-381
 FLDZ instruction, 3-381
 Floating point instructions
 machine encodings, B-92
 Floating-point exceptions
 SSE and SSE2 SIMD, 3-17
 x87 FPU, 3-17
 Flushing
 caches, 3-526, 4-497
 TLB entry, 3-528
 FMUL instruction, 3-388
 FMULP instruction, 3-388
 FNCLEX instruction, 3-338
 FNINIT instruction, 3-369
 FNOP instruction, 3-392
 FNSAVE instruction, 3-410
 FNSTCW instruction, 3-426

INDEX

FNSTENV instruction, 3-385, 3-429
FNSTSW instruction, 3-432
FPATAN instruction, 3-393
FPREM instruction, 3-396
FPREM1 instruction, 3-399
FPTAN instruction, 3-402
FRNDINT instruction, 3-405
FRSTOR instruction, 3-407
FS register, 3-569
FSAVE instruction, 3-410
FSAVE/FNSAVE instructions, 3-407
FSCALE instruction, 3-414
FSIN instruction, 3-416
FSINCOS instruction, 3-418
FSQRT instruction, 3-421
FST instruction, 3-423
FSTCW instruction, 3-426
FSTENV instruction, 3-429
FSTP instruction, 3-423
FSTSW instruction, 3-432
FSUB instruction, 3-435
FSUBP instruction, 3-435
FSUBR instruction, 3-439
FSUBRP instruction, 3-439
FTST instruction, 3-443
FUCOM instruction, 3-445
FUCOMI instruction, 3-346
FUCOMIP instruction, 3-346
FUCOMP instruction, 3-445
FUCOMPP instruction, 3-445
FXAM instruction, 3-448
FXCH instruction, 3-450
FXRSTOR instruction, 3-452
 CUID flag, 3-198
FXSAVE instruction, 3-455, 4-507, 4-518, 4-523,
 4-527
 CUID flag, 3-198
FXTRACT instruction, 3-414, 3-466
FYL2X instruction, 3-468
FYL2XP1 instruction, 3-470

G

GDT (global descriptor table), 3-581, 3-584
GDTR (global descriptor table register), 3-581, 4-393
General-purpose instructions
 64-bit encodings, B-24
 non-64-bit encodings, B-9
General-purpose registers
 moving value to and from, 3-640
 popping all, 4-210
 pushing all, 4-300
GETSEC, 6-1, 6-3, 6-7
GS register, 3-569

H

HADDPS instruction, 3-472, 3-473

HADDPS instruction, 3-476
Hexadecimal numbers, 1-6
HLT instruction, 3-480
HSUBPD instruction, 3-482
HSUBPS instruction, 3-486
Hyper-Threading Technology
 CUID flag, 3-199

I

IA-32e mode
 CUID flag, 3-187
 introduction, 2-9
 see 64-bit mode
 see compatibility mode
IA32_SYSENTER_CS MSR, 4-463, 4-466, 4-467
IA32_SYSENTER_EIP MSR, 4-463
IA32_SYSENTER_ESP MSR, 4-463
IDIV instruction, 3-490
IDT (interrupt descriptor table), 3-512, 3-581
IDTR (interrupt descriptor table register), 3-581,
 4-408
IF (interrupt enable) flag, EFLAGS register, 3-128,
 4-430
Immediate operands, 2-4
IMUL instruction, 3-494
IN instruction, 3-499
INC instruction, 3-501, 3-589
Index (operand addressing), 2-4
Initialization x87 FPU, 3-369
initiating logical processor, 6-4, 6-6, 6-12, 6-13, 6-27,
 6-28
INS instruction, 3-504, 4-333
INSB instruction, 3-504
INSD instruction, 3-504
instruction encodings, B-88, B-96
Instruction format
 base field, 2-4
 description of reference information, 3-1
 displacement, 2-4
 immediate, 2-4
 index field, 2-4
 Mod field, 2-4
 ModR/M byte, 2-4
 opcode, 2-3
 operands, 1-5
 prefixes, 2-1
 reg/opcode field, 2-4
 r/m field, 2-4
 scale field, 2-4
 SIB byte, 2-4
 See also: machine instructions, opcodes
Instruction reference, nomenclature, 3-1
Instruction set, reference, 3-1
INSW instruction, 3-504
INT 3 instruction, 3-511
Integer, storing, x87 FPU data type, 3-371
Intel 64 architecture

- definition of, 1-3
- instruction format, 2-1
- relation to IA-32, 1-3
- Intel developer link, 1-9
- Intel NetBurst microarchitecture, 1-2
- Intel software network link, 1-9
- Intel VTune Performance Analyzer
 - related information, 1-9
- Intel Xeon processor, 1-1
- Intel® Trusted Execution Technology, 6-4
- Inter-privilege level
 - call, CALL instruction, 3-106
 - return, RET instruction, 4-336
- Interrupts
 - interrupt vector 4, 3-511
 - returning from, 3-530
 - software, 3-511
- INTn instruction, 3-511
- INTO instruction, 3-511
- Intrinsics
 - compiler functional equivalents, C-1
 - composite, C-16
 - description of, 3-11
 - list of, C-1
 - simple, C-2
- INVD instruction, 3-526
- INVLPG instruction, 3-528
- IOPL (I/O privilege level) field, EFLAGS register, 3-128, 4-303, 4-430
- IRET instruction, 3-530
- IRETD instruction, 3-530

J

- Jcc instructions, 3-541
- JMP instruction, 3-548
- Jump operation, 3-548

L

- L1 Context ID, 3-194
- LAHF instruction, 3-558
- LAR instruction, 3-560
- Last branch
 - interrupt & exception recording
 - description of, 4-348
- LDDQU instruction, 3-564
- LDMXCSR instruction, 3-567
- LDS instruction, 3-569
- LDT (local descriptor table), 3-584
- LDTR (local descriptor table register), 3-584, 4-411
- LEA instruction, 3-575
- LEAVE instruction, 3-578
- LES instruction, 3-569
- LFENCE instruction, 3-580
- LFS instruction, 3-569
- LGDT instruction, 3-581
- LGS instruction, 3-569

- LIDT instruction, 3-581
- LLDT instruction, 3-584
- LMSW instruction, 3-587
- Load effective address operation, 3-575
- LOCK prefix, 3-35, 3-38, 3-61, 3-96, 3-99, 3-102, 3-168, 3-288, 3-501, 3-589, 4-2, 4-7, 4-10, 4-379, 4-442, 4-501, 4-505, 4-512
- Locking operation, 3-589
- LODS instruction, 3-591, 4-333
- LODSB instruction, 3-591
- LODSD instruction, 3-591
- LODSQ instruction, 3-591
- LODSW instruction, 3-591
- Log epsilon, x87 FPU operation, 3-468
- Log (base 2), x87 FPU operation, 3-470
- LOOP instructions, 3-595
- LOOPcc instructions, 3-595
- LSL instruction, 3-598
- LSS instruction, 3-569
- LTR instruction, 3-602

M

- Machine check architecture
 - CPUID flag, 3-198
 - description, 3-198
- Machine instructions
 - 64-bit mode, B-1
 - condition test (tttn) field, B-7
 - direction bit (d) field, B-8
 - floating-point instruction encodings, B-92
 - general description, B-1
 - general-purpose encodings, B-9–B-53
 - legacy prefixes, B-2
 - MMX encodings, B-54–B-58
 - opcode fields, B-2
 - operand size (w) bit, B-5
 - P6 family encodings, B-59
 - Pentium processor family encodings, B-53
 - reg (reg) field, B-3, B-4
 - REX prefixes, B-2
 - segment register (sreg) field, B-6
 - sign-extend (s) bit, B-5
 - SIMD 64-bit encodings, B-54
 - special 64-bit encodings, B-92
 - special fields, B-2
 - special-purpose register (eee) field, B-6
 - SSE encodings, B-60–B-69
 - SSE2 encodings, B-69–B-85
 - SSE3 encodings, B-86–B-88
 - SSSE3 encodings, B-88–B-92
 - VMX encodings, B-112–B-113, B-114–??
 - See also: opcodes
- Machine status word, CR0 register, 3-587, 4-413
- MASKMOVDQU instruction, 3-605
- MASKMOVQ instruction, 3-608
- MAXPD instruction, 3-611
- MAXPS instruction, 3-614

INDEX

MAXSD instruction, 3-617
MAXSS instruction, 3-620
measured environment, 6-1
Measured Launched Environment, 6-1, 6-33
MFENCE instruction, 3-623
MINPD instruction, 3-624
MINPS instruction, 3-627
MINSD instruction, 3-630
MINSS instruction, 3-633
MLE, 6-1
MMX instructions
 CPUID flag for technology, 3-198
 encodings, B-54
Mod field, instruction format, 2-4
Model & family information, 3-203
ModR/M byte, 2-4
 16-bit addressing forms, 2-6
 32-bit addressing forms of, 2-7
 description of, 2-4
MONITOR instruction, 3-636
 CPUID flag, 3-193
 feature data, 3-203
MOV instruction, 3-639
MOV instruction (control registers), 3-645
MOV instruction (debug registers), 3-648, 3-656
MOVAPD instruction, 3-650
MOVAPS instruction, 3-653
MOVD instruction, 3-656
MOVDDUP instruction, 3-663
MOVDDQ instruction, 3-671
MOVDDQA instruction, 3-666
MOVDDQU instruction, 3-668
MOVHLPS instruction, 3-673
MOVHPD instruction, 3-675
MOVHPS instruction, 3-678
MOVLHP instruction, 3-681
MOVLHPS instruction, 3-681
MOVLPD instruction, 3-683
MOVLPS instruction, 3-685
MOVMSKPD instruction, 3-688
MOVMSKPS instruction, 3-690
MOVNTDQ instruction, 3-695
MOVNTI instruction, 3-698
MOVNTPD instruction, 3-700
MOVNTPS instruction, 3-703
MOVNTQ instruction, 3-706
MOVQ instruction, 3-656, 3-709
MOVQ2DQ instruction, 3-712
MOVS instruction, 3-714, 4-333
MOVSB instruction, 3-714
MOVSD instruction, 3-714, 3-719
MOVSHDUP instruction, 3-722
MOVSLDUP instruction, 3-725
MOVSQ instruction, 3-714
MOVSS instruction, 3-728
MOVSW instruction, 3-714
MOVSX instruction, 3-731
MOVFXD instruction, 3-731

MOVUPD instruction, 3-733
MOVUPS instruction, 3-736
MOVZX instruction, 3-739
MSRs (model specific registers)
 reading, 4-322
MUL instruction, 3-30, 3-745
MULPD instruction, 3-748
MULPS instruction, 3-751
MULSD instruction, 3-754
MULSS instruction, 3-757
Multi-byte no operation, 4-5, B-16
MVMM, 6-1, 6-6, 6-7, 6-48
MWAIT instruction, 3-760
 CPUID flag, 3-193
 feature data, 3-203

N

NaN. testing for, 3-443
Near
 return, RET instruction, 4-336
NEG instruction, 3-589, 4-2
NetBurst microarchitecture (see Intel NetBurst microarchitecture)
No operation, 4-5, B-16
Nomenclature, used in instruction reference pages, 3-1
NOP instruction, 4-5
NOT instruction, 3-589, 4-7
Notation
 bit and byte order, 1-4
 exceptions, 1-6
 hexadecimal and binary numbers, 1-6
 instruction operands, 1-5
 reserved bits, 1-4
 segmented addressing, 1-6
Notational conventions, 1-4
NT (nested task) flag, EFLAGS register, 3-530

O

OF (carry) flag, EFLAGS register, 3-495
OF (overflow) flag, EFLAGS register, 3-37, 3-511, 3-745, 4-379, 4-396, 4-399, 4-442
Opcode format, 2-3
Opcodes
 addressing method codes for, A-2
 extensions, A-20
 extensions tables, A-21
 group numbers, A-20
 integers
 one-byte opcodes, A-10
 two-byte opcodes, A-12
 key to abbreviations, A-2
 look-up examples, A-4, A-20, A-23
 ModR/M byte, A-20
 one-byte opcodes, A-4, A-10
 opcode maps, A-1

- operand type codes for, A-3
- register codes for, A-4
- superscripts in tables, A-7
- two-byte opcodes, A-5, A-6, A-12
- VMX instructions, B-112, B-114
- x87 ESC instruction opcodes, A-23

Operands, 1-5

OR instruction, 3-589, 4-9

ORPD instruction, 4-12

ORPS instruction, 4-14

OUT instruction, 4-16

OUTS instruction, 4-18, 4-333

OUTSB instruction, 4-18

OUTSD instruction, 4-18

OUTSW instruction, 4-18

Overflow exception (#OF), 3-511

P

P6 family processors

- description of, 1-1

- machine encodings, B-59

PABSB instruction, 4-23

PABSD instruction, 4-23

PABSW instruction, 4-23

PACKSSDW instruction, 4-27

PACKSSWB instruction, 4-27

PACKUSWB instruction, 4-35

PADDB instruction, 4-39

PADD instruction, 4-39

PADDQ instruction, 4-43

PADDSB instruction, 4-46

PADDSW instruction, 4-46

PADDUSB instruction, 4-50

PADDUSW instruction, 4-50

PADDW instruction, 4-39

PALIGNR instruction, 4-54

PAND instruction, 4-57

PANDN instruction, 4-60

GETSEC, 6-5

PAUSE instruction, 4-63

PAVGB instruction, 4-64

PAVGW instruction, 4-64

PCE flag, CR4 register, 4-326

PCMPSEQB instruction, 4-75

PCMPSEQD instruction, 4-75

PCMPSEQW instruction, 4-75

PCMPGTB instruction, 4-93

PCMPGTD instruction, 4-93

PCMPGTW instruction, 4-93

PE (protection enable) flag, CR0 register, 3-587

Pending break enable, 3-199

Pentium 4 processor, 1-1

Pentium II processor, 1-2

Pentium III processor, 1-2

Pentium Pro processor, 1-2

Pentium processor, 1-1

Pentium processor family processors

- machine encodings, B-53

Performance-monitoring counters

- CPUID inquiry for, 3-204

- reading, 4-324

PEXTRW instruction, 4-103

PHADDD instruction, 4-107

PHADDSW instruction, 4-110

PHADDW instruction, 4-107

PHSUBD instruction, 4-116

PHSUBSW instruction, 4-119

PHSUBW instruction, 4-116

Pi, 3-381

PINSRW instruction, 4-125, 4-242

PMADDUBSW instruction, 4-128

PMADDUDSW instruction, 4-128

PMADDWD instruction, 4-131

PMAXSW instruction, 4-141

PMAXUB instruction, 4-144

PMINSW instruction, 4-159

PMINUB instruction, 4-162

PMOVMSKB instruction, 4-165

PMULHRSW instruction, 4-184

PMULHUW instruction, 4-187

PMULHW instruction, 4-191

PMULLW instruction, 4-196

PMULUDQ instruction, 4-200

POP instruction, 4-203

POPA instruction, 4-210

POPAD instruction, 4-210

POPF instruction, 4-214

POPFD instruction, 4-214

POPfq instruction, 4-214

POR instruction, 4-218

PREFETCHh instruction, 4-221

Prefixes

- Address-size override prefix, 2-2

- Branch hints, 2-2

- branch hints, 2-2

- instruction, description of, 2-1

- legacy prefix encodings, B-2

- LOCK, 2-2, 3-589

- Operand-size override prefix, 2-2

- REP or REPE/REPZ, 2-2

- REPNE/REPnz, 2-2

- REP/REPE/REPZ/REPNE/REPnz, 4-331

- REX prefix encodings, B-2

- Segment override prefixes, 2-2

PSADBW instruction, 4-223

Pseudo-functions

- VMfail, 5-2

- VMfailInvalid, 5-2

- VMfailValid, 5-2

- VMsucceed, 5-2

PSHUFB instruction, 4-227

PSHUFD instruction, 4-231

PSHUFW instruction, 4-234

PSHUFLW instruction, 4-237

PSHUFW instruction, 4-240

INDEX

PSIGNB instruction, 4-242
PSIGND instruction, 4-242
PSIGNW instruction, 4-242
PSLLD instruction, 4-249
PSLLDQ instruction, 4-247
PSLLQ instruction, 4-249
PSLLW instruction, 4-249
PSRAD instruction, 4-254
PSRAW instruction, 4-254
PSRLD instruction, 4-261
PSRLDQ instruction, 4-259
PSRLQ instruction, 4-261
PSRLW instruction, 4-261
PSUBB instruction, 4-266
PSUBD instruction, 4-266
PSUBQ instruction, 4-270
PSUBSB instruction, 4-273
PSUBSW instruction, 4-273
PSUBUSB instruction, 4-277
PSUBUSW instruction, 4-277
PSUBW instruction, 4-266
PUNPCKHBW instruction, 4-284
PUNPCKHDQ instruction, 4-284
PUNPCKHQDQ instruction, 4-284
PUNPCKHWD instruction, 4-284
PUNPCKLBW instruction, 4-290
PUNPCKLDQ instruction, 4-290
PUNPCKLQDQ instruction, 4-290
PUNPCKLWD instruction, 4-290
PUSH instruction, 4-295
PUSHA instruction, 4-300
PUSHAD instruction, 4-300
PUSHF instruction, 4-303
PUSHFD instruction, 4-303
PXOR instruction, 4-306

R

RC (rounding control) field, x87 FPU control word,
3-372, 3-381, 3-423
RCL instruction, 4-309
RCPPS instruction, 4-316
RCPS instruction, 4-319
RCR instruction, 4-309
RDMSR instruction, 4-322, 4-326, 4-329
 CPUID flag, 3-197
RDPMC instruction, 4-324
RDTSC instruction, 4-329
Reg/opcode field, instruction format, 2-4
Related literature, 1-8
Remainder, x87 FPU operation, 3-399
REP/REPE/REPZ/REPNE/REPZ prefixes, 3-156,
3-505, 4-19, 4-331
Reserved
 use of reserved bits, 1-4
Responding logical processor, 6-6
responding logical processor, 6-4, 6-5, 6-6
RET instruction, 4-336

REX prefixes
 addressing modes, 2-11
 and INC/DEC, 2-10
 encodings, 2-10, B-2
 field names, 2-11
 ModR/M byte, 2-10
 overview, 2-9
 REX.B, 2-10
 REX.R, 2-10
 REX.W, 2-10
 special encodings, 2-13
RIP-relative addressing, 2-14
ROL instruction, 4-309
ROR instruction, 4-309
Rounding
 modes, floating-point operations, 4-349
Rounding control (RC) field
 MXCSR register, 4-349
 x87 FPU control word, 4-349
Rounding, round to integer, x87 FPU operation, 3-405
RPL field, 3-71
RSM instruction, 4-361
RSQRTPS instruction, 4-363
RSQRTPSS instruction, 4-366
R/m field, instruction format, 2-4

S

Safer Mode Extensions, 6-1
SAHF instruction, 4-369
SAL instruction, 4-371
SAR instruction, 4-371
SBB instruction, 3-589, 4-378
Scale (operand addressing), 2-4
Scale, x87 FPU operation, 3-414
Scan string instructions, 4-382
SCAS instruction, 4-333, 4-382
SCASB instruction, 4-382
SCASD instruction, 4-382
SCASW instruction, 4-382
Segment
 descriptor, segment limit, 3-598
 limit, 3-598
 registers, moving values to and from, 3-640
 selector, RPL field, 3-71
Segmented addressing, 1-6
Self Snoop, 3-199
GETSEC, 6-2, 6-4, 6-6
SENTER sleep state, 6-12
SETcc instructions, 4-387
GETSEC, 6-5
SF (sign) flag, EFLAGS register, 3-37
SFENCE instruction, 4-392
SGDT instruction, 4-393
SHAF instruction, 4-369
Shift instructions, 4-371
SHL instruction, 4-371
SHLD instruction, 4-396

SHR instruction, 4-371
 SHRD instruction, 4-399
 SHUFPS instruction, 4-402
 SHUFPS instruction, 4-405
 SIB byte, 2-4
 32-bit addressing forms of, 2-8
 description of, 2-4
 SIDT instruction, 4-393, 4-408
 Significand, extracting from floating-point number,
 3-466
 SIMD floating-point exceptions, unmasking, effects of
 , 3-567
 Sine, x87 FPU operation, 3-416, 3-418
 SINIT, 6-5
 SLDT instruction, 4-411
 GETSEC, 6-5
 SMSW instruction, 4-413
 SpeedStep technology, 3-194
 SQRTPD instruction, 4-416
 SQRTPS instruction, 4-419
 SQRTSD instruction, 4-422
 SQRTSS instruction, 4-425
 Square root, Fx87 PU operation, 3-421
 SS register, 3-569, 3-641, 4-204
 SSE extensions
 cacheability instruction encodings, B-68
 CPUID flag, 3-199
 floating-point encodings, B-60
 instruction encodings, B-60
 integer instruction encodings, B-67
 memory ordering encodings, B-68
 SSE2 extensions
 cacheability instruction encodings, B-85
 CPUID flag, 3-199
 floating-point encodings, B-69
 integer instruction encodings, B-78
 SSE3
 CPUID flag, 3-193
 SSE3 extensions
 CPUID flag, 3-193
 event mgmt instruction encodings, B-87
 floating-point instruction encodings, B-86
 integer instruction encodings, B-87, B-88
 SSSE3 extensions, B-88, B-96
 CPUID flag, 3-194
 Stack, pushing values on, 4-296
 Status flags, EFLAGS register, 3-138, 3-141, 3-340,
 3-346, 3-545, 4-389, 4-471
 STC instruction, 4-428
 STD instruction, 4-429
 Stepping information, 3-203
 STI instruction, 4-430
 STMXCSR instruction, 4-433
 STOS instruction, 4-333, 4-435
 STOSB instruction, 4-435
 STOSD instruction, 4-435
 STOSQ instruction, 4-435
 STOSW instruction, 4-435

STR instruction, 4-439
 String instructions, 3-154, 3-504, 3-591, 3-714,
 4-18, 4-382, 4-435
 SUB instruction, 3-32, 3-286, 3-589, 4-441
 SUBPD instruction, 4-444
 SUBSS instruction, 4-453
 Summary table notation, 3-7
 SWAPGS instruction, 4-456
 SYSCALL instruction, 4-458
 SYSENTER instruction, 4-460
 CPUID flag, 3-197
 SYSEXIT instruction, 4-464
 CPUID flag, 3-197
 SYSRET instruction, 4-468

T

Tangent, x87 FPU operation, 3-402
 Task register
 loading, 3-602
 storing, 4-439
 Task switch
 CALL instruction, 3-106
 return from nested task, IRET instruction, 3-530
 TEST instruction, 4-470
 Thermal Monitor
 CPUID flag, 3-199
 Thermal Monitor 2, 3-194
 CPUID flag, 3-194
 Time Stamp Counter, 3-197
 Time-stamp counter, reading, 4-329
 TLB entry, invalidating (flushing), 3-528
 Trusted Platform Module, 6-6
 TS (task switched) flag, CR0 register, 3-131
 TSD flag, CR4 register, 4-329
 TSS, relationship to task register, 4-439

U

UCOMISD instruction, 4-473
 UCOMISS instruction, 4-476
 UD2 instruction, 4-479
 Undefined, format opcodes, 3-443
 Unordered values, 3-342, 3-443, 3-445
 UNPCKHPD instruction, 4-480
 UNPCKHPS instruction, 4-483
 UNPCKLPD instruction, 4-486
 UNPCKLPS instruction, 4-489

V

VERR instruction, 4-492
 Version information, processor, 3-180
 VERW instruction, 4-492
 Virtual Machine Monitor, 6-1
 VM (virtual 8086 mode) flag, EFLAGS register, 3-530
 VMCALL instruction, 5-1
 VMCLEAR instruction, 5-1
 VMCS

INDEX

- error numbers, 5-38
- VM-instruction error field, 5-38
- VMLAUNCH instruction, 5-1
- VMM, 6-1
- VMPTRLD instruction, 5-1
- VMPTRST instruction, 5-1
- VMREAD instruction, 5-1
- VMRESUME instruction, 5-1, 5-2
- VMWRITE instruction, 5-1
- VMXOFF instruction, 5-1
- VMXON instruction, 5-2

W

- WAIT/FWAIT instructions, 4-495
- GETSEC, 6-6
- WBINVD instruction, 4-497
- WBINVD/INVD bit, 3-183
- Write-back and invalidate caches, 4-497
- WRMSR instruction, 4-499
 - CPUID flag, 3-197

X

- x87 FPU
 - checking for pending x87 FPU exceptions, 4-495
 - constants, 3-381
 - initialization, 3-369
 - instruction opcodes, A-23
- x87 FPU control word
 - loading, 3-383, 3-385
 - RC field, 3-372, 3-381, 3-423
 - restoring, 3-407
 - saving, 3-410, 3-429
 - storing, 3-426
- x87 FPU data pointer, 3-385, 3-407, 3-410, 3-429
- x87 FPU instruction pointer, 3-385, 3-407, 3-410, 3-429
- x87 FPU last opcode, 3-385, 3-407, 3-410, 3-429
- x87 FPU status word
 - condition code flags, 3-342, 3-362, 3-443, 3-445, 3-448
 - loading, 3-385
 - restoring, 3-407
 - saving, 3-410, 3-429, 3-432
 - TOP field, 3-367
 - x87 FPU flags affected by instructions, 3-14
- x87 FPU tag word, 3-385, 3-407, 3-410, 3-429
- XADD instruction, 3-589, 4-501
- XCHG instruction, 3-589, 4-504
- XFEATURE_ENABLED_MASK, 4-507, 4-518, 4-519, 4-523, 4-527, 4-528
- XGETBV, 4-507, 4-518, B-59
- XLAB instruction, 4-509
- XLAT instruction, 4-509
- XOR instruction, 3-589, 4-511
- XORPD instruction, 4-514
- XORPS instruction, 4-516

- XRSTOR, 4-523, B-59
- XSAVE, 4-507, 4-518, 4-519, 4-520, 4-521, 4-522, 4-523, 4-525, 4-526, 4-527, 4-528, B-59
- XSETBV, 4-527, B-59

Z

- ZF (zero) flag, EFLAGS register, 3-168, 3-560, 3-595, 3-598, 4-333, 4-492