

Princeton University
COS 217: Introduction to Programming Systems
A Subset of IA-32 Assembly Language

1. Instruction Operands

1.1. Immediate Operands

Syntax: $\$i$

Semantics: Evaluates to i . Note that i could be a label...

Syntax: $\$label$

Semantics: Evaluates to the memory address denoted by $label$.

1.2. Register Operands

Syntax: $\%r$

Semantics: Evaluates to $\text{reg}[r]$, that is, the contents of register r .

1.3. Memory Operands

Syntax: $disp(\%base, \%index, scale)$

Semantics:

$disp$ is a literal or label.

$base$ is a general purpose register.

$index$ is any general purpose register except EBP.

$scale$ is the literal 1, 2, 4, or 8.

One of $disp$, $base$, or $index$ is required. All other fields are optional.

Evaluates to the contents of memory at a certain address. The address is computed using this formula:

$$disp + \text{reg}[base] + (\text{reg}[index] * scale)$$

The default $disp$ is 0. The default $scale$ is 1. If $base$ is omitted, then $\text{reg}[base]$ evaluates to 0. If $index$ is omitted, then $\text{reg}[index]$ evaluates to 0.

2. Commonly Used Memory Operands

Syntax	Semantics	Description
<i>label</i>	disp: <i>label</i> base: (none) index: (none) scale: (none) mem[0+(0*0)+ <i>label</i>] mem[<i>label</i>]	<p>Direct Addressing. The contents of memory at a certain address. The offset of that address is denoted by <i>label</i>.</p> <p>Often used to access a long, word, or byte in the bss, data, or rodata section.</p>
(% <i>r</i>)	disp: (none) base: <i>r</i> index: (none) scale: (none) mem[reg[<i>r</i>]+(0*0)+0] mem[reg[<i>r</i>]]	<p>Indirect Addressing. The contents of memory at a certain address. The offset of that address is the contents of register <i>r</i>.</p> <p>Often used to access a long, word, or byte in the stack section.</p>
<i>i</i> (% <i>r</i>)	disp: <i>i</i> base: <i>r</i> index: (none) scale: (none) mem[reg[<i>r</i>]+(0*0)+ <i>i</i>] mem[reg[<i>r</i>]+ <i>i</i>]	<p>Base-Pointer Addressing. The contents of memory at a certain address. The offset of that address is the sum of <i>i</i> and the contents of register <i>r</i>.</p> <p>Often used to access a long, word, or byte in the stack section.</p>
<i>label</i> (% <i>r</i>)	disp: <i>label</i> base: <i>r</i> index: (none) scale: (none) mem[reg[<i>r</i>]+(0*0)+ <i>label</i>] mem[reg[<i>r</i>]+ <i>label</i>]	<p>Indexed Addressing. The contents of memory at a certain address. The offset of that address is the sum of the address denoted by <i>label</i> and the contents of register <i>r</i>.</p> <p>Often used to access an array of bytes (characters) in the bss, data, or rodata section.</p>
<i>label</i> (,% <i>r</i> , <i>i</i>)	disp: <i>label</i> base: (none) index: <i>r</i> scale: <i>i</i> mem[0+(reg[<i>r</i>]* <i>i</i>)+ <i>label</i>] mem[(reg[<i>r</i>]* <i>i</i>)+ <i>label</i>]	<p>Indexed Addressing. The contents of memory at a certain address. The offset of that address is the sum of the address denoted by <i>label</i>, and the contents of register <i>r</i> multiplied by <i>i</i>.</p> <p>Often used to access an array of longs or words in the bss, data, or rodata section.</p>

3. Assembler Mnemonics

Key:

src: a source operand
dest: a destination operand
I: an immediate operand
R: a register operand
M: a memory operand
label: a label operand

For each instruction, at most one operand can be a memory operand.

3.1. Data Transfer Mnemonics

Syntax	Semantics	Description
<code>mov{1,w,b} srcIRM, destRM</code>	$dest = src;$	Move. Copy <i>src</i> to <i>dest</i> . Flags affected: None
<code>movsb{1,w} srcRM, destR</code>	$dest = src;$	Move Sign-Extended Byte. Copy byte operand <i>src</i> to word or long operand <i>dest</i> , extending the sign of <i>src</i> . Flags affected: None
<code>movswl srcRM, destR</code>	$dest = src;$	Move Sign-Extended Word. Copy word operand <i>src</i> to long operand <i>dest</i> , extending the sign of <i>src</i> . Flags affected: None
<code>movzb{1,w} srcRM, destR</code>	$dest = src;$	Move Zero-Extended Byte. Copy byte operand <i>src</i> to word or long operand <i>dest</i> , setting the high-order bytes of <i>dest</i> to 0. Flags affected: None
<code>movzwl srcRM, destR</code>	$dest = src;$	Move Zero-Extended Word. Copy word operand <i>src</i> to long operand <i>dest</i> , setting the high-order bytes of <i>dest</i> to 0. Flags affected: None
<code>push{1,w} srcIRM</code>	$reg[ESP] = reg[ESP] - \{4,2\};$ $mem[reg[ESP]] = src;$	Push. Push <i>src</i> onto the stack. Flags affected: None
<code>pop{1,w} destRM</code>	$dest = mem[reg[ESP]];$ $reg[ESP] = reg[ESP] + \{4,2\};$	Pop. Pop from the stack into <i>dest</i> . Flags affected: None
<code>lea{1,w} srcM, destR</code>	$dest = \&src;$	Load Effective Address. Assign the address of <i>src</i> to <i>dest</i> . Flags affected: None
<code>cld</code>	$reg[EDX:EAX] = reg[EAX];$	Convert Long to Double Register. Sign extend the contents of register EAX into the register pair EDX:EAX, typically in preparation for <code>divl</code> . Flags affected: None
<code>cwtd</code>	$reg[DX:AX] = reg[AX];$	Convert Word to Double Register. Sign extend the contents of register AX into the register pair DX:AX, typically in preparation for <code>divw</code> . Flags affected: None
<code>cbtw</code>	$reg[AX] = reg[AL];$	Convert Byte to Word. Sign extend the contents of register AL into register AX, typically in preparation for <code>divb</code> . Flags affected: None
<code>leave</code>	Equivalent to: <code>movl %ebp, %esp</code> <code>popl %ebp</code>	Pop a stack frame in preparation for leaving a function. Flags affected: None

3.2. Arithmetic Mnemonics

Syntax	Semantics	Description
<code>add{1,w,b} srcIRM, destRM</code>	$dest = dest + src;$	Add. Add <i>src</i> to <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>adc{1,w,b} srcIRM, destRM</code>	$dest = dest + src + C;$	Add with Carry. Add <i>src</i> and the carry flag to <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>sub{1,w,b} srcIRM, destRM</code>	$dest = dest - src;$	Subtract. Subtract <i>src</i> from <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>inc{1,w,b} destRM</code>	$dest = dest + 1;$	Increment. Increment <i>dest</i> . Flags affected: O, S, Z, A, P
<code>dec{1,w,b} destRM</code>	$dest = dest - 1;$	Decrement. Decrement <i>dest</i> . Flags affected: O, S, Z, A, P
<code>neg{1,w,b} destRM</code>	$dest = -dest;$	Negate. Negate <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>imull srcRM</code>	$reg[EDX:EAX] = reg[EAX]*src;$	Signed Multiply. Multiply the contents of register EAX by <i>src</i> , and store the product in registers EDX:EAX. Flags affected: O, S, Z, A, C, P
<code>imulw srcRM</code>	$reg[DX:AX] = reg[AX]*src;$	Signed Multiply. Multiply the contents of register AX by <i>src</i> , and store the product in registers DX:AX. Flags affected: O, S, Z, A, C, P
<code>imulb srcRM</code>	$reg[AX] = reg[AL]*src;$	Signed Multiply. Multiply the contents of register AL by <i>src</i> , and store the product in AX. Flags affected: O, S, Z, A, C, P
<code>idivl srcRM</code>	$reg[EAX] = reg[EDX:EAX]/src;$ $reg[EDX] = reg[EDX:EAX]\%src;$	Signed Divide. Divide the contents of registers EDX:EAX by <i>src</i> , and store the quotient in register EAX and the remainder in register EDX. Flags affected: O, S, Z, A, C, P
<code>idivw srcRM</code>	$reg[AX] = reg[DX:AX]/src;$ $reg[DX] = reg[DX:AX]\%src;$	Signed Divide. Divide the contents of registers DX:AX by <i>src</i> , and store the quotient in register AX and the remainder in register DX. Flags affected: O, S, Z, A, C, P
<code>idivb srcRM</code>	$reg[AL] = reg[AX]/src;$ $reg[AH] = reg[AX]\%src;$	Signed Divide. Divide the contents of register AX by <i>src</i> , and store the quotient in register AL and the remainder in register AH. Flags affected: O, S, Z, A, C, P
<code>mull srcRM</code>	$reg[EDX:EAX] = reg[EAX]*src;$	Unsigned Multiply. Multiply the contents of register EAX by <i>src</i> , and store the product in registers EDX:EAX. Flags affected: O, S, Z, A, C, P
<code>mulw srcRM</code>	$reg[DX:AX] = reg[AX]*src;$	Unsigned Multiply. Multiply the contents of register AX by <i>src</i> , and store the product in registers DX:AX. Flags affected: O, S, Z, A, C, P
<code>mulb srcRM</code>	$reg[AX] = reg[AL]*src;$	Unsigned Multiply. Multiply the contents of register AL by <i>src</i> , and store the product in AX.
<code>divl srcRM</code>	$reg[EAX] = reg[EDX:EAX]/src;$ $reg[EDX] = reg[EDX:EAX]\%src;$	Unsigned Divide. Divide the contents of registers EDX:EAX by <i>src</i> , and store the quotient in register EAX and the remainder in register EDX. Flags affected: O, S, Z, A, C, P
<code>divw srcRM</code>	$reg[AX] = reg[DX:AX]/src;$ $reg[DX] = reg[DX:AX]\%src;$	Unsigned Divide. Divide the contents of registers DX:AX by <i>src</i> , and store the quotient in register AX and the remainder in register DX. Flags affected: O, S, Z, A, C, P

<code>divb <i>srcRM</i></code>	<code>reg[AL] = reg[AX]/<i>src</i>;</code> <code>reg[AH] = reg[AX]%<i>src</i>;</code>	Unsigned Divide. Divide the contents of register AX by <i>src</i> , and store the quotient in register AL and the remainder in register AH. Flags affected: O, S, Z, A, C, P
--------------------------------	--	--

3.3. Bitwise Mnemonics

Syntax	Semantics	Description
<code>and{1,w,b} <i>srcIRM, destRM</i></code>	<code>dest = dest & <i>src</i>;</code>	And. Bitwise and <i>src</i> into <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>or{1,w,b} <i>srcIRM, destRM</i></code>	<code>dest = dest <i>src</i>;</code>	Or. Bitwise or <i>src</i> into <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>xor{1,w,b} <i>srcIRM, destRM</i></code>	<code>dest = dest ^ <i>src</i>;</code>	Exclusive Or. Bitwise exclusive or <i>src</i> into <i>dest</i> . Flags affected: O, S, Z, A, C, P
<code>not{1,w,b} <i>destRM</i></code>	<code>dest = ~<i>dest</i>;</code>	Not. Bitwise not <i>dest</i> . Flags affected: None
<code>sal{1,w,b} <i>srcIR, destRM</i></code>	<code>dest = dest << <i>src</i>;</code>	Shift Arithmetic Left. Shift <i>dest</i> to the left <i>src</i> bits, filling with zeros. Flags affected: O, S, Z, A, C, P
<code>sar{1,w,b} <i>srcIR, destRM</i></code>	<code>dest = dest >> <i>src</i>;</code>	Shift Arithmetic Right. Shift <i>dest</i> to the right <i>src</i> bits, sign extending the number. Flags affected: O, S, Z, A, C, P
<code>shl{1,w,b} <i>srcIR, destRM</i></code>	(Same as <i>sal</i>)	Shift Left. (Same as <i>sal</i>). Flags affected: O, S, Z, A, C, P
<code>shr{1,w,b} <i>srcIR, destRM</i></code>	(Same as <i>sar</i>)	Shift Right. Shift <i>dest</i> to the right <i>src</i> bits, filling with zeros. Flags affected: O, S, Z, A, C, P

3.4. Control Transfer Mnemonics

Syntax	Semantics	Description
<code>cmp{1,w,b} <i>srcIRM1,srcRM2</i></code>	<code>reg[EFLAGS] = <i>srcRM2</i> comparedWith <i>srcIRM1</i></code>	Compare. Compute <i>src2</i> - <i>src1</i> and set flags in the EFLAGS register based upon the result. Flags affected: O, S, Z, A, C, P
<code>test{1,w,b} <i>srcIRM1,srcRM2</i></code>	<code>reg[EFLAGS] = <i>srcRM2</i> andedWith <i>srcIRM1</i></code>	Test. Compute <i>src2</i> & <i>src1</i> and set flags in the EFLAGS register based upon the result. Flags affected: S, Z, P (O and C set to 0)
<code>jmp <i>label</i></code>	<code>reg[EIP] = <i>label</i>;</code>	Jump. Jump to <i>label</i> . Flags affected: None
<code>j{e,ne} <i>label</i></code>	<code>if (reg[EFLAGS] appropriate) reg[EIP] = <i>label</i>;</code>	Conditional Jump. Jump to <i>label</i> iff the flags in the EFLAGS register indicate an equality or inequality (respectively) relationship between the most recently compared numbers. Flags affected: None
<code>j{1,le,g,ge} <i>label</i></code>	<code>if (reg[EFLAGS] appropriate) reg[EIP] = <i>label</i>;</code>	Signed Conditional Jump. Jump to <i>label</i> iff the condition codes in the EFLAGS register indicate a less than, less than or equal to, greater than, or greater than or equal to (respectively) relationship between the most recently compared numbers. Flags affected: None
<code>j{b,be,a,ae} <i>label</i></code>	<code>if (reg[EFLAGS] appropriate) reg[EIP] = <i>label</i>;</code>	Unsigned Conditional Jump. Jump to <i>label</i> iff the condition codes in the EFLAGS register indicate a below, below or equal to, above, or above or equal to (respectively) relationship between the most recently compared numbers. Flags affected: None

<code>call label</code>	<code>reg[ESP] = reg[ESP] - 4;</code> <code>mem[reg[ESP]] = reg[EIP];</code> <code>reg[EIP] = label;</code>	Call. Call the function that begins at <i>label</i> . Flags affected: None
<code>call *srcR</code>	<code>reg[ESP] = reg[ESP] - 4;</code> <code>mem[reg[ESP]] = reg[EIP];</code> <code>reg[EIP] = reg[srcR];</code>	Call. Call the function whose address is in <i>src</i> . Flags affected: None
<code>ret</code>	<code>reg[EIP] = mem[reg[ESP]];</code> <code>reg[ESP] = reg[ESP] + 4;</code>	Return. Return from the current function. Flags affected: None
<code>int srcIRM</code>	Generate interrupt number <i>src</i>	Interrupt. Generate interrupt number <i>src</i> . Flags affected: None

4. Assembler Directives

Syntax	Description
<code>label:</code>	Record the fact that <i>label</i> marks the current location within the current section
<code>.section ".sectionname"</code>	Make the <i>sectionname</i> section the current section
<code>.skip n</code>	Skip <i>n</i> bytes of memory in the current section
<code>.align n</code>	Skip as many bytes of memory in the current section as necessary so the current location is evenly divisible by <i>n</i>
<code>.byte bytevalue1, bytevalue2, ...</code>	Allocate one byte of memory containing <i>bytevalue1</i> , one byte of memory containing <i>bytevalue2</i> , ... in the current section
<code>.word wordvalue1, wordvalue2, ...</code>	Allocate two bytes of memory containing <i>wordvalue1</i> , two bytes of memory containing <i>wordvalue2</i> , ... in the current section
<code>.long longvalue1, longvalue2, ...</code>	Allocate four bytes of memory containing <i>longvalue1</i> , four bytes of memory containing <i>longvalue2</i> , ... in the current section
<code>.ascii "string1", "string2", ...</code>	Allocate memory containing the characters from <i>string1</i> , <i>string2</i> , ... in the current section
<code>.asciz "string1", "string2", ...</code>	Allocate memory containing <i>string1</i> , <i>string2</i> , ..., where each string is '\0' terminated, in the current section
<code>.string "string1", "string2", ...</code>	(Same as <code>.asciz</code>)
<code>.globl label1, label2, ...</code>	Mark <i>label1</i> , <i>label2</i> , ... so they are accessible by code generated from other source code files
<code>.equ name, expr</code>	Define <i>name</i> as a symbolic alias for <i>expr</i>
<code>.lcomm label, n [,align]</code>	Allocate <i>n</i> bytes, marked by <i>label</i> , in the bss section [and align the bytes on an <i>align</i> -byte boundary]
<code>.comm label, n [,align]</code>	Allocate <i>n</i> bytes, marked by <i>label</i> , in the bss section, mark <i>label</i> so it is accessible by code generated from other source code files [and align the bytes on an <i>align</i> -byte boundary]
<code>.type label,@function</code>	Mark <i>label</i> so the linker knows that it denotes the beginning of a function

Copyright © 2009 by Robert M. Dondero, Jr.