x86-64 Programming III

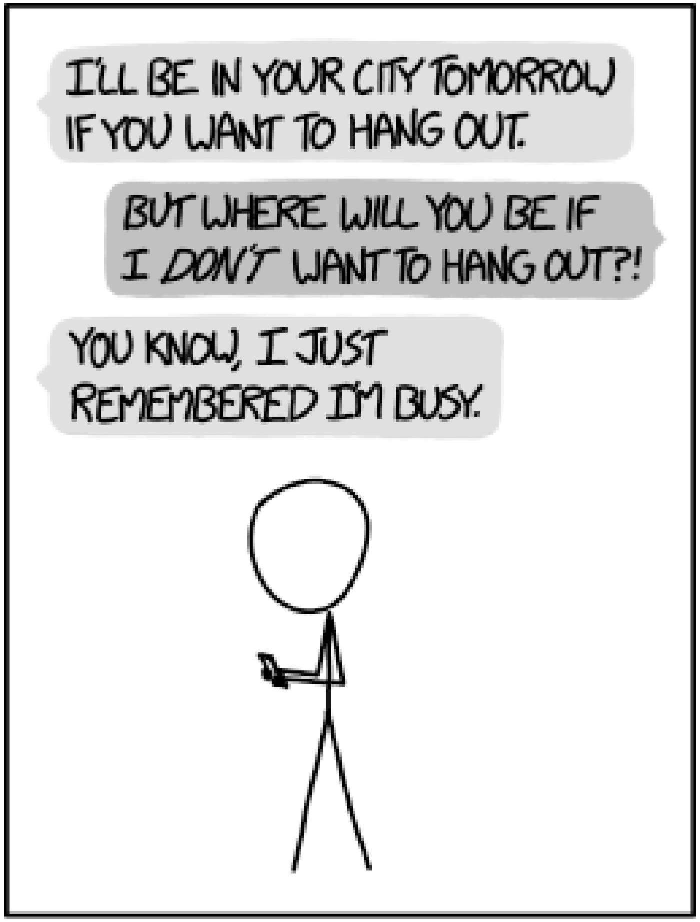
CSE 351 Autumn 2024

Instructor:

Ruth Anderson

Teaching Assistants:

Alexandra Michael
Connie Chen
Chloe Fong
Chendur Jayavelu
Joshua Tan
Nikolas McNamee
Nahush Shrivatsa
Naama Amiel
Neela Kausik
Renee Ruan
Rubee Zhao
Samantha Dreussi
Sean Siddens
Waleed Yagoub



WHY I TRY NOT TO BE PEDANTIC ABOUT CONDITIONALS.

http://xkcd.com/1652/

Relevant Course Information

- HW7 due TONIGHT, Monday (10/14) @ 11:59 pm
- Lab 1b, due TONIGHT, Monday (10/14) @ 11:59 pm
  - Submit `aisle_manager.c`, `store_client.c`, and `lab1Bsynthesis.txt`
  - Submissions that fail the autograder get a **ZERO**
    - No excuses – make full use of tools & Gradescope's interface
- HW8 due Wednesday (10/16) @ 11:59 pm
- Lab 2 (x86-64) due next Friday (10/25)
  - coming soon!
  - Learn to read x86-64 assembly and use GDB

Move extension: `movz` and `movs`

2 width specifiers: b, w, l, q
1 2 4 8 bytes

`movz_ _ src, regDest` *# Move with zero extension*

`movs_ _ src, regDest` *# Move with sign extension*

- Copy from a *smaller* source value to a *larger* destination
- Source can be memory or register; Destination *must* be a register
- Fill remaining bits of dest with **zero** (`movz`) or **sign bit** (`movs`)

`movz`*SD* / **`movs`*SD*:**

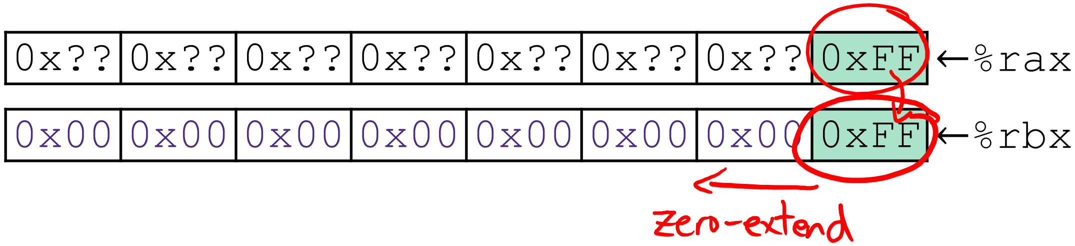
S – size of source (**`b`** = 1 byte, **`w`** = 2)

D – size of dest (**`w`** = 2 bytes, **`l`** = 4, **`q`** = 8)

Example:

`movzbq %al, %rbx`

zero-extend 1 byte 8 bytes



0x??	0x??	0x??	0x??	0x??	0x??	0x??	0xFF	←%rax
0x00	0x00	0x00	0x00	0x00	0x00	0x00	0xFF	←%rbx

zero-extend

Move extension: `movz` and `movs`

`movz__` *src, regDest* *# Move with zero extension*

`movs__` *src, regDest* *# Move with sign extension*

- Copy from a *smaller* source value to a *larger* destination
- Source can be memory or register; Destination *must* be a register
- Fill remaining bits of dest with **zero** (`movz`) or **sign bit** (`movs`)

`movzSD` / **`movsSD`**:

S – size of source (**b** = 1 byte, **w** = 2)

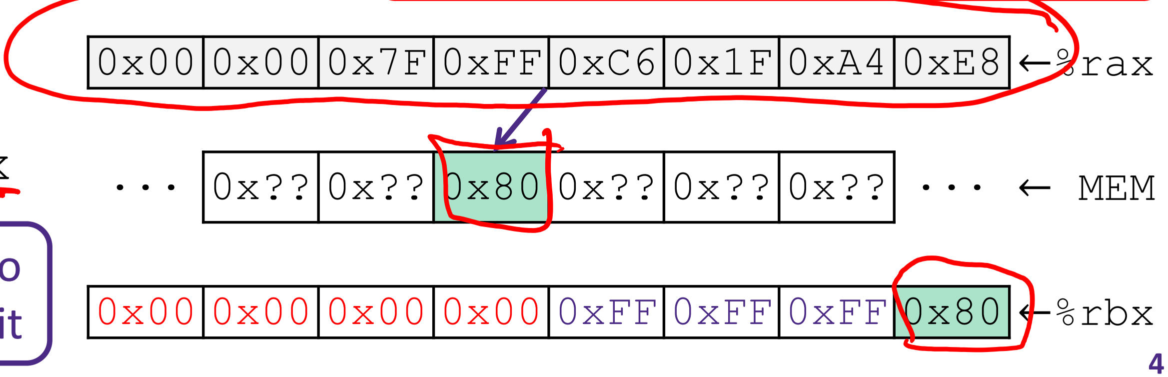
D – size of dest (**w** = 2 bytes, **l** = 4, **q** = 8)

Note: In x86-64, *any instruction* that generates a 32-bit (long word) value for a register also sets the high-order portion of the register to 0. Good example on p. 184 in the textbook.

Example:

`movsbl (%rax), %ebx`

Copy 1 byte from memory into 8-byte register & sign extend it


0x00 0x00 0x7F 0xFF 0xC6 0x1F 0xA4 0xE8 ←%rax

... 0x?? 0x?? 0x80 0x?? 0x?? 0x?? ... ← MEM

0x00 0x00 0x00 0x00 0xFF 0xFF 0xFF 0x80 ←%rbx

Review Question

%si

0. . . . . 0 FF FE

- If `%rsi` is `0x B0BACAFE ~~1EE7~~ F0 0D`, what is its value after executing: 2byte 4byte

%esi

```
movswl %si, %esi?
```

x86 Control Flow

- **Condition codes**
- **Conditional and unconditional branches**
- Loops
- Switches

Conditionals and Control Flow

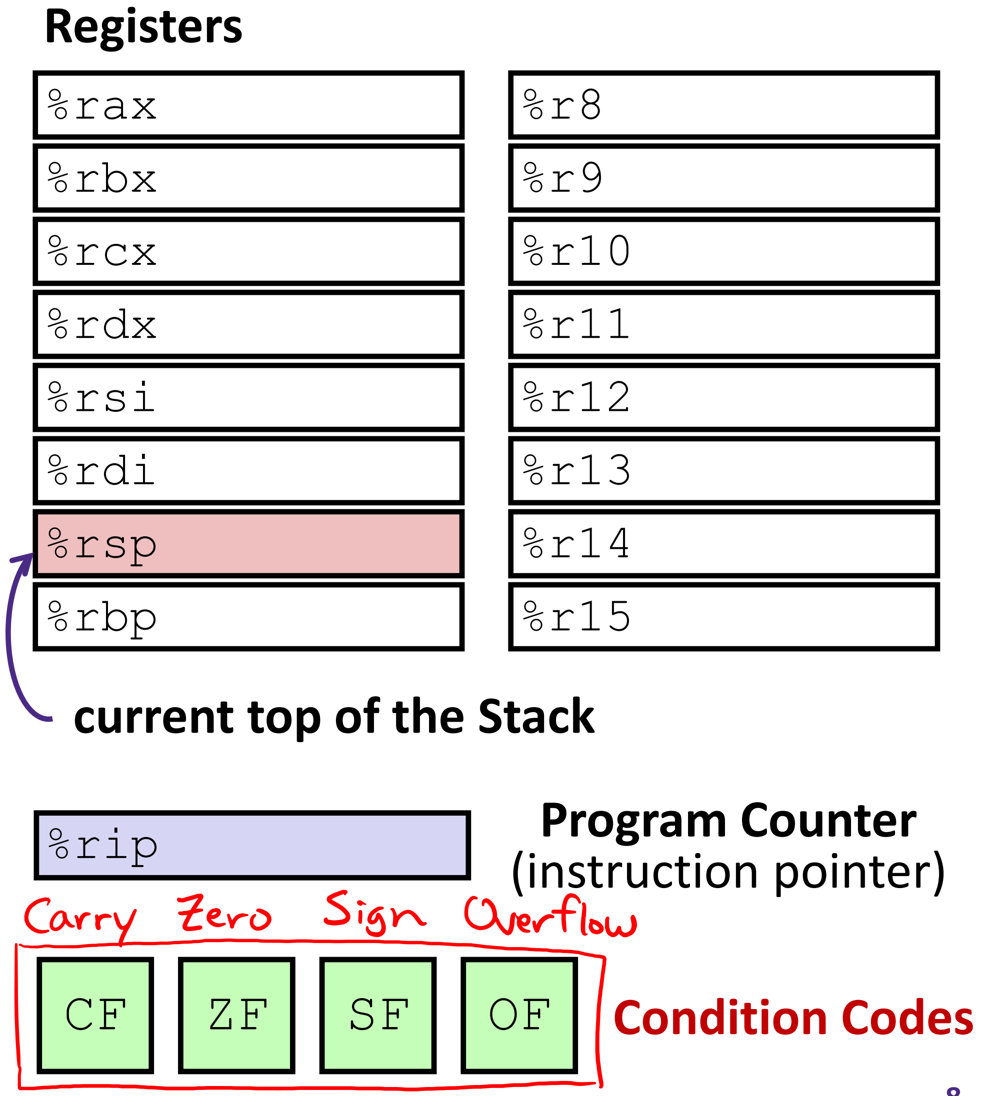
- Conditional branch/*jump*
  - Jump to somewhere else if some condition is true, otherwise execute next instruction
- Unconditional branch/*jump*
  - Always jump when you get to this instruction

- Together, they can implement most control flow constructs in high-level languages:
  - `if (condition) then {…} else {…}`
  - `while (condition) {…}`
  - `do {…} while (condition)`
  - `for (initialization; condition; iterative) {…}`
  - `switch {…}`

How to check conditions and implement?!

Processor State (x86-64, partial)

- Information about currently executing program
  - Temporary data (`%rax`, …)
  - Location of runtime stack (`%rsp`)
  - Location of current code control point (`%rip`, …)
  - Status of recent tests (**CF**, **ZF**, **SF**, **OF**) "flags"
    - Single bit registers:



Registers

`%rax`	`%r8`
`%rbx`	`%r9`
`%rcx`	`%r10`
`%rdx`	`%r11`
`%rsi`	`%r12`
`%rdi`	`%r13`
`%rsp`	`%r14`
`%rbp`	`%r15`

current top of the Stack

`%rip`

Program Counter
(instruction pointer)

Carry Zero Sign Overflow

CF	ZF	SF	OF

Condition Codes

4 bits

signed: -8 . . . 7

unsigned: 0 ⟶ 15

Condition Codes

CF : 1

carry out

$$\begin{array}{r} 1011 \\ +\,0110 \\ \hline \boxed{1}\,\underbrace{0001} \end{array} \qquad \begin{array}{r} \text{unsigned} \\ 11 \\ 6 \\ \hline 1 \end{array}$$

CF *Carry Flag* **ZF** *Zero Flag* **SF** *Sign Flag* **OF** *Overflow Flag*

- Carry Flag (CF): Set to 1 if most recent op result *carried out* data which couldn't be stored; i.e. unsigned overflow (usually when *dest* < *src*)
- Zero Flag (ZF): Set to 1 if most recent op result computed to `0`
- Sign Flag (SF): Set to 1 if most recent op result is a signed (negative) value i.e. MSB produced is 1
- Overflow Flag (OF): Similar as carry flag, but applies to signed overflow i.e. if MSBs were both `0`, and now result MSB is 1, or vice versa

$$\begin{array}{r} 0111 \\ +\,0011 \\ \hline 1010 \end{array} \qquad \begin{array}{r} \text{signed} \\ 7 \\ 3 \\ \hline -6 \end{array}$$

$\oplus + \oplus = \ominus$ OF : 1

Use flag values to decide whether to jump: How do we set them?

Setting Condition Codes: Implicit Setting

- Implicitly set by **arithmetic** + logical operations: a fun side effect!
  - Example: `addq src, dst ↔ r = d+s`
  - **`CF=1`** if carry out from MSB (*unsigned* overflow)
  - **`ZF=1`** if `r==0`
  - **`SF=1`** if `r<0` (if MSB is 1)
  - **`OF=1`** if *signed* overflow

`(s>0 && d>0 && r<0)||(s<0 && d<0 && r>=0)`

⊕ ⊕ → ⊖ ⊖ ⊖ → ⊕

Not set by `lea` instruction 🙄

Suppose we only want to set the flags but not save the result…

CF *Carry Flag* ZF *Zero Flag* SF *Sign Flag* OF *Overflow Flag*

Setting Condition Codes: Explicit Setting with `cmp`

- Explicitly set by the **Compare** instruction
  - **`cmpq`** $\overset{a}{\texttt{src1}}$, $\overset{b}{\texttt{src2}}$ ↔ sets flags based on `b-a`

    Kind of like **`subq`** $\underset{b-a}{\texttt{a, b}}$ but doesn't store result anywhere
  - **`CF=1`** if carry out from MSB (good for *unsigned* comparison)
  - **`ZF=1`** if `a==b`, because `b-a==0`!
  - **`SF=1`** if `(b-a)<0` (if MSB is 1)
  - **`OF=1`** if *signed* overflow

    `(a>0 && b<0 && (b-a)>0) || (a<0 && b>0 && (b-a)<0)`

$\ominus - \oplus \longrightarrow \oplus$ $\oplus - \ominus \longrightarrow \ominus$

CF *Carry Flag* ZF *Zero Flag* SF *Sign Flag* OF *Overflow Flag*

Setting Condition Codes: Explicit Setting with `test`

- Explicitly set by **Test** instruction
  - **`testq`** `src2, src1` ↔ sets flags based on `a&b`

    Kind of like **`andq`** `a, b` but doesn't store result anywhere

    Tip: Useful to have one of the operands be a mask

  - Can't have carry out (**`CF`**) or overflow (**`OF`**)—why?
  - **`ZF=1`** if `a&b==0`
  - **`SF=1`** if `a&b<0` (signed)

Just flipping bits!

`CF`	*Carry Flag*	`ZF`	*Zero Flag*	`SF`	*Sign Flag*	`OF`	*Overflow Flag*

Example Condition Code Setting

- Assuming that `%al` = `0x80` and `%bl` = `0x81`, which flags (CF, ZF, SF, OF) are set when we execute:

a b

`cmpb %al, %bl` → %bl - %al

0x81 - 0x80

↓ ↓

(-127) - (-128)

-127 + 128

1

1 111 1 1 1 1

%bl → 0b 1000 0001

~%al 0b 0111 1111

+1 +0b 0000 0001

(1) 0000 0001

CF: 1 ZF: 0 SF: 0 OF: 0

Using Condition Codes: Jumping

- `j*` Instructions
  - Jumps to ***target*** (an address) based on condition codes

don't worry about the details

(always compared to 0)

Instruction	Condition	Description
`jmp` *target*	`1`	Unconditional
`je` *target*	`ZF`	Equal / Zero
`jne` *target*	`~ZF`	Not Equal / Not Zero
`js` *target*	`SF`	Negative
`jns` *target*	`~SF`	Nonnegative
`jg` *target*	`~(SF^OF)&~ZF`	Greater (Signed)
`jge` *target*	`~(SF^OF)`	Greater or Equal (Signed)
`jl` *target*	`(SF^OF)`	Less (Signed)
`jle` *target*	`(SF^OF)|ZF`	Less or Equal (Signed)
`ja` *target*	`~CF&~ZF`	Above (unsigned ">")
`jb` *target*	`CF`	Below (unsigned "<")

Note: We can't define our own **`j*`** instructions. But we can simulate customizing one by "saving" flags for a compound conditional, and jumping based on that…

Use set!

Using Condition Codes: Setting

- `set*` Instructions
  - Set low-order byte of `dst` to 0 or 1 based on condition codes
  - Does not alter remaining 7 bytes

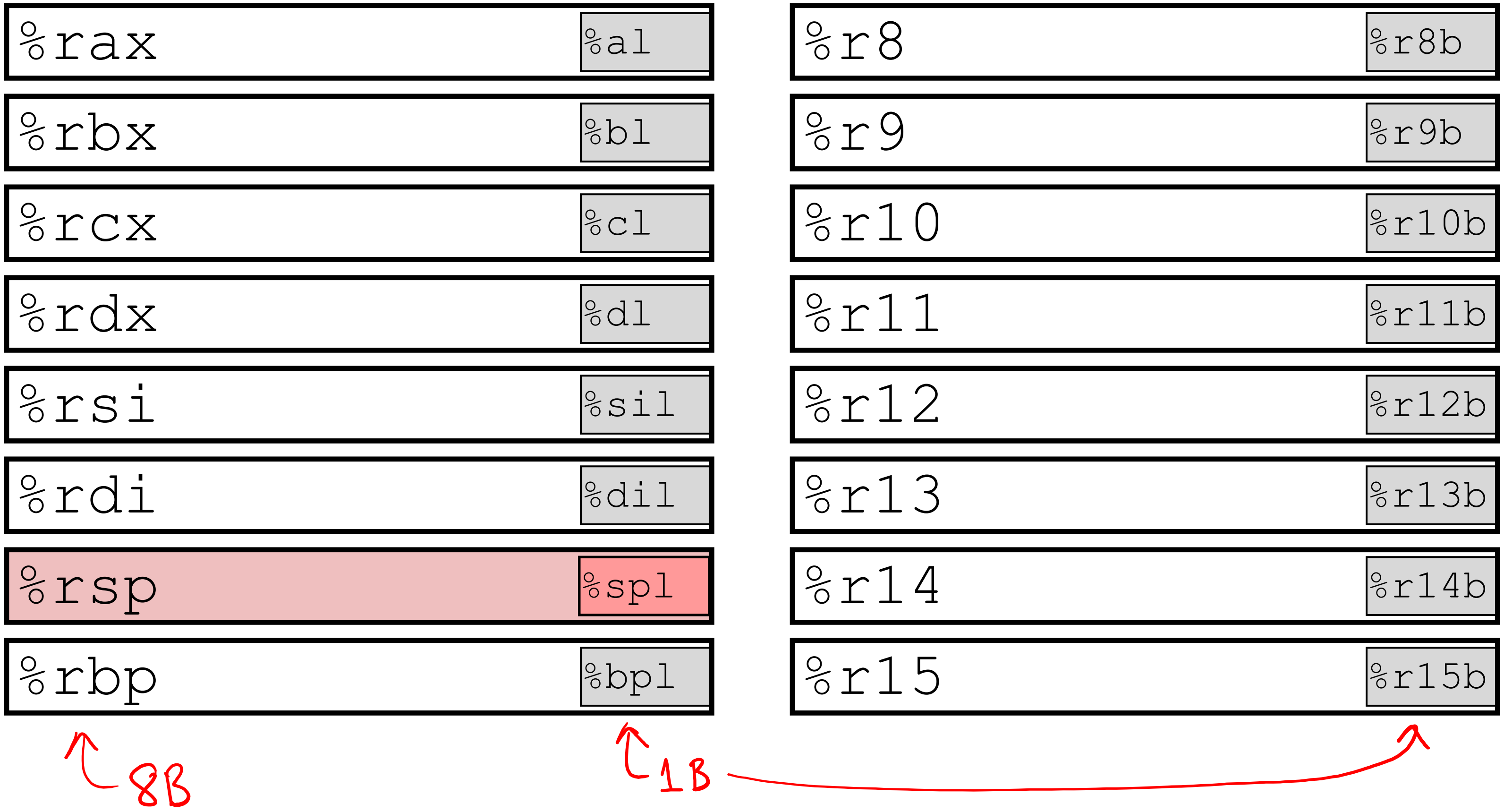
False → 0b 0000 0000 = 0x00
True → 0b 0000 0001 = 0x01

Same instruction suffixes as j* instructions!

Instruction	Condition	Description
`sete` *dst*	`ZF`	Equal / Zero
`setne` *dst*	`~ZF`	Not Equal / Not Zero
`sets` *dst*	`SF`	Negative
`setns` *dst*	`~SF`	Nonnegative
`setg` *dst*	`~(SF^OF)&~ZF`	Greater (Signed)
`setge` *dst*	`~(SF^OF)`	Greater or Equal (Signed)
`setl` *dst*	`(SF^OF)`	Less (Signed)
`setle` *dst*	`(SF^OF)|ZF`	Less or Equal (Signed)
`seta` *dst*	`~CF&~ZF`	Above (unsigned “>”)
`setb` *dst*	`CF`	Below (unsigned “<”)

Reminder: x86-64 Integer Registers

- Accessing the low-order byte:



%rax	%al	%r8	%r8b
%rbx	%bl	%r9	%r9b
%rcx	%cl	%r10	%r10b
%rdx	%dl	%r11	%r11b
%rsi	%sil	%r12	%r12b
%rdi	%dil	%r13	%r13b
%rsp	%spl	%r14	%r14b
%rbp	%bpl	%r15	%r15b

8B

1B

Reading Condition Codes

%eax

rax | 0 0 | 00 | 00 | 00 | 00 | 00 | 00 | |

%al

Register	Use(s)
`%rdi`	1st argument (`x`)
`%rsi`	2nd argument (`y`)
`%rax`	return value

- `set*` Instructions
  - Set a low-order byte to 0 or 1 based on condition codes
  - Operand is byte register (e.g., `%al`) or a byte in memory
  - Do not alter remaining bytes in register
    - Typically use `movzbl` (zero-extended `mov`) to "finish the job"

rdi rsi

```
int gt(long x, long y)
{
   return x > y;
}
```

rdi rsi

y x

```
cmpq    %rsi, %rdi    #
setg    %al           #
movzbl  %al, %eax     #
ret
```

$x - y \overset{?}{>} 0$

$x \overset{?}{>} y$

Reading Condition Codes

Register	Use(s)
`%rdi`	1st argument (`x`)
`%rsi`	2nd argument (`y`)
`%rax`	return value

- `set*` Instructions
  - Set a low-order byte to 0 or 1 based on condition codes
  - Operand is byte register (e.g., `%al`) or a byte in memory
  - Do not alter remaining bytes in register
    - Typically use `movzbl` (zero-extended `mov`) to "finish the job"

```
int gt(long x, long y)
{
  return x > y;
}
```

```
cmpq   %rsi, %rdi     # Compare x:y
setg   %al            # Set when >
movzbl %al, %eax      # Zero rest of %rax
ret
```

Choosing instructions for conditionals

- All arithmetic instructions set condition flags based on result of operation (`op`)
  - Conditionals are comparisons against 0
- Come in instruction *pairs*: ***first set flags, then jump!***

```
         addq 5, (p)
je:      *p+5 == 0
jne:     *p+5 != 0
jg:      *p+5 >  0
jl:      *p+5 <  0
```

```
         orq a, b
je:      b|a == 0
jne:     b|a != 0
jg:      b|a >  0
jl:      b|a <  0
```

		(op) s, d
`je`	"Equal"	`d (op) s == 0`
`jne`	"Not equal"	`d (op) s != 0`
`js`	"Sign" (negative)	`d (op) s < 0`
`jns`	(non-negative)	`d (op) s >= 0`
`jg`	"Greater"	`d (op) s > 0`
`jge`	"Greater or equal"	`d (op) s >= 0`
`jl`	"Less"	`d (op) s < 0`
`jle`	"Less or equal"	`d (op) s <= 0`
`ja`	"Above" (unsigned >)	`d (op) s > 0U`
`jb`	"Below" (unsigned <)	`d (op) s < 0U`

Choosing instructions for conditionals

?

$b-a \overset{?}{\geq} 0 \Rightarrow b \geq a$

- Reminder: `cmp` is like `sub`, `test` is like `and`
  - Result is not stored anywhere

		`cmp a,b`	**`test a,b`**
`je`	"Equal"	`b == a`	`b&a == 0`
`jne`	"Not equal"	`b != a`	`b&a != 0`
`js`	"Sign" (negative)	`b-a < 0`	`b&a < 0`
`jns`	(non-negative)	`b-a >=0`	`b&a >= 0`
`jg`	"Greater"	`b > a`	`b&a > 0`
`jge`	"Greater or equal"	`b >= a`	`b&a >= 0`
`jl`	"Less"	`b < a`	`b&a < 0`
`jle`	"Less or equal"	`b <= a`	`b&a <= 0`
`ja`	"Above" (unsigned >)	`b-a > 0U`	`b&a > 0U`
`jb`	"Below" (unsigned <)	`b-a < 0U`	`b&a < 0U`

	`cmpq` `5, (p)`
`je:`	`*p == 5`
`jne:`	`*p != 5`
`jg:`	`*p > 5`
`jl:`	`*p < 5`

	`testq` `a, a`
`je:`	`a == 0`
`jne:`	`a != 0`
`jg:`	`a > 0`
`jl:`	`a < 0`

	`testb` `a, 0x1`
`je:`	a_{LSB} `== 0`
`jne:`	a_{LSB} `== 1`

Choosing instructions for conditionals

$x \overset{?}{<} 3$

$x-3 \overset{?}{<} 0$

		`cmp a,b`	`test a,b`
`je`	“Equal”	`b == a`	`b&a == 0`
`jne`	“Not equal”	`b != a`	`b&a != 0`
`js`	“Sign” (negative)	`b-a < 0`	`b&a < 0`
`jns`	(non-negative)	`b-a >=0`	`b&a >= 0`
`jg`	“Greater”	`b > a`	`b&a > 0`
`jge`	“Greater or equal”	`b >= a`	`b&a >= 0`
`jl`	“Less”	`b < a`	`b&a < 0`
`jle`	”Less or equal”	`b <= a`	`b&a <= 0`
`ja`	“Above” (unsigned >)	`b > a`	`b&a > 0U`
`jb`	“Below” (unsigned <)	`b < a`	`b&a < 0U`

Register	Use(s)
`%rdi`	argument `x`
`%rsi`	argument `y`
`%rax`	return value

```
if (x < 3) {
  return 1;
}
return 2;
```

```
  cmpq $3, %rdi
  jge T2
T1: # x < 3:
  movq $1, %rax
  ret
T2: # !(x < 3):
  movq $2, %rax
  ret
```

x

if $(x-3 \geq 0)$

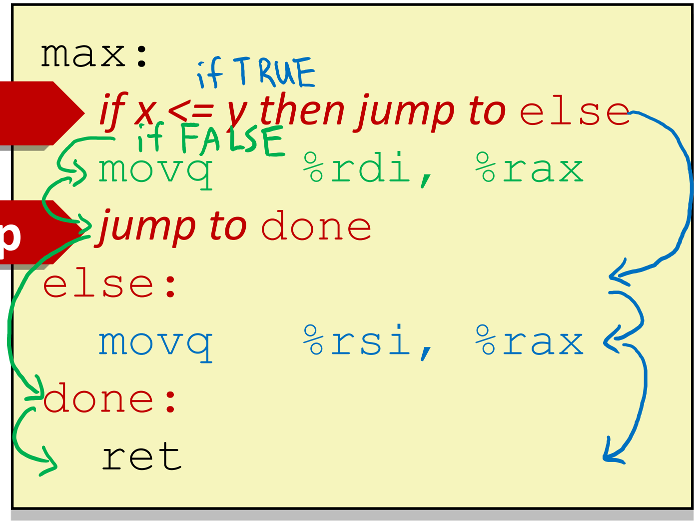
Control Flow

Register	Use(s)
`%rdi`	1st argument (`x`)
`%rsi`	2nd argument (`y`)
`%rax`	return value

```
long max(long x, long y)
{
  long max;
  if (x > y) {
    max = x;
  } else {
    max = y;
  }
  return max;
}
```

Conditional jump

Unconditional jump



```
max:
   if x <= y then jump to else
   movq    %rdi, %rax
   jump to done
else:
   movq    %rsi, %rax
done:
   ret
```

Practice Question 1

Register	Use(s)
`%rdi`	1st argument (`x`)
`%rsi`	2nd argument (`y`)
`%rax`	return value

```
long absdiff(long x, long y)
{
   long result;
   if (x > y)
      result = x-y;
   else // x ≤ y
      result = y-x;
   return result;
}
```

$x \overset{?}{>} y$

$x-y \overset{?}{>} 0$

← Jump here if x ≤ y

```
absdiff:

    ______________________

    ______________________
                                # x > y:
    movq    %rdi, %rax
    subq    %rsi, %rax          rax: x-y
    ret
.L4:                            # x <= y:
    movq    %rsi, %rax
    subq    %rdi, %rax          rax: y-x
    ret
```

[✓ **A.**] `cmpq %rsi, %rdi` (y, x)
`jle .L4`

$x-y \overset{?}{\le} 0$

B. `cmpq %rsi, %rdi` (y, x)
`jg .L4`

$x-y \overset{?}{>} 0$

~~**C.**~~ `testq %rsi, %rdi`
`jle .L4`

~~**D.**~~ `testq %rsi, %rdi`
`jg .L4`

E. We're lost…

Labels

```
swap:
    movq   (%rdi), %rax
    movq   (%rsi), %rdx
    movq   %rdx, (%rdi)
    movq   %rax, (%rsi)
    ret
```

```
max:
    movq %rdi, %rax
    cmpq %rsi, %rdi
    jg   done
    movq %rsi, %rax
done:
    ret
```

- A jump changes the program counter (`%rip`)
  - `%rip` tells the CPU the *address* of the next instruction to execute
- **Labels** give us a way to refer to a specific instruction in our assembly/machine code
  - Associated with the *next* instruction found in the assembly code (ignores whitespace)
  - Each ***use*** of the label will eventually be replaced with something that indicates the final address of the instruction that it is associated with

Summary

- Control flow in x86 determined by Condition Codes
  - Showed **C**arry, **Z**ero, **S**ign, and **O**verflow, though others exist
  - Set flags with arithmetic instructions (implicit) or Compare and Test (explicit)
  - Set instructions read out flag values
  - Jump instructions use flag values to determine next instruction to execute
  - Most control flow constructs (*e.g.*, if-else, for-loop, while-loop) can be implemented in assembly using combinations of conditional and unconditional jumps