

x86-64 Assembly

debugging!

CS 2130: Computer Systems and Organization 1
March 11, 2026

Announcements

- Homework 5 **due Monday at 11:59pm** on Gradescope
- Prof Hott office hour updates!
 - Rice 401 (no longer in 210)
 - Tuesdays 9-10am (earlier!)
 - This week only: No Weds hours, Thurs 10-11am

AT&T x86-84 Assembly

instruction source, destination

- Instruction followed by 0 or more operands (arguments)
- 4 types of operands:
 - Number (immediate value): `$0x123`
 - Register: `%rax`
 - Address of memory: `(%rax)` or 24 or `labelname`
 - Value at an address in memory: `(%rax)` or 24 or `labelname`

lea

Instructions

Instructions have different versions depending on number of bits to use

- `movq` - 64-bit move
 - q = quad word
- `movl` - 32-bit move
 - l = long
- There are encodings for shorter things, but we will mostly see 32- and 64-bit

More powerful than our ISA

Instructions can move/operate between memory and register

- `movq %rax, %rcx` - register to register
 - Remember our icode 0
- `movq (%rax), %rcx` - memory to register
 - Remember our icode 3
- `movq %rax, (%rcx)` - register to memory
 - Remember our icode 4
- `movq $21, %rax` - Immediate to register
 - Remember our icode 6 (b=0)

Note: at most one memory address per instruction

Other Instructions

Other instructions work the same way

- `addq %rax, %rcx` — `rcx += rax`
- `subq (%rbx), %rax` — `rax -= M[rbx]`
- `xor`, `and`, and others work the same way!
- Assembly has virtually no 3-argument instructions
 - All will be modifying something (i.e., `+=`, `&=`, ...)

Load Effective Address

Load effective address: `leaq 4(%rcx), %rax`

- Performs memory address calculation
- Stores address, not value at the address in memory

*addq
movq 4(%rcx), %rax*

Jumps

`jmp foo`

- Unconditional jump to `foo`
- `foo` is a label or memory address
- Need `jmp*` to use register value

Conditional jumps

<code>jnl</code>	<code>jle</code>	<code>je</code>	<code>jne</code>	<code>jg</code>	<code>jge</code>	<code>ja</code>	<code>jb</code>	<code>js</code>	<code>jo</code>
$<$	$<=$	$=$	\neq	$>$	$>=$	$>$	$<$	sign	overflow

unsigned

Unlike our Toy ISA, these do not compare given register to 0

Jumps

Condition codes - 4 1-bit registers set by every math operation, `cmp`, and `test`

- Result for the operation compared to 0 (if no overflow)

• Example:

rax += -5 ⇒ 0

`addq $-5, %rax`

`// ...code that doesn't set condition codes...`

`je foo`

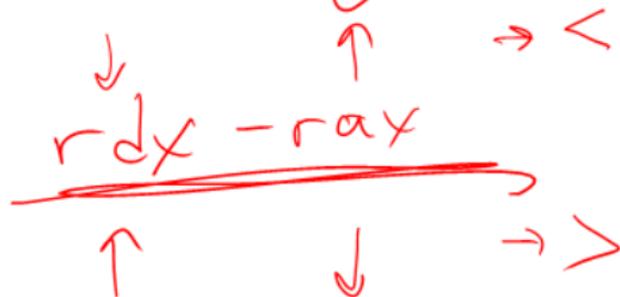
- Sets condition codes from doing math (subtract 5 from rax)
- Tells whether result was positive, negative, 0, if there was overflow, ...
- Then jump if the result of operation should have been = 0

Jumps: compare...

$\text{cmpq } \overset{\text{src}}{\text{\%rax}}, \overset{\text{dest}}{\text{\%rdx}}$

- Compare checks result of -- and sets condition codes
- How $\text{rdx} - \text{rax}$ compares with 0
- Be aware of ordering!
 - if rax is bigger, sets $<$ flag
 - if rdx is bigger, sets $>$ flag

$\text{rdx} - = \text{rax}$



Jumps: ... and test

```
testq %rax, %rdx
```

- Sets the condition codes based on `rdx` & `rax`
- Less common

Neither save their result, just set condition codes!

Example: Loops

```
while (i < 42)
    i += 1
```

Functions

```
f(x,y):  
    ...  
    ...  
    return 4
```

```
...  
z = f(2,5)
```

Function Calls: Calling Conventions

`callq myfun`

- Push return address, then jump to `myfun`
- Convention: Store arguments in registers and stack before call
 - First 6 arguments (in order): `rdi`, `rsi`, `rdx`, `rcx`, `r8`, `r9`
 - If more arguments, pushed onto stack (last to first)

`retq`

- Pop return address from stack and jump back
- Convention: store return value in `rax` before calling `retq`

This is similar to our Toy ISA's function calls in homework 4

Calling Conventions: Registers

Calling conventions - recommendations for making function calls

- Where to put arguments/parameters for the function call?
- Where to put return value? in `rax` before calling `retq`
- What happens to values in the registers?
 - **Callee-save** - The function should ensure the values in these registers are unchanged when the function returns
 - * `rbx, rsp, rbp, r12, r13, r14, r15`
 - **Caller-save** - Before making a function call, save the value, since the function may change it

Most Common Instructions

- `mov` - =
- `lea` - load effective address
- `call` - push PC and jump to address
- `add` - +=
- `cmp` - set flags as if performing subtract
- `jmp` - unconditional jump
- `test` - set flags as if performing &
- `je` - jump iff flags indicate == 0
- `pop` - pop value from stack
- `push` - push value onto stack
- `ret` - pop PC from the stack