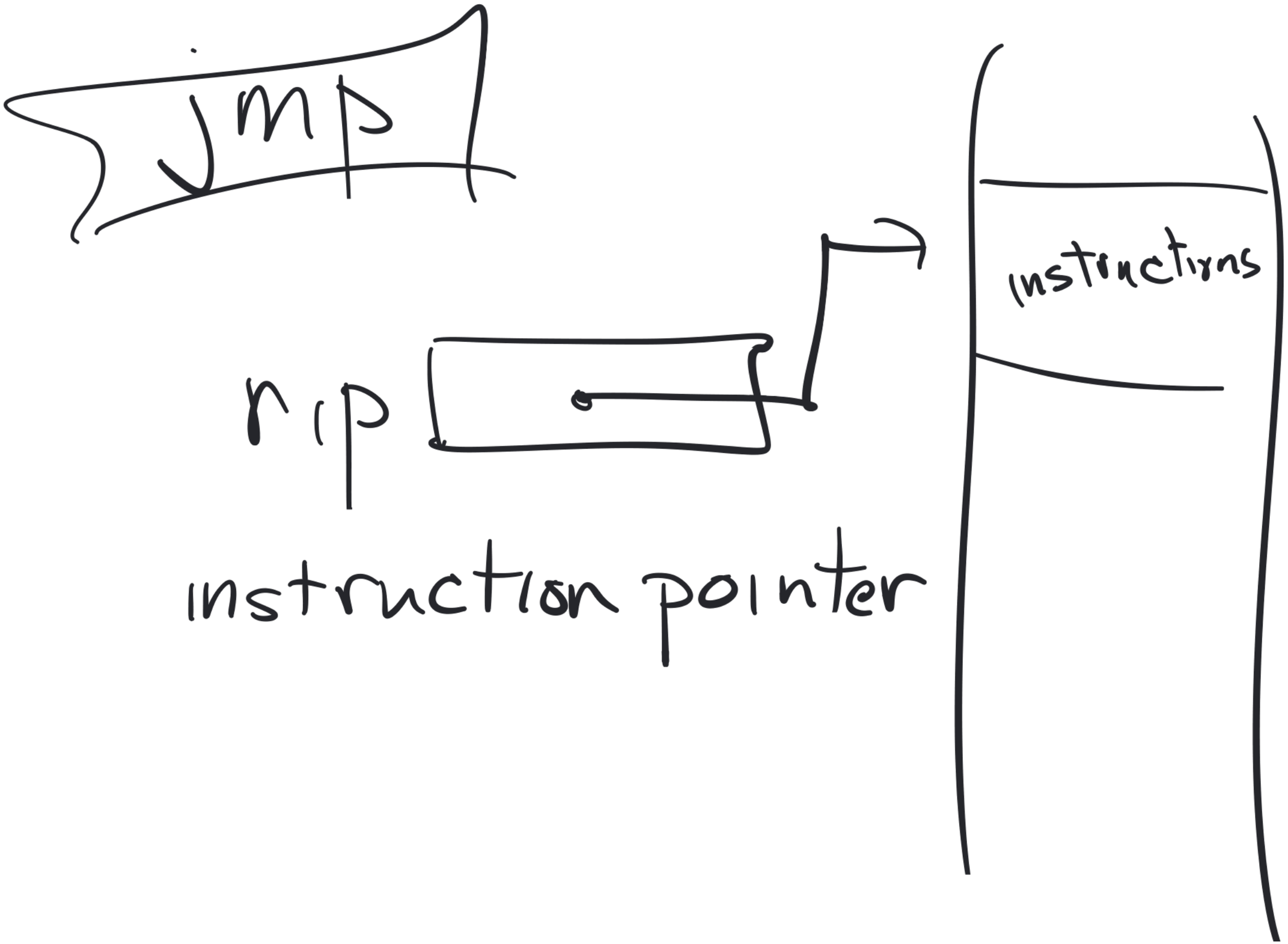
CS208

Fri, 5 May 2023


jmp
rip
instruction pointer
instructions

jmp changes the value of rip

jmpq 0x400000(,%rax,8)

destination address

0x400000 + %rax*8

lea vs. mov

lea: compntes some number + puts it in its destination

mov: copies data from here to there

Addressing Modes: indirect with offset

```
lea 0x8(%rsp), %rbx
```

rbx = 0x8 + rsp

```
mov 0x8(%rsp), %rbx
```

- go to mem. addr 8+rsp
- get the 8-byte block there
- put it in rbx

Function calling

Caller (eg. phase4)
Function (eg. fun4)

Caller:
- set up parameter(s)
- callq
  1. push rip
  2. jmp function

Function:
- make space for local vars on stack
- save old values of registers that caller might be using

How does function know where to return to?

func4(6, user's 2nd #)

Function returning

- Tear down stack
  - add some val
    to rsp
- Restore saved registers ← pop
- Pop return address
  & jmp there
  (modifies rsp & rip)
  } ← retq