Logic Structures in Assembly Language

Anonymous

Peking University

2021

Logic Structures in Assembly Language

Anonymous

Commands

Program Counter Condition Codes

Compare

Test

Conditions

...

Jumps

Jump Tables

Conditiona

Conditional Jump

Conditional Moves

Logic Structures

Conditional Branches (if) Loops (for, while)

witch Statemen

Outline

Commands

Program Counter

Condition Codes

Compare

Test

Conditions

Set

Jumps

Jump Tables

Conditional Commands

Conditional Jumps

Conditional Moves

Logic Structures

Conditional Branches (if)

Loops (for, while)

Switch Statements (switch)

Exercises

Logic Structures in Assembly Language

Anonymous

4 ロ ト 4 倒 ト 4 亘 ト 亘 め 9 0 0

Basic Assembly Commands

In Lesson 5, we learnt a bunch of new features, syntax and commands. Now let's take a little time to go over them once again.

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte

Test

Conditions

Cat

Jumps

Jump Tables

Conditional

Conditional Jump

Conditional Woves

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

▶ Definition: A register storing the address of the next command.

Logic Structures in Assembly Language

Anonymous

- Definition: A register storing the address of the next command.
- Only an abstract concept; Has different implementations, like %rip(RIP) in x86.

Logic Structures in Assembly Language

Anonymous

- Definition: A register storing the address of the next command.
- Only an abstract concept; Has different implementations, like %rip(RIP) in x86.
- Cannot be directly written (read-only).

Logic Structures in Assembly Language

Anonymous

- Definition: A register storing the address of the next command.
- Only an abstract concept; Has different implementations, like %rip(RIP) in x86.
- Cannot be directly written (read-only).

Remark

Can be used to access data stored in memory with relative address difference.

Example movq 8(%rip) %rax

Logic Structures in Assembly Language

Anonymous

Condition Codes

► Synonym: State Flag

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte

Condition Codes

Compare

Compare

Conditions

...

Jumps

Jump Tables

Conditional

Conditional Jumps

. . .

Conditional Broaders

.oops (for, while)

E.....

Condition Codes

► Synonym: State Flag

► Four Condition Codes:

rour '	Condition Codes:	
	Full Name	Meaning
CF	Carry Flag	unsigned overflow
ZF	Zero Flag	zero
SF	Sign Flag	negative result
OF	Overflow Flag	signed overflow

Logic Structures in Assembly Language

Anonymous

ommands

Program Counter

Condition Codes

Condition Code

ompare

Test

Conditions

Jumps

Jump Tables

Conditiona

Conditional Jumps

Londitional Moves

Logic Structures

Conditional Branches (if)
Loops (for, while)

Condition Codes

► Synonym: State Flag

► Four Condition Codes:

	Full Name	Meaning
CF	Carry Flag	unsigned overflow
ZF	Zero Flag	zero
SF	Sign Flag	negative result
OF	Overflow Flag	signed overflow

 Programmers should know which sort of (signed, unsigned) data they are dealing with. No checker inside CPU. Logic Structures in Assembly Language

Anonymous

ommands

Program Counter

Condition Codes

Compar Test

Conditions

Set

Jump Tables

Conditional

Conditional Jumps Conditional Moves

ogic Structures

Conditional Branches (if) Loops (for, while)

Evercises

The state of condition code depends on the result of the last arithmetic command.

Logic Structures in Assembly Language

Anonymous

ommands

Program Counte

Condition Codes

Compar

Conditions

Jet.

Jump Tables

Condition

ommands

onditional Jumps

ogic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Language Anonymous

Logic Structures in

Assembly

Condition Codes

The state of condition code depends on the result of the last arithmetic command.

Example

Suppose all the flags are 0 at first, doing sub %rax %rax mov %rbx %rax only changes ZF to be 1.

The state of condition code depends on the result of the last arithmetic command.

Example

Suppose all the flags are 0 at first, doing sub %rax %rax mov %rbx %rax only changes ZF to be 1.

Remark

leag doesn't change the condition code.

Logic Structures in Assembly Language

Anonymous

Condition Codes

Logic Structures in Assembly Language

Anonymous

ommands

rogram Counter

Condition Codes

Compare

Condition

Conditions

Jumps

Jump Tables

Conditiona

Commands
Conditional Jumi

Conditional Mov

ogic Structures

Conditional Branches (if

Loops (for, while) Switch Statements (switch

Exercise

The state of condition code depends on the result of the last arithmetic command.

Example

Suppose all the flags are 0 at first, doing sub %rax %rax mov %rbx %rax only changes ZF to be 1.

Remark

leaq doesn't change the condition code.

Remark

inc and dec set OF and ZF flags, but leave CF untouched.

Compare

There are two commands designed explicitly for setting the condition code: cmp (compare) and test.

definition

cmpX S2 S1 ($X \in \{b, w, l, q\}$): Do S1 - S2 without storing the result.

Logic Structures in Assembly Language

Anonymous

ommands

Program Counte Condition Codes

Compare

Test

Conditions

Set

Jump Tables

C !!..

Commands

Conditional Jump
Conditional Move

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Compare

Assembly Language

Anonymous

Logic Structures in

Compare

There are two commands designed explicitly for setting the condition code: cmp (compare) and test.

definition

cmpX S2 S1 ($X \in \{b, w, l, q\}$): Do S1 - S2 without storing the result.

Remark

Used to compare the order of two (un)signed numbers.

Test

definition

cmpX S2 S1 ($X \in \{b, w, l, q\}$): Do S1 & S2 without storing the result.

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte

Test

Conditions

Set

Jump Tables

Conditional

Conditional Jump

Conditional Jump

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Test

definition

cmpX S2 S1 ($X \in \{b, w, l, q\}$): Do S1 & S2 without storing the result.

Remark

Useful with a mask to check if some given digits are all 0.

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte

Test

Conditions

et

lump Tables

Conditional Commands

Conditional Jum

Conditional Moves

Logic Structures

Conditional Branches (if)
Loops (for, while)

Evercises

Test

definition

cmpX S2 S1 ($X \in \{b, w, l, q\}$): Do S1 & S2 without storing the result.

Remark

Useful with a mask to check if some given digits are all 0.

Remark

Frequently used as testq %rax %rax to check if a number if zero. (Shorter than cmpq %rax 0!)

Logic Structures in Assembly Language

Anonymous

Commands

Program Counter Condition Codes Compare

Test

Set

Jumps
Jump Tables

Conditiona

Commands
Conditional Jumps

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Canonical

n: not

e: equal ZF

z: zero ZF

Logic Structures in Assembly Language

Anonymous

Commands

Program Counter Condition Codes

Test

Conditions

Set Jumps Jump Tables

Conditional

Lommands Conditional Jumps

Conditional Moves

Logic Structures

Conditional Branches (if)
Loops (for, while)

Canonical

n: not

e: equal ZF

z: zero ZF

Signed

▶ g: greater (SF ⊕ OF)&ZF

► I: less SF ⊕ OF

Logic Structures in Assembly Language

Anonymous

Conditions

- Canonical
 - n: not
 - e: equal ZF
 - z: zero ZF
- Signed
 - ▶ g: greater (SF ⊕ OF)&ZF
 - ► I: less SF ⊕ OF
- Unsigned
 - ► a: above CF& ZF
 - b: below CF

Logic Structures in Assembly Language

Anonymous

ommands

Program Counter Condition Codes

Test

Conditions

Jumps Jumps

Jump Tables

Conditional

Conditional Jumps

ogic Structures

Conditional Branches (if)
Loops (for, while)

E....in

Canonical

n: not

e: equal ZF

> z: zero 7F

Signed

g: greater (SF ⊕ OF)&ZF

I: less SF ⊕ OF

Unsigned

► a: above CF& 7F

b: below CF

Remark

n is used as a prefix to negate the conditions that follow.

Remark

e can be used as a suffix to a,b,g,l representing 'or equal'.

Logic Structures in Assembly Language

Anonymous

Conditions

Program Counte Condition Codes

Test

Condition

Set

Jumps

Jump Tables

Conditional Commands

Conditional Jumps

Lagia Structura

Logic Structures

Conditional Branches (if)
Loops (for, while)

ricer Statemen

Exercises

We need a way to retrieve and manipulate the condition codes.

definition

set X D (X is a condition): moving the corresponding combination of condition codes into the lower-order byte of D.

Remark

Set doesn't clear the high-order bytes.

Jumps

To implement more complicated structures while minimizing the size of the assembly program, jumps are introduced.

definition

jmp X: jump to an memory address specified by X (can be a label)

jmp R: jump to the memory address specified in register R jmp R: jump to the memory address specified in the memory specified by register R

Logic Structures in Assembly Language

Anonymous

Commands

Program Counter Condition Codes

Test

Conditions

Jumps

Jumps

Jump Tables

Conditional
Commands
Conditional Jumi

Conditional Jump Conditional Move

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Jumps

To implement more complicated structures while minimizing the size of the assembly program, jumps are introduced.

definition

jmp X: jump to an memory address specified by X (can be a label)

jmp R: jump to the memory address specified in register R jmp R: jump to the memory address specified in the memory specified by register R

Remark

PC-relative encoding have two advantages:

- more compactly encoded instruction
- more portable code

Logic Structures in Assembly Language

Anonymous

Commands

Program Count

Condition Code

Test

Conditions

Jumps

Jumps

Jump Tables

Commands

Conditional Jump Conditional Move

ogic Structures

Conditional Branches (if) Loops (for, while) Switch Statements (switch

Jump Tables

We can also use a constant table to refer to what's the jump destination.

definition

An anchor label and an alignment specification.

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte Condition Codes

Compare

°onditions

at.

Jumps

Jump Tables

Conditio

Commands

Conditional Jumi

Conditional Jump

Logic Structures

Conditional Branches (if)
Loops (for, while)

Jump Tables

We can also use a constant table to refer to what's the jump destination.

definition

An anchor label and an alignment specification.

structure

```
.section .rodata /* stands for read-only data */
.align 8 /* specifies the alignment used in the table */
.L4: /* the anchor label */
.quad .L8
.quad .L2
```

usage

jmp .L2(,%rax,8): jump to the label specified by %rax

Logic Structures in Assembly Language

Anonymous

ommands

Program Counter Condition Codes

Test

Conditions

et

Jump Tables

Commands

Conditional Jumps Conditional Moves

Logic Structure

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Jump Tables

We can also use a constant table to refer to what's the jump destination.

definition

An anchor label and an alignment specification.

structure

```
.section .rodata /* stands for read-only data */
.align 8 /* specifies the alignment used in the table */
.L4: /* the anchor label */
.quad .L8
```

.quad .L2

usage

jmp .L2(,%rax,8): jump to the label specified by %rax

Remark

Jump tables help perform jumps automatically. 4ロト 4倒ト 4 三ト 4 三ト 三 めの()

Logic Structures in Assembly Language

Anonymous

Jump Tables

Conditional Jumps

To harness the power of condition codes, conditional jumps are introduced.

definition

jX D (X is a condition): jump to the address specified by D if X is satisfied.

Remark

Conditional jump are the reason why we could implement logic structure.

Logic Structures in Assembly Language

Anonymous

Commands

Program Counter

Compare

Conditions

onditions.

Jumps

Jump Tables

Commands

Conditional Jumps

Logic Structures

Conditional Branches (if) Loops (for, while)

oops (for, while) vitch Statement

rep&repz

In the assembly code provided in the CSAPP textbook and the bomb lab, sometimes **ret** is written as **rep ret** or **repz ret**.

So, why are they there in the first place?

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte

Compare

Condition

Condition

Jumps

Jump Table

Commands

Commands
Conditional Jumps

Conditional Jumps

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

rep&repz

In the assembly code provided in the CSAPP textbook and the bomb lab, sometimes ret is written as rep ret or repz ret

So, why are they there in the first place?

Answer

They are only used for AMD CPUs since these CPUs cannot handle the return address if ret is reached from a conditional jump. In another word, rep and repz are meaningless occupiers that could avoid this situation from happening.

Logic Structures in Assembly Language

Anonymous

Conditional Jumps

Before diving into details why we introduce conditional moves, we first review the definition of conditional moves(cmov).

definition

cmovSX R1 R2 (S is the size and X is a condition): if X is satisfied, move data from R1 to R2. R1, R2 cannot both be memory address.

Example

movq %rdi, %rax subq %rsi, %rax movq %rsi, %rdx subq %rdi, %rdx cmpq %rsi, %rdi cmovge %rdx, %rax ret Logic Structures in Assembly Language

Anonymous

Commands

Program Counter Condition Codes

Test

onditions

Set

Jump Tables

Conditional Commands

Conditional Jump

Conditional Moves

ogic Structures

Conditional Branches (if) Loops (for, while) Switch Statements (switch

So, why use cmov?

Logic Structures in Assembly Language

Anonymous

Commands

Program Count Condition Code

Compare

Condition

Condition

Jumps

Candisian

Commands

Conditional Jur

Conditional Moves

I a mia Cammaanna

Logic Structures

Loops (for, while)
Switch Statements (switch

Evercises

So, why use cmov?

- Advantages
 - Save space
 - Enhanced performance on pipelined CPUs (while jmp perform terribly) due to condition code transfers.

Logic Structures in Assembly Language

Anonymous

Lommands

Program Counter Condition Codes

Compare

Conditions

onditions

Jumps

Jump Tables

onditional

Conditional Jumps

ogic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Exercises

Remark

Pipelined CPU achieves high performance by overlapping the steps of the successive instructions.



So, why use cmov?

- Advantages
 - Save space
 - Enhanced performance on pipelined CPUs (while jmp perform terribly) due to condition code transfers.
- Disadvantages
 - May break the structure of assembly code
 - Increase the calculation workload
 - Forbidden in some cases

Logic Structures in Assembly Language

Anonymous

ommands

Program Counter Condition Codes

Compare

Test

Conditions

Set

Jumps

Conditiona

Commands

Conditional Jumps

Conditional Moves

ogic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch

Exercises

Remark

Pipelined CPU achieves high performance by overlapping the steps of the successive instructions.



So, why use cmov?

- Advantages
 - Save space
 - Enhanced performance on pipelined CPUs (while jmp perform terribly) due to condition code transfers.
- Disadvantages
 - May break the structure of assembly code
 - Increase the calculation workload
 - Forbidden in some cases
- Bad cases
 - Expensive evaluations: function-involved
 - Risky computation: p ? *p : 0
 - ► Computations with side effects: +=, *=

Remark

Pipelined CPU achieves high performance by overlapping the steps of the successive instructions.

Logic Structures in Assembly Language

Anonymous

ommands

Program Counter Condition Codes

Test

Conditions

lumns

Jump Tables

Conditional

Conditional Jump

Conditional Moves

Logic Structures

onditional Branches (pops (for, while)

Evercises

Logic Structures in Assembly Language

Anonymous

Conditional Branches (if)

Implementation

cmov, conditional jumps

Example

Implement a function that return abs of the first argument.

Answer

mov %rdi %rax test %rax %rax ige .L1 sub \$0 %rax

.L1:

repz ret

for, while

Implementation conditional jumps

Example

Implement a loop using %rdi and %rsi where the outer i iterates from 0 to 9 and the inner one iterates from i to 9

Logic Structures in Assembly Language

Anonymous

Loops (for, while)

for, while

Answer mov \$0 %rdi jmp .CHECK1 .LOOP1: mov %rdi %rsi jmp .CHECK2 .LOOP2: ... //do stuff .CHECK2: cmp %rsi \$9 ile .LOOP2 .CHECK1: cmp %rdi \$9

ile .LOOP1

Logic Structures in Assembly Language

Anonymous

Loops (for, while)

switch

Implementation

jump tables

Example

Implement a function on a 64x machine to jump to .L1 when %rax is prime and .L1 when it is not. (% $rax \in \{1,2,3,4\}$)

Answer

.section .rodata

.align 8

.ANCHOR:

.quad .L0

.quad .L1

.quad .L1

.quad .L0

. . .

jmp .ANCHOR(,%rax,\$8)

Logic Structures in Assembly Language

Anonymous

Commands

Program Counter Condition Codes Compare

Conditions

Jumps

Jump Tables

Conditional Commands

onditional Jumps

Conditional Moves

Logic Structures

Conditional Branches (if)
Loops (for, while)
Switch Statements (switch)

,

Exercises

Logic Structures in Assembly Language

Anonymous

Commands

Program Counte

Compare

Carathera

Condition

Set

lumn Tabl

Conditiona

Conditional Jum

Conditional Moves

Logic Structures

Conditional Branches (if) Loops (for, while)

witch Statements (