ICS Seminar Week3 Prep

王善上 贾博暄 倪嘉怡 许珈铭

2023.9.23

寻址

1．判断下列 x86-64 ATT 操作数格式是否合法。

(1) (　　) 8(%rax, ,2)

(2) (　　) $30(%rax,%rax,2)

(3) (　　) 0x30

(4) (　　) 13(,%rdi,4)

(5) (　　) (%rsi,%rdi,6)

(6) (　　) %ecx

(7) (　　) (%ecx)

(8)★(　　) (%rbp,%rsp)

F
F
T
T
F
T
F
F

7、x86体系结构的内存寻址方式有多种格式，请问下列哪些指令是正确的：（　　）

A. movl　$34,　(%eax)

B. movl　(%eax),　%eax

C. movl　$23,　10(%edx, %eax)

D. movl　(%eax),　8(%ebx)

ABC

5、下列指令中，寻址方式不正确的是

A. MOVB %ah, 0x20(, %ecx, 8)

B. LEAL (0xA, %eax), %ebx

C. SUBB 0x1B, %bl

D. INCL (%ebx, %eax)

答:(　　)

B

6. 下列寻址模式中，正确的是：

A. (%eax, , 4)　　B. (%eax, %esp, 3)

C. 123　　D. $1(%ebx, %ebp, 1)

C

3．下列操作不等价的是(　　)

A．movzbq 和 movzbl

B．movzwq 和 movzwl

C．movl 和 movslq

D．movslq %eax, %rax 和 cltq

C

4．判断下列 x86-64 ATT 数据传送指令是否合法。

(1)　(　　) movl $0x400010, $0x800010

(2)　(　　) movl $0x400010, 0x800010

(3)　(　　) movl 0x400010, 0x800010

(4)　(　　) movq $-4, (%rsp)

(5)　(　　) movq $0x123456789AB, %rax

(6)　(　　) movabsq $0x123456789AB,%rdi

(7)★(　　) movabsq $0x123456789AB,16(%rcx)

(8)★(　　) movq 8(%rsp),%rip

F
T
F
T
F
T
F
F

4. 在 x86-64 下，以下哪个选项的说法是错误的？

A) movl 指令以寄存器作为目的时，会将该寄存器的高位 4 字节设置为 0

B) cltq 指令的作用是将%eax 符号扩展到%rax

C) movabsq 指令只能以寄存器作为目的

D) movswq 指令的作用是将零扩展的字传送到四字节目的

D

6.以下关于 x86-64 指令的描述，说法正确的是：

A. 数据传送指令 movabsq $Imm, (%rax) 将以 64 位二进制补码表示的立即数 Imm 放到目的地址(%rax)中。

B. INC 和 DEC 指令会设置溢出标志 OF 和零标志 ZF，但不会改变进位标志 CF。

C. call *%rax 指令以%rax 中的值作为读地址，从内存中读出调用目标。

D. popq %rax 指令的行为等效于 movq %rsp, %rax; addq $8, %rsp。

B

(　　)9.在32位机器下,假设有如下定义int array[10] = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}; 某一时刻,%ecx存着第一个元素的地址,%ebx值为3,那么下列操作中____将array[3]移入了%eax.

A. leal 12(%ecx), %eax
B. leal (%ecx,%ebx,4), %eax
C. movl (%ecx,%ebx,4), %eax
D. movl 8(%ecx,%ebx,2), %eax

C

(　　)2.下列关于数据传送指令的说法中,正确的是____.

A.常规的movq指令只能以表示为32位补码数字的立即数作为源操作数(注：这里的"只能"强调的是不能以64位数作为源操作数),然后把这个值零扩展到64位的值,放到目的位置.movabsq指令能够以任意64位立即数值作为源操作数,并且只能以寄存器为目的.

B.在Imm(rb,ri,s)这一寻址模式中,s必须是1,2,4或者8,基址和变址寄存器必须是64位寄存器.

C.cqto指令不需要额外操作数,它的作用是把%eax符号扩展到%rax.

D.CPU执行指令"movl -1 %eax"后,%rax的值为0x00000000ffffffff.

B

9. `pushq %rbp` 的行为等价于以下（）中的两条指令。

A. `subq $8,%rsp  movq %rbp, (%rdx)`

B. `subq $8,%rsp  movq %rbp, (%rsp)`

C. `subq $8,%rsp  movq %rax, (%rsp)`

D. `subq $8,%rax  movq %rbp, (%rdx)`

B

1、某 C 语言程序中对数组变量 a 的声明为“int a[10][10];”，有如下一段代码：

```
for (i=0; i<10; i++)
    for (j=0; j<10; j++)
       sum+= a[i][j];
```

假设执行到“sum+= a[i][j];”时，sum 的值在%rax 中，a[i][0]所在的地址在%rdx 中，j 在%rsi 中，则“sum+= a[i][j];”所对应的指令是（　　）。

A. addl 0 (%rdx, %rsi, 4), %rax

B. addl 0 (%rsi, %rdx, 4) , %rax

C. addl 0 (%rdx, %rsi, 2) , %rax

D. addl 0 (%rsi, %rdx, 2) , %rax

A

条件码

10. 下列的指令组中，哪一组指令只改变条件码，而不改变寄存器的值？

A. CMP, SUB

B. TEST, AND

C. CMP, TEST

D. LEAL, CMP

C

1. 在下列指令中，其执行会影响条件码中的 CF 位的是：

A. jmp NEXT　　B. jc NEXT　　C. inc %bx　　D. shl $1,%ax

D

7. 已知短整型数组 S 的起始地址和下标 i 分别存放在寄存器%rdx 和%rcx，将&S[i]存放在寄存器%rax 中所对应的汇编代码是（ ）

A. leaq (%rdx, %rcx, 1), %rax　　B.movw (%rdx, %rcx, 2), %rax

C. leaq (%rdx, %rcx, 2), %rax　　D.movw (%rdx, %rcx, 1), %rax

C

4. 在下列的 x86-64 汇编代码中，错误的是：

A. `movq %rax, (%rsp)`　　B. `movl $0xFF, (%ebx)`

C. `movsbl (%rdi), %eax`　　D. `leaq (%rdx, 1), %rdx`

B/D

8. 下列关于条件码的描述中，不正确的是（）

A) 所有算术指令都会改变条件码

B) 所有比较指令都会改变条件码

C) 所有与数据传送有关的指令都会改变条件码

D) 条件码一般不会直接读取，但可以直接修改

C

6. X86-64 指令提供了一组条件码寄存器；其中 ZF 为零标志，ZF=1 表示最近的操作得出的结构为 0；SF 为符号标志，SF=1 表示最近的操作得出的结果为负数；OF 为溢出标志，OF=1 表示最近的操作导致一个补码溢出（正溢出或负溢出）。当我们在一条 cmpq 指令后使用条件跳转指令 jg 时，那么发生跳转等价于以下哪一个表达式的结果为 1？

A. ~(SF ^ OF) & ~ZF

B. ~(SF ^ OF)

C. SF ^ OF

D. (SF ^ OF) | ZF

A

2、条件码描述了最近一次算术或逻辑操作的属性。下列关于条件码的叙述中，哪一个是不正确的？

A. set 指令可以根据条件码的组合将一个字节设置为 0 或 1

B. cmp 指令和 test 指令可以设置条件码但不更改目的寄存器

C. leaq 指令可以设置条件码 CF 和 OF

D. 除无条件跳转指令 jmp 外，其他跳转指令都是根据条件码的某种组合跳转到标号指示的位置

C

CMP

5. 将 AX 清零，下列指令错误的是（ ）

A. sub %ax, %ax　　B. xor %ax, %ax

C. test %ax, %ax　　D. and $0, %ax

C

2． 下列关于比较指令 CMP 说法中，正确的是：

A．专用于有符号数比较　　B．专用于无符号数比较

C．专用于串比较　　D．不区分比较的对象是有符号数还是无符号数

D

控制

4. 对于如下的C语言中的条件转移指令，它所对应的汇编代码中至少包含几条条件转移指令：`if (a > 0 && a != 1 || a < 0 && a != -1) b=a;`

A. 2条　　B. 3条　　C. 4条　　D. 5条

B

3. 在如下代码段的跳转指令中，目的地址是：

```
400020: 74 F0     je _________
400022: 5d     pop %rbp
```

A. 400010　　B. 400012　　C. 400110　　D. 400112

B

8、对简单的 switch 语句常采用跳转表的方式实现，在 x86-64 系统中，下述最有可能正确的 switch 分支跳转汇编指令为哪个？

A. jmp .L3(,%eax,4)

B. jmp .L3(,%eax,8)

C. jmp *.L3(,%eax,4)

D. jmp *.L3(,%eax,8)

答：（ ）

D

8. 假设某条 C 语言 switch 语句编译后产生了如下的汇编代码及跳转表：

```
    movl 8(%ebp), %eax                  .L7:
    subl $48, %eax                      .long .L3
    cmpl $8, %eax                       .long .L2
    ja .L2                              .long .L2
    jmp *.L7(, %eax, 4)                 .long .L5
                                        .long .L4
                                        .long .L5
                                        .long .L6
                                        .long .L2
                                        .long .L3
```

在源程序中，下面的哪些（个）标号出现过：

A. '2', '7'

B. 1

C. '3'

D. 5

C

6. 在如下 switch 语句对应的跳转表中，哪些标号没有出现在分支中（ ）

```
addq $1, %rdi
cmpq $8, %rdi
ja .L2
jmp *.L4(, %rdi, 8)
.L4:   .quad .L9    .quad .L5    .quad .L6    .quad .L7
       .quad .L2
       .quad.L7     .quad .L8    .quad .L2    .quad .L5
```

A. 3, 6　　B. -1, 4　　C. 0, 7　　D. 2, 4

A

7. 下列关于程序控制结构的机器代码实现的说法中，正确的是：

A) 使用条件跳转（conditional jump）语句实现的程序片段比使用条件赋值（conditional move）语句实现的同一程序片段的运行效率高

B) 使用条件跳转语句实现的程序片段与使用条件赋值语句实现的同一程序片段虽然效率可能不同，但在 C 语言的层面上看总是有着相同的行为

C) 一些 switch 语句不会被 gcc 用跳转表的方式实现

D) 以上说法都不正确

C

5． 在下列关于条件传送的说法中，正确的是：

A．条件传送可以用来传送字节、字、双字、和 4 字的数据

B．C 语言中的“?:”条件表达式都可以编译成条件传送

C．使用条件传送总可以提高代码的执行效率

D．条件传送指令不需要用后缀（例如 b，w，l，q）来表明操作数的长度

D

End

4. 以下关于 x86-64 指令的描述，说法正确的有几项？

a) 有符号除法指令 idivq S 将%rdx（高 64 位）和%rax（低 64 位）中的 128 位数作为被除数，将操作数 S 的值作为除数，做有符号除法运算；指令将商存在%rdx 寄存器中，将余数存在%rax 寄存器中。

b) 我们可以使用指令 jmp %rax 进行间接跳转，跳转的目标地址由寄存器%rax 的值给出。

c) 算术右移指令 shr 的移位量既可以是一个立即数，也可以存放在单字节寄存器%cl 中。

d) leaq 指令不会改变任何条件码。

A. 1

B. 2

C. 3

D. 4

A

)6. x86 体系结构中,下面哪个说法是正确的?

A. leal 指令只能够用来计算内存地址

B. x86_64 机器可以使用栈来给函数传递参数

C. 在一个函数内,改变任一寄存器的值之前必须先将其原始数据保存在栈内

D. 判断两个寄存器中值大小关系,只需要 SF 和 ZF 两个条件码

B