第二章 指令系统原理与实例

- ❖ 2.1 简介
- ❖ 2.2 指令集系统结构的分类
- ❖ 2.3 存储器寻址
- ❖ 2.4 操作数的类型
- ❖ 2.5 指令系统的操作
- ❖ 2.6 控制流指令
- ❖ 2.7 指令系统的编码
- ❖ 2.8 编译器的角色
- ❖ 2.9 MIPS系统结构
- ❖ 2.10 谬误和易犯的错误
- **※ 2.11 结论**

- ☆控制流指令分类条件转移, 跳转, 过程调用, 过程返回
- ❖ "跳转" (Jump): 当控制指令为无条件改变控制流时,我们称之为"跳转"。
- ❖ "分支" (Branch): 而当控制指令是有条件改变控制流时,我们称之为"分支"。
- ❖控制流程的改变情况:
 - 条件分支(conditional branch);
 - 跳转(jump);
 - 过程调用(call);
 - 过程返回(return)。

MIPS Branch Operations

- Branch to a labeled instruction if a condition is true
 - Otherwise, continue sequentially
 - beq rs, rt, L1
 - if (rs == rt) branch to instruction labeled L1;
 - bne rs, rt, L1
 - if (rs != rt) branch to instruction labeled L1;

Example if Statement if.s

Assuming translations below, compile if block

$$f \rightarrow \$s0$$
 $g \rightarrow \$s1$ $h \rightarrow \$s2$
 $i \rightarrow \$s3$ $j \rightarrow \$s4$
if (i == j) bne \$s3,\$s4,Exit
 $f = g + h;$ add \$s0,\$s1,\$s2

May need to negate branch condition

Exit:

Example if simple_branch.asm

```
# MIPS assembly code
  # C code:
  #
 + x = 0 
                                          move $t0, $zero
  # \text{ if } (x == 0) \{
                                          bne $t0, $zero, after_print
                            # printf("x is zero")
                                          li $v0, 4
                            la $a0, x_is_zero
  # }
                            # exit()
                                          syscall
                            after_print:
                                          li $v0, 10
                            syscall
```

Compiling if-else Statements

C code:

```
i≠i
                                       i = = j?
if (i==j) f = g+h;
                                             Else:
                                               f=g-h
else f = g-h;
• f, g, h, i, j in $s0, $s1, ...
                                     Exit:
```

Assembler calculates addresses

Compiled MIPS code: if then else.s

```
bne $s3, $s4, Else
      add $s0, $s1, $s2
      i Exit
Else: sub $s0, $s1, $s2
Exit: *...
```

Compiling Loop Statements

C code:

```
while (save[i] == k) i += 1;
```

- i in \$s3, k in \$s5, address of save in \$s6
- Compiled MIPS code:while.s

```
Loop: sll $t1, $s3, 2
add $t1, $t1, $s6
lw $t0, 0($t1)
bne $t0, $s5, Exit
addi $s3, $s3, 1
j Loop
Exit: ...
```

Example add_0_to_n.s

```
.text
                                                main:
// Adds up all numbers between 0 and N.
// For example, if N = 3, then it would find
//0 + 1 + 2 + 3 = 6
                                                    li $t0, 3 # value of N
sum = 0;
                                                    li $t1, 0
                                                              # running sum
while (N != 0) {
                                                loop:
                                                    beg $t0, $zero, loop exit
 sum += N;
                                                    addu $t1, $t1, $t0
  N--;
                                                    addi $t0, $t0, -1
                                                    j loop
                                                loop exit:
```

For Loops

```
for (initialization; condition; loop operation)
  statement
```

- initialization: executes before the loop begins
- condition: is tested at the beginning of each iteration
- loop operation: executes at the end of each iteration
- statement: executes each time the condition is met

demo: for_loop.s

C Code

```
// add the numbers from 0 to 9
int sum = 0;
int i;

for (i=0; i!=10; i = i+1) {
   sum = sum + i;
}
```

MIPS assembly code

done:

More Conditional Operations

- Set result to 1 if a condition is true
 - Otherwise, set to 0
- slt rd, rs, rt
 - if (rs < rt) rd = 1; else rd = 0;
- slti rt, rs, constant
 - if (rs < constant) rt = 1; else rt = 0;</p>
- Use in combination with beq, bne

```
slt $t0, $s1, $s2 # if ($s1 < $s2)
bne $t0, $zero, L # branch to L</pre>
```

Demo: slt.s

C Code

```
// add the powers of 2 from 1
// to 10
int sum = 0;
int i,j;

for (i=1,j=2; i < 11; i= i+1,j=j*2)
{
   sum = sum + j;
}</pre>
```

MIPS assembly code

```
\# \$s0 = i, \$s1 = sum, \$s2 = j
       addi $s1, $0, 0
       addi $s0, $0, 1
       addi $s2, $0, 2
loop: slti $t1, $s0, 11
       beq $t1, $0, done
       add $s1, $s1, $s2
      addi $s0, $s0, 1
       sll $s2, $s2, 1
            loop
done:
```

Example max.s

.end main

```
# stores the max of two numbers
    .text
main:
    # two initial numbers
    li $t0, 5
    li $t1, 10
    # put max in $t3
    #
    # max = $t0
    # if ($t0 < $t1) {
    # max = $t1
    # }
    move $t3, $t0
    slt $t2, $t0, $t1 # $t0 < $t1?
    beq $t2, $zero, have_max # if not, we are done
    move $t3, $t1
have max:
    # print out the result
    li $v0, 1
    move $a0, $t3
    syscall
    # exit the program
    li $v0, 10
    syscall
```

COD 5e Exercise 2.23

- Assume \$t0 holds the value 0x00101000. What is the value of \$t2 after the following instructions?
- 假设\$t0中存放数值 0x00101000, 在执行下列指令后\$t2的值 是多少?

```
slt $t2, $0, $t0
bne $t2, $0, ELSE
DONE
```

ELSE: addi \$t2, \$t2, 2

DONE:

COD 5e Exercise 2.23

Assume \$t0 holds the value 0x00101000. What is the value of \$t2 after the following instructions?

```
slt $t2, $0, $t0
bne $t2, $0, ELSE
j DONE
ELSE: addi $t2, $t2, 2
DONE:
```

2.23 (Answer)

❖ Assume \$t0 holds the value 0x00101000. What is the value of \$t2 after the following instructions?

```
slt $t2, $0, $t0
```

bne \$t2, \$0, ELSE

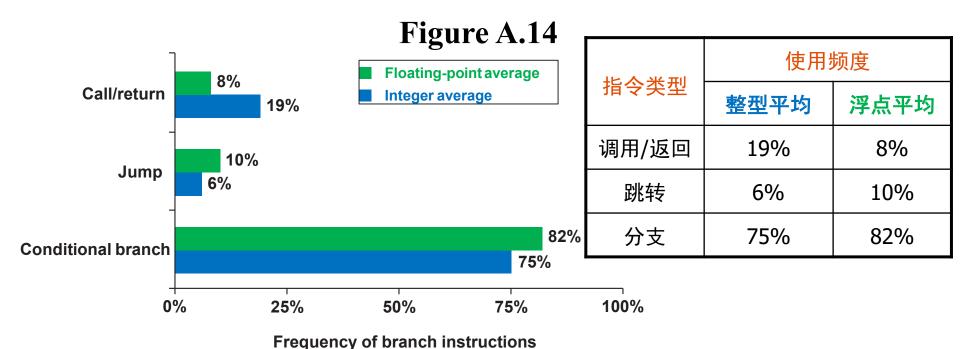
j DONE

ELSE: addi \$t2, \$t2, 2

DONE:

$$$t2 = 3$$

- ☆控制流指令分类条件转移,跳转,过程调用,过程返回
- ❖ 控制流指令不同类型出现的相对频率(Alpha 上测试)



❖不同类型条件转移中的频率(Alpha 上测试)

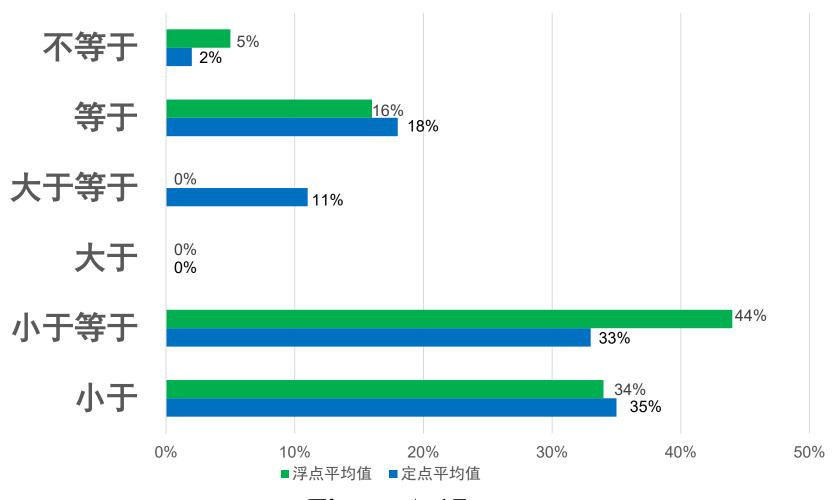


Figure A.17

- ❖ 控制流指令的寻址方式
 - 一般要指明转移的目标地址。 过程返回是例外,因为编译时不知道返回地址。
- PC相对寻址,即使用基于程序计数器(PC)的位移量来 指定目标地址。

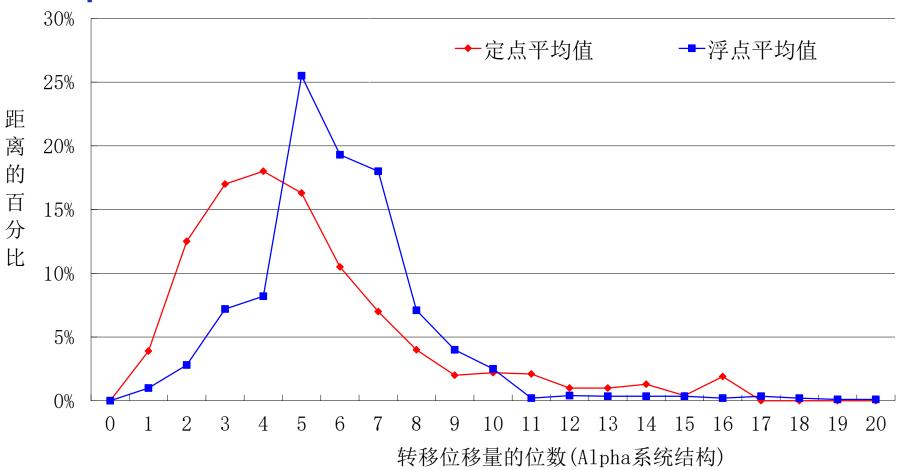
PC相对寻址指令的优点:

目标与当前指令离得不远; 使用相对偏移地址可以 缩减指令长度。

使用相对寻址的程序可以载入到主存任何位置, 称为位置无关, 对在执行时才链接的程序可以减少工作量。

PC相对寻址转移距离:转移指令与目标之间的指令数

(Alpha 上测试) Figure A.15



定点相对寻址转移位移量: 至少8位。MIPS是16位

例如: 64位MIPS主要控制流指令

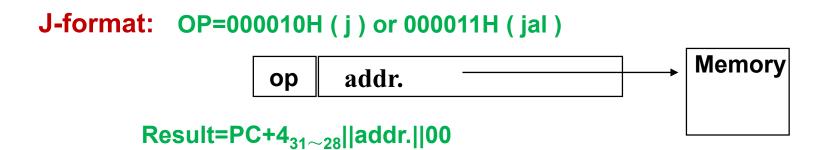
❖ MIPS控制流指令 Figure A.25

指令举例	指令名称	含义
j name	跳转	PC←PC+4 _{GPRLENGTH-128} name 2b'00
jal name	跳转并链接	Regs[r31]←PC+8 PC← PC +4 _{GPRLENGTH-128} name 2b'00
jalr r2	寄存器跳转并链接	Regs[r31]←PC+8 PC←Regs[r2]
jr r3	寄存器跳转	PC←Regs[r3]
beqz r1, name	等于零时分支	If(Regs[r1]==0) PC←PC+4 + name << 2
bne r3, r4, name	不等于时分支	If(Regs[r3]!=(Regs[r4]) PC←PC+4 + name << 2
movz r1, r2, r3	等于零时传送	if(Regs[r3]==0) Regs[r1]←Regs[r2]

分支的目标地址=16位带符号位移量左移2位+(PC+4)

MIPS指令是32位,4个字节长

J-Format Instructions



● 寄存器间接跳转

编译时不知道目标位置,为了实现返回和间接跳转,需要使用寄存器间接跳转:给出包含目标地址的寄存器名称。

寄存器间接跳转还支持:

- * 分支选择语句case或者switch
- * 面向对象语言中的虚拟函数或者方法
- * 高阶函数或者函数指针
- * 动态共享库

以上四种情况,编译时都不知道目标地址,因此通常在寄存器 间接跳转之前,才把地址从存储器载入到寄存器中。

COD 5e Exercise 2.24

- Suppose the program counter (PC) is set to 0x2000 0000. Is it possible to use one jump (j) MIPS assembly instruction to set the PC to the address as 0x4000 0000? Is it possible to use one branch-on-equal (beq) MIPS assembly instruction to set the PC to this same address?
- 假设程序计数器 (PC) 被设置为 0x2000 0000, 是否可以使用 MIPS的跳转(j)指令将 PC 设置为地址 0x4000 0000? 是否可以 使用MIPS的相等则分支(beq)指令将 PC 设置为该地址?

2.24(Answer)

Suppose the program counter (PC) is set to 0x2000 0000. Is it possible to use the jump (j) MIPS assembly instruction to set the PC to the address as 0x4000 0000? Is it possible to use the branch-on-equal (beq) MIPS assembly instruction to set the PC to this same address?

jump: no, beq: no

COD 5e Exercise 2.26

- Consider the following MIPS loop:
- 考虑如下的MIPS循环:
- LOOP: slt \$t2, \$0, \$t1
- beq \$t2, \$0, DONE
- addi \$t1, \$t1, -1
- addi \$s2, \$s2, 2
- i LOOP
- DONE:

COD 5e Exercise 2.26

- Consider the following MIPS loop:
- LOOP: slt \$t2, \$0, \$t1
- beq \$t2, \$0, DONE
- addi \$t1, \$t1, -1
- addi \$s2, \$s2, 2
- j LOOP
- **DONE:**

2.26

- [1] Assume that the register \$t1 is initialized to the value 10.
 What is the value in register \$s2 assuming \$s2 is initially zero?假设寄存器\$t1的初始值为10,假设\$t2初始值为0,则循环执行完毕时寄存器\$t2的值是多少?
- [2] For each of the loops above, write the equivalent C code routine. Assume that the registers \$s1, \$s2, \$t1, and \$t2 are integers A, B, i, and temp, respectively.对于上面的循环体, 写出等价的C代码例程。假定寄存器\$s1、\$s2、\$t1和\$t2分别为整数A、B、i和temp。
- [3] For the loops written in MIPS assembly above, assume that the register \$t1 is initialized to the value N. How many MIPS instructions are executed?假定寄存器\$t1的初始值为 N,上面的MIPS汇编循环执行了多少条指令?

2.26

- [1] Assume that the register \$t1 is initialized to the value 10. What is the value in register \$s2 assuming \$s2 is initially zero?
- [2] For each of the loops above, write the equivalent C code routine. Assume that the registers \$s1, \$s2, \$t1, and \$t2 are integers A, B, i, and temp, respectively.
- [3] For the loops written in MIPS assembly above, assume that the register \$t1 is initialized to the value N. How many MIPS instructions are executed?

2.26 Answer (1)

- Consider the following MIPS loop:
- LOOP: slt \$t2, \$0, \$t1
- beq \$t2, \$0, DONE
- addi \$t1, \$t1, -1
- addi \$s2, \$s2, 2
- j LOOP
- DONE:

[1] Assume that the register \$t1 is initialized to the value 10. What is the value in register \$s2 assuming \$s2 is initially zero?

[1] 20

2.26 Answer(2)

- Consider the following MIPS loop:
- LOOP: slt \$t2, \$0, \$t1
- beq \$t2, \$0, DONE
- addi \$t1, \$t1, -1
- addi \$s2, \$s2, 2
- j LOOP
- **DONE:**

[2] For each of the loops above, write the equivalent C code routine. Assume that the registers \$\$1, \$\$\$2, \$\$\$1, and \$\$\$2 are integers A, B, i, and temp, respectively.

```
i = 10;
While (0 < i) {
i += -1;
B += 2;
}
```

2.26 Answer(3)

- Consider the following MIPS loop:
- LOOP: slt \$t2, \$0, \$t1
- beq \$t2, \$0, DONE
- addi \$t1, \$t1, -1
- addi \$s2, \$s2, 2
- j LOOP
- DONE:

[3] For the loops written in MIPS assembly above, assume that the register \$t1 is initialized to the value N. How many MIPS instructions are executed?

- [3] 5*N+2 (when N > 0)
- 2 (when N<=0)

2.26 Answer

```
[1] 20
[2]
      i = 10;
      While (0 < i)
      i += -1;
      B += 2:
 [3] 5*N+2 ( when N > 0 )
            (when N \le 0)
```

COD 5e Exercise 2.29

- Translate the following loop into C. Assume that the C-level integer i is held in register \$11, \$s2 holds the C-level integer called result, and \$s0 holds the base address of the integer MemArray.
- 将下面的循环翻译成C代码。假定寄存器\$t1中存放C语言的整数i, \$s2中存放C语言的整数result, \$s0存放整数数组MemArray的基地 址。

```
addi $t1, $0, 0
LOOP: lw $s1, 0($s0)
add $s2, $s2, $s1
addi $s0, $s0, 4
addi $t1, $t1, 1
slti $t2, $t1, 100
bne $t2, $s0, LOOP
```

COD 5e Exercise 2.29

Translate the following loop into C. Assume that the C-level integer i is held in register \$t1, \$s2 holds the C-level integer called result, and \$s0 holds the base address of the integer MemArray.

```
addi $t1, $0, 0
LOOP: Iw $s1, 0($s0)
add $s2, $s2, $s1
addi $s0, $s0, 4
addi $t1, $t1, 1
slti $t2, $t1, 100
bne $t2, $s0, LOOP
```

2.29

Translate the following loop into C. Assume that the C-level integer i is held in register \$t1, \$s2 holds the C-level integer called result, and \$s0 holds the base address of the integer MemArray.

```
MemArray.
                               for (i=0; i<100; i++) {
      addi $t1, $0, 0
                                  result += MemArray[i];
LOOP: lw $s1, 0($s0)
      add $s2, $s2, $s1
      addi $s0, $s0, 4
                               Or
     addi $t1, $t1, 1
           $t2, $t1, 100
     slti
                               i = 0;
           $t2, $0, LOOP
      bne
                               do
                                result += MemArray[i];
                                i++;
```

} while(i < 100)

2.6控制流指令

❖过程调用的可选方案

有两种基本、传统的方法用来保存子程序使用的寄存器: 调用者保存和被调用者保存。

- 调用者保存:调用者调用其他过程时,必须保存在调用过程后还要使用的寄存器,被调用者则无须维护这些寄存器。
- 被调用者保存:被调用的过程必须保存它要使用的寄存器, 调用者则不受这种限制。

有时候,如果两个不同的过程都要访问相同的全局变量,则必须使用调用者保存方法。大多数实际使用的编译器会结合这两种方法。

8086 中断处理子程序(被调用者保存)

```
PRT INT PROC FAR
      PUSH
               AX
      PUSH
               \mathbf{B}\mathbf{X}
                          保护现场
      PUSH
            DX
      PUSH
             DS
                               ; 装入地址指针BX, DS
            BX, POINT
      LDS
                               ; 取打印数据
      MOV AL, [BX]
      POP
               DS
      POP
               \mathbf{D}\mathbf{X}
                          恢复现场
      POP
               \mathbf{B}\mathbf{X}
      POP
               AX
                              中断返回
      IRET
PRT INT
           ENDP
```

Six Steps in Execution of a Procedure

- 1. Main routine (caller) places parameters in a place where the procedure (callee) can access them
 - \$a0 \$a3: four argument registers
- 2. Caller transfers control to the callee (jal Dest)
- 3. Callee acquires the storage resources needed
- 4. Callee performs the desired task
- 5. Callee places the result value in a place where the caller can access it
 - \$v0 \$v1: two value registers for result values
- 6. Callee returns control to the caller (jr \$ra)
 - \$ra: one return address register to return to the point of original

Register Usage

- \$v0, \$v1: result values (reg's 2 and 3)
- \$t0 \$t9: temporaries
 - Can be overwritten by callee
- - Must be saved/restored by callee
- \$gp: global pointer for static data (reg 28)
- \$sp: stack pointer (reg 29)
- \$fp: frame pointer (reg 30)
- \$ra: return address (reg 31)

Register Usage

Register	Software	Register Usage	Saver	
Name	Name			
\$0	zero	Constant zero- Always returns 0		
\$1	at	Assembler temp(Reserved for assembler)		
\$2\$3	v0,v1	Function return	Caller	
\$4\$7	a0-a3	Incoming Arguments	Caller	
\$8\$15	t0-t7	Temporary Registers	Caller	
\$16\$23	s0-s7	Saved Registers	Callee	
\$24\$25	t8,t9	Temporary Registers	Caller	
\$26\$27	k0,k1	Exception Handling (Reserved for OS)	Callee	
\$28	gp	Global Pointer	Callee	
\$29	sp	Stack Pointer	Callee	
\$30	s8 or fp	Save register or Frame pointer if needed	Callee	
\$31	ra	Return Address	Caller	

Procedure Call Instructions

- Procedure call: jump and link jal ProcedureLabel
 - Address of following instruction put in \$ra
 - Jumps to target address
- Procedure return: jump register jr \$ra
 - Copies \$ra to program counter
- jump register can also be used for computed jumps
 - e.g., for switch/case statements

Leaf Procedure Example

C code:

```
int leaf_example (int g, h, i, j)
{ int f;
    f = (g + h) - (i + j);
    return f;
}
```

- Arguments g, ..., j in \$a0, ..., \$a3
- f in \$s0 (hence, need to save \$s0 on stack)
- Result in \$v0

Leaf Procedure Example

MIPS code: leaf_example.s

<pre>leaf_example:</pre>				
addi	\$sp,	\$sp, -4		
SW	\$s0,	0(\$sp)	•	
add	\$t0,	\$a0, \$a1		
add	\$t1,	\$a2, \$a3		
sub	\$s0,	\$t0, \$t1		
add	\$v0,	\$s0, \$zero		
٦w	\$s0,	0(\$sp)	ı	
addi	\$sp,	\$sp, 4		
jr	\$ra		l	

Save \$s0 on stack

Procedure body

Result

Restore \$s0

Return

Non-Leaf Procedures

- Procedures that call other procedures
- For nested call, caller needs to save on the stack:
 - Its return address
 - Any arguments and temporaries needed after the call
- Restore from the stack after the call

MIPS jump, branch, compare instructions

Instruction	Example	<u>Meaning</u>
branch on equal	beq \$1,\$2,100 Equal test; PC re	if (\$1 == \$2) go to PC+4+100*4 elative branch
branch on not eq.	bne \$1,\$2,100 Not equal test; P	if (\$1!= \$2) go to PC+4+100*4 C relative
set on less than	slt \$1,\$2,\$3 Compare less the	if (\$2 < \$3) \$1=1; else \$1=0 an; 2's comp.
set less than imm.	slti \$1,\$2,100 Compare < cons	if (\$2 < 100) \$1=1; else \$1=0 tant; 2's comp.
set less than uns.		if (\$2 < \$3) \$1=1; else \$1=0 an; natural numbers
set I. t. imm. uns.		if (\$2 < 100) \$1=1; else \$1=0 tant; natural numbers
jump	j 10000 Jump to target a	go to $PC+4_{31\sim28}$ 10000*4 ddress
jump register	jr \$31 For switch, proce	•
jump and link	jal 10000 For procedure ca	\$31 = PC + 4; go to $PC+4_{31\sim28} 10000*4$

2.6控制流指令

❖条件转移的可选方案 Figure A.16

名称	举例	如何测试条件	优点	缺点
条件码 (CC)	80x86, ARM, PowerPC, SPARC, SuperH	由ALU操作设定的 某些特定位,可能 是由程序控制的	有时条件可自由设置	CC是附加状态。条件 码强制限制了指令顺 序,因为它把信息从 一条指令传送给一个 转移
条件寄 存器	Alpha, MIPS	用比较结果测试任 意寄存器	简单	占用一个寄存器
比较并 转移	PA-RISC, VAX	比较是转移的一部 分,通常比较只限 于子集内部	一个转移是 一条而不是 两条指令	对流水线执行来说, 一条指令要做的事情 可能太多了

上图列出了目前使用的三种方法和它们各自的优缺点。

Discussion

- ❖ 考虑条件分支指令的两种不同设计方法:
 - (1) CPU1: 通过比较指令设置条件码, 然后测试条件码进行分支。
 - (2) CPU2: 在分支指令中包括比较过程。

在这两种CPU中,条件分支指令都占用2个时钟周期,而所有其它指令占用1个时钟周期。对于CPU1,执行的指令中分支指令占30%;由于每条分支指令之前都需要有比较指令,因此比较指令也占30%。由于CPU1在分支时不需要比较,因此CPU2的时钟周期时间是CPU1的1.35倍。问:哪一个CPU更快?如果CPU2的时钟周期时间只是CPU1的1.15倍,哪一个CPU更快呢?

Discussion

- ❖ 考虑条件分支指令的两种不同设计方法:
 - (1) CPU1: 通过比较指令设置条件码, 然后测试条件码进行分支。
 - (2) CPU2: 在分支指令中包括比较过程。

在这两种CPU中,条件分支指令都占用2个时钟周期,而所有其它指令占用1个时钟周期。对于CPU1,执行的指令中分支指令占30%;由于每条分支指令之前都需要有比较指令,因此比较指令也占30%。由于CPU1在分支时不需要比较,因此CPU2的时钟周期时间是CPU1的1.35倍。问:哪一个CPU更快?如果CPU2的时钟周期时间只是CPU1的1.15倍,哪一个CPU更快呢?

Discussion

考虑条件分支指令的两种不同设计方法:

- (1) CPU_1 : 通过比较指令设置条件码,然后测试条件码进行分支。
 - (2) CPU2: 在分支指令中包括比较过程。

在这两种CPU中,条件分支指令都占用2个时钟周期,而所有 其它指令占用1个时钟周期。对于CPU₁,执行的指令中分支指令占 30%;由于每条分支指令之前都需要有比较指令,因此比较指令也 占30%。由于CPU₁在分支时不需要比较,因此CPU₂的时钟周期时间 是CPU₁的1.35倍。问:哪一个CPU更快?如果CPU₂的时钟周期时间 只是CPU₁的1.15倍,哪一个CPU更快呢? 解 采用CPU时间公式。占用2个时钟周期的分支指令占总指令的30%,剩下的指令占用1个时钟周期。所以

$$CPI_1 = 0.3 \times 2 + 0.70 \times 1 = 1.3$$

则CPU₁性能为:

总CPU时间₁ =
$$IC_1 \times 1.3 \times$$
时钟周期₁

根据假设,有:

时钟周期
$$_2 = 1.35 \times 时钟周期_1$$

在CPU₂中没有独立的比较指令,所以CPU₂的程序量为CPU₁的 70%,分支指令的比例为:

$$30\%/70\% = 42.8\%$$

$$30\%/70\% = 42.8\%$$

这些分支指令占用2个时钟周期,而剩下的57.2%的指令占用1个时钟周期,因此:

$$CPI_2 = 0.428 \times 2 + 0.572 \times 1 = 1.428$$

因为CPU。不执行比较,故:

$$IC_2 = 0.7 \times IC_1$$

因此CPU。性能为:

总CPU时间₂ =
$$IC_2 \times CPI_2 \times DPP = IC_2 \times D$$

前面计算 总CPU时间₁ = IC₁ × 1.3 ×时钟周期₁

在这些假设之下,尽管CPU₂执行指令条数较少,CPU₁因为有着更短的执行时间,所以更快。

如果 CPU_2 的时钟周期时间仅仅是 CPU_1 的1.15倍,则时钟周期₂ = 1.15 ×时钟周期₁

CPU2的性能为:

前面计算 总CPU时间 $_1 = IC_1 \times 1.3 \times$ 时钟周期 $_1$ 因此 CPU_2 更快。