

2.9 人机交互

! (@ | = > (wow open tab at bar is great)

——键盘诗《Hatless Atlas》的第4行，1991

(对ASCII字符的一些命名：“!”是wow，“(”是open，“|”是bar，等等)

发明计算机是为了数字计算，不过计算机很快被用于商业方面的文字处理。今天大多数计算机使用8位的字节来表示字符，也就是几乎每个人都遵循的ASCII（American Standard Code for Information Interchange）码。图2-15对ASCII进行了总结。

ASCII值	字符	ASCII值	字符	ASCII值	字符	ASCII值	字符	ASCII值	字符	ASCII值	字符
32	space	48	0	64	@	80	P	96	`	112	p
33	!	49	1	65	A	81	Q	97	a	113	q
34	"	50	2	66	B	82	R	98	b	114	r
35	#	51	3	67	C	83	S	99	c	115	s
36	\$	52	4	68	D	84	T	100	d	116	t
37	%	53	5	69	E	85	U	101	e	117	u
38	&	54	6	70	F	86	V	102	f	118	v
39	'	55	7	71	G	87	W	103	g	119	w
40	(56	8	72	H	88	X	104	h	120	x
41)	57	9	73	I	89	Y	105	i	121	y
42	*	58	:	74	J	90	Z	106	j	122	z
43	+	59	;	75	K	91	[107	k	123	{
44	,	60	<	76	L	92	\	108	l	124	l
45	-	61	=	77	M	93]	109	m	125	
46	.	62	>	78	N	94	^	110	n	126	~
47	/	63	?	79	O	95	_	111	o	127	DEL

图2-15 字符的ASCII码表示。注意所有大写字母和对应小写字母的差均为32，这个观测结果可以得到一条检查和切换大小写的简便方法。没有给出的ASCII值包括格式化字符。例如，8代表退格，9代表tab字符，而13代表回车。另外一个有用的值0表示null，C编程语言用这个来标记字符串的结尾。这些内容可以在MIPS参考数据卡的第3列中找到

106

01 例题·ASCII码与二进制数对比

我们可以使用一串ASCII码而不用整数来表示数字。如果用ASCII码表示10亿这个数将比用32位整数表示增加多少存储呢？

01 答案

10亿就是1 000 000 000，需要使用10位ASCII码表示，每一个ASCII码都是8位长。所以存储将增长到 $(10 \times 8) / 32$ ，即2.5倍。除了存储空间要增加外，用于对这些十进制数字进行加法、减法、乘法和除法的硬件的设计也是困难的。这些困难解释了为什么计算专家越来越相信使用二进制的计算机是自然的，而偶然出现的十进制计算机则是奇怪的。□

可以使用一系列指令从一个字中提取出一个字节，所以字的读取和存储同样可以完成对字节的传输。然而，由于在某些程序中对文本的操作十分普遍，所以MIPS还提供字节传输指令。字节读取1b（load byte）指令从内存中读出一个字节，并将其放在一个寄存器最右边的8位。

字节存储 sb (store byte) 指令把一个寄存器最右边的 8 位取出来然后写到内存中。这样，我们可以按下面的顺序复制一个字节：

```
lb $t0,0($sp)      # Read byte from source
sb $t0,0($gp)      # Write byte to destination
```

字符串通常被组合为字符数目可变的字符串。表示一个字符串的方式有三种选择：1) 保留字符串的第一个位置用于给出字符串的长度；2) 附加一个带有字符串长度的变量（如在结构体中）；3) 字符串最后的位置用一个字符来标识其结尾。C 语言使用第三种选择，用一个值为 0 (ASCII 码中的 null) 的字节来结束字符串。所以，字符串“Cal”在 C 中用 4 字节表示，用十进制表示分别为：67、97、108、0。（下面即将看到，Java 采用第一种表示方法。）

107

01 例题·通过编译一个字符串复制过程，来展示如何使用 C 字符串

strcpy 过程将 C 语言中约定使用 null 字节结束的字符串 y 复制到字符串 x：

```
void strcpy (char x[], char y[])
{
    int i;

    i = 0;
    while ((x[i] = y[i]) != '\0') /* copy & test byte */
        i += 1;
}
```

编译后的 MIPS 汇编代码是什么？

01 答案

下面是基本的 MIPS 汇编代码段。假定数组 x 和 y 的基地址在 \$a0 和 \$a1 中，而 i 在 \$s0 中。strcpy 调整栈指针然后将保存的寄存器 \$s0 保存在栈中。

```
strcpy:
    addi   $sp,$sp,-4  # adjust stack for 1 more item
    sw    $s0, 0($sp)  # save $s0
```

为了将 i 初始化为 0，下一条指令通过对 0 和 0 做加法并将和放到 \$s0 中的方法将 \$s0 置为 0：

```
add   $s0,$zero,$zero # i = 0 + 0
```

这是循环的开始。y [i] 地址的形成是通过把 i 加到 y [] 上：

```
L1: add   $t1,$s0,$a1 # address of y[i] in $t1
```

注意我们不必将 i 乘以 4，因为 y 是字节的数组而非字的数组，和前面的例子一样。

为了读取 y [i] 中的字符，我们使用无符号字节读取指令，将字符放入 \$t2 中：

```
lbu   $t2, 0($t1) # $t2 = y[i]
```

采用类似的计算方式将 x [i] 的地址放在 \$t3 中，然后将 \$t2 中的字符保存到该地址中。

```
add   $t3,$s0,$a0  # address of x[i] in $t3
sb   $t2, 0($t3)  # x[i] = y[i]
```

接下来，如果字符是 0 则退出循环。也就是说，如果它是字符串的最后一个字符则退出：

```
beq   $t2,$zero,L2 # if y[i] == 0, go to L2
```

如果不是，将 i 加 1 继续循环：

```
addi  $s0, $s0,1   # i = i + 1
j     L1           # go to L1
```

如果不继续循环，那就是到了字符串的最后一个字符，我们还原 \$s0 和栈指针，然后返回。

108

```

L2: lw      $s0, 0($sp) # y[i] == 0: end of string.
      # Restore old $s0
      addi   $sp,$sp,4   # pop 1 word off stack
      jr    $ra           # return

```

在 C 中字符串复制通常使用指针而不是数组，从而避免上面代码中对 i 的操作。详见 2.14 节数组和指针对比的相关解释。□

由于 strcpy 是一个叶过程，编译器可以把 i 放在临时寄存器中以避免对 \$s0 进行保存和恢复。因此，我们可以不把 \$t 寄存器用做临时寄存器，而是将其用作被调用者可以方便使用的寄存器。当编译器遇到一个叶过程时，它会在用完所有临时寄存器之后，才使用那些必须保存的寄存器。

Java 中的字符和字符串

Unicode 是大多数人类语言中字母的通用编码。图 2-16 是一个 Unicode 字母表的示例，Unicode 中字母数和 ASCII 编码中有用的字符数一样多。为了更有包容性，Java 对字符使用 Unicode，它默认使用 16 位来表示一个字符。
109

Latin	Malayalam	Tagbanwa	General Punctuation
Greek	Sinhala	Khmer	Spacing Modifier Letters
Cyrillic	Thai	Mongolian	Currency Symbols
Armenian	Lao	Limbu	Combining Diacritical Marks
Hebrew	Tibetan	Tai Le	Combining Marks for Symbols
Arabic	Myanmar	Kangxi Radicals	Superscripts and Subscripts
Syriac	Georgian	Hiragana	Number Forms
Thaana	Hangul Jamo	Katakana	Mathematical Operators
Devanagari	Ethiopic	Bopomofo	Mathematical Alphanumeric Symbols
Bengali	Cherokee	Kanbun	Braille Patterns
Gurmukhi	Unified Canadian Aboriginal Syllabic	Shavian	Optical Character Recognition
Gujarati	Ogham	Osmanya	Byzantine Musical Symbols
Oriya	Runic	Cypriot Syllabary	Musical Symbols
Tamil	Tagalog	Tai Xuan Jing Symbols	Arrows
Telugu	Hanunoo	Yijing Hexagram Symbols	Box Drawing
Kannada	Buhid	Aegean Numbers	Geometric Shapes

图 2-16 Unicode 字母表示例。Unicode 4.0 版本有超过 160 个“块”，每个块是一个符号集的名字，且是 16 的整数倍。例如，希腊字符（Greek）从 0370₁₆ 开始，西里尔字符（Cyrillic）从 0400₁₆ 开始。前三列以 Unicode 的数字顺序粗略地列出了 48 个块对应的 48 种人类语言。最后一列中的 16 个块是多种语言，并没有按照顺序排列。默认的是 16 位编码，称为 UTF-16。一种称为 UTF-8 的变长编码，将 ASCII 子集保持为 8 位，其余字符用 16 或 32 位来表示。UTF-32 使用 32 位表示一个字符。更多内容请参见 www.unicode.org

MIPS 指令集包含显式的读取和存储 16 位半字（halfword）的指令。读取半字指令 lh (load half) 从存储器中读出一个半字，然后将其放在寄存器的最右边 16 位。与读取字节类似，读取半字指令 lh 也将半字看作有符号数并进行符号扩展，以填充寄存器左侧的 16 位。而无符号读取半字指令 lhu (load halfword unsigned) 将半字看作无符号数，与 lh 相比，这条指令更加常用。存储半字指令 sh (store half) 将寄存器最右边的 16 位写入存储器。我们按照下面的序列来复制半字：

```

lhu $t0,0($sp) # Read halfword (16 bits) from source
sh $t0,0($gp)  # Write halfword (16 bits) to destination

```

字符串是一个标准的 Java 类，它对连接、比较、转换的方法提供了专门的内建支持和预定义方法。与 C 不同的是，Java 包含一个字来给出字符串长度，这和 Java 数组相似。

110

01 精解 MIPS 软件试图保持栈和字地址的对齐，这样就允许程序总是使用 `lw` 和 `sw`（要求必须是对齐的）来访问栈。这一约定意味着一个 `char` 类型变量在栈中被分配 4 字节，尽管它并不需要这么多。然而，一个 C 字符串变量或一个字节数组会把每 4 字节压缩为 1 个字，而一个 Java 字符串变量或 `short` 类型数组会把每 2 个半字压缩为 1 个字。

01 精解 为了反映 web 的全球性特征，当今的大部分 web 页面采用 Unicode，而非 ASCII。

01 小测验

I. 下面关于 C 和 Java 中字符和字符串的陈述哪些是正确的？

1. C 中一个字符串占用的内存是 Java 中同样字符串的一半。
2. C 和 Java 中字符串只是一个一维字符数组的非正规名字。
3. C 和 Java 中采用 `null` (0) 来标记字符串的结尾。
4. 对字符串的操作，例如求长度，在 C 中比在 Java 中更快。

II. 下面哪种类型的变量存放 $1\ 000\ 000\ 000_{10}$ 占用的内存空间最大？

1. C 语言的 `int`
2. C 语言的 `string`
3. Java 的 `string`

2.10 MIPS 中 32 位立即数和寻址

虽然保持所有 MIPS 指令为 32 位长简化了硬件，但有时使用 32 位常量或 32 位地址更加方便。本节先介绍使用较大常量的一般解决方法，然后描述了用于分支和跳转指令寻址的优化措施。

111

2.10.1 32 位立即数

尽管常数往往比较短而且适于 16 位字段，但有时它们会更大。MIPS 指令集中的读取立即数高位指令 `lui` (load upper immediate) 专门用于设置寄存器中常数的高 16 位，允许后续指令设置常数的低 16 位。图 2-17 描述了 `lui` 的操作。

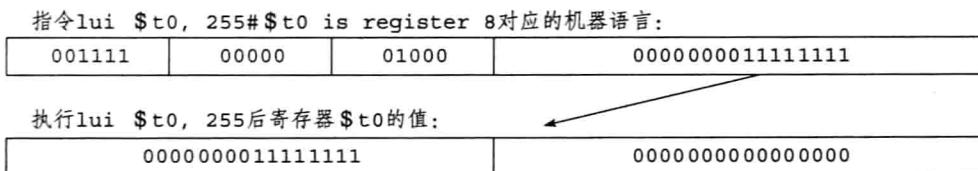


图 2-17 `lui` 指令的效果。`lui` 指令将 16 位立即数常量存放到寄存器的高 16 位，低 16 位用 0 填充

01 例题·加载 32 位常量

加载下面这个 32 位常量到寄存器 `$s0` 的 MIPS 汇编代码是什么？

0000 0000 0011 1101 0000 1001 0000 0000

01 答案

首先，我们使用命令 `lui` 加载高 16 位，十进制表示是 61：

`lui $s0, 61 # 61 decimal = 0000 0000 0011 1101 binary`

执行上面的指令后，寄存器 \$s0 的值为

0000 0000 0011 1101 0000 0000 0000 0000

下一步是插入低 16 位，十进制表示是 2304：

ori \$s0, \$s0, 2304 # 2304 decimal = 0000 1001 0000 0000

寄存器 \$s0 中的最终值就是所需要的值：

0000 0000 0011 1101 0000 1001 0000 0000

112

□

01 硬件/软件接口 编译器或汇编程序必须把大的常数分解为若干小的常数，然后再合并到一个寄存器中。正如你想象的那样，立即数字段大小的限制，无论在取/存数指令中对存储器的地址还是在立即数指令中对常数都可能带来问题。如果这项工作由汇编程序来做，如 MIPS 软件，那么汇编程序必须有一个可用的临时寄存器来创建长整数值。这是给汇编程序保留 \$at 寄存器的一个原因。

因此，MIPS 机器语言的符号表示不再受到硬件限制，但仍受汇编程序构造者所选择包括的内容的限制（见 2.12 节）。我们以靠近硬件层的方式解释计算机的体系结构，需要注意的是，我们所使用汇编程序的增强扩展语言，在实际处理器中是不存在的。

01 精解 构造 32 位常数时必须小心。指令 addi 将指令最左边的 16 位立即数字段复制到一个字的高 16 位中。2.6 节的立即数逻辑或操作（logical or immediate）把 0 读到高 16 位中，所以可被汇编程序用于和 lui 一起创建 32 位常数。

2.10.2 分支和跳转中的寻址

MIPS 跳转指令寻址采用最简单的寻址方式。它们使用最后一种 MIPS 指令格式，称为 J 型。J 型除了 6 位操作码之外，其余位都是地址字段。所以

j 10000 # go to location 10000

可以汇编为下面的格式（实际中要更加复杂一些，正如我们后面将看到的那样）：

2	10000
6位	26位

其中跳转操作码的值为 2，跳转地址为 10000。

和跳转指令不同，条件分支指令除了规定分支地址之外还必须指定两个操作数。因此

bne \$s0,\$s1,Exit # go to Exit if \$s0 ≠ \$s1

被汇编为下面的指令，只保留了 16 位用于指定分支地址：

5	16	17	Exit
6位	5位	5位	16位

如果让程序地址适应该 16 位字段，则意味着任何程序都不能大于 2^{16} ，这在今天来说太小，因此是一种很不现实的选择。另一个可选的办法是指定一个总是加到分支地址上的寄存器，这样分支指令的地址可按如下方式计算：

$$\text{程序计数器} = \text{寄存器} + \text{分支地址}$$

这个求和结果允许程序的大小达到 2^{32} ，并且仍能使用条件分支，从而解决了分支地址大小的问题。随之而来的问题是使用哪个寄存器呢？

答案取决于条件分支是如何使用的。条件分支在循环和 if 语句中都可以找到，它们倾向于转到附近的指令。例如，在 SPEC 基准测试程序中，大概一半条件分支的跳转距离小于 16 条指令。因为程序计数器（Program Counter, PC）包含当前指令的地址，如果我们使用 PC 来作为

增加地址的寄存器，我们可转移到离当前指令距离为 $\pm 2^{15}$ 个字的地方。几乎所有循环和if语句都远远小于 2^{16} 个字，因此PC是一个理想的选择。

这种分支寻址形式称为PC相对寻址(PC-relative addressing)。正如在第4章中将会看到的那样，提前递增PC来指向下一条指令会对硬件带来很多方便。所以，MIPS寻址实际上是相对于下一条指令的地址(PC+4)，而不是相对于当前指令(PC)。寻址附近的指令是加速大概率事件的另外一个例子。

② PC相对寻址：一种寻址方式，它将PC和指令中的常数相加作为寻址结果。

像近期的大多数计算机一样，MIPS对所有条件分支使用PC相对寻址，因为这些指令的跳转目标一般都比较接近其分支地址。另一方面，跳转链接指令并非总是靠近调用者的过程，所以它们通常使用其他寻址方式。因此，MIPS体系结构通过使用跳转和跳转链接指令的J型格式来为过程调用提供长地址。

因为所有MIPS指令都是4字节长，所以在PC相对寻址时所加的地址被设计为字地址而不是字节地址。相对于16位的字节地址，16位的字地址跳转范围扩大了4倍。同样，跳转指令的26位字段也是字地址，它可以表示28位的字节地址。

01 精解 因为PC是32位，所以有4位必须来自于跳转指令之外的其他地方。MIPS跳转指令仅仅代替PC的低28位，而高4位保持不变。装载器和链接器(见2.12节)必须十分小心以避免程序超过256MB的寻址界限(6400万条指令)；否则，该跳转必须替换为寄存器跳转指令，并在执行前使用其他指令将完整的32位地址加载到一个寄存器中。

114

① 例题·在机器语言中描述分支偏移

假设2.7.1节的while循环语句被编译成下面的MIPS汇编代码：

```
Loop: sll $t1,$s3,2      # Temp reg $t1 = 4 * i
    add $t1,$t1,$s6      # $t1 = address of save[i]
    lw   $t0,0($t1)       # Temp reg $t0 = save[i]
    bne $t0,$s5, Exit    # go to Exit if save[i] ≠ k
    addi $s3,$s3,1        # i = i + 1
    j    Loop             # go to Loop
Exit:
```

如果我们假设把loop的开始位置放在内存的80 000处，那么该循环的MIPS机器代码是什么呢？

① 答案

汇编指令和它们的地址如下：

80000	0	0	19	9	2	0
80004	0	9	22	9	0	32
80008	35	9	8		0	
80012	5	8	21		2	
80016	8	19	19		1	
80020	2			20000		
80024	...					

注意MIPS指令使用字节寻址，所以相邻字的地址相差4，即一个字中的字节的数量。第4行的bne指令将2个字或是8字节加到下一条指令地址(80016)上，使用相对下一条指令的偏移($8 + 80016$)指明跳转目标，而不是使用相对该分支指令的偏移($12 + 80012$)，也不是使用完整的目的地址(80024)。最后一行的跳转指令采用完整的地址($20000 \times 4 = 80000$)，

115 对应于 Loop 标签。 □

01 硬件/软件接口 大多数条件分支都转移到一个附近的位置，但有时也会转移很远，距离超过条件分支指令的 16 位可以表示的范围。汇编器的解决方法就像处理对大地址或大常数的方法一样：插入一个跳转到分支目标的无条件跳转，并将条件取反以便由分支决定是否跳过该无条件跳转指令。

01 例题·远距离的分支转移

假设在寄存器 \$s0 与寄存器 \$s1 值相等时需要跳转，可以使用如下指令：

beq \$s0, \$s1, L1

用两条指令替换上面的指令，以获得更远的转移距离。

01 答案

可用下面的指令替换短地址的条件分支指令：

bne \$s0, \$s1, L2

j L1

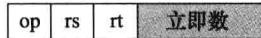
L2:

□

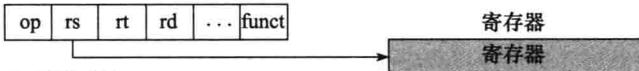
2.10.3 MIPS 寻址模式总结

多种不同的寻址形式一般统称为寻址模式（addressing mode），图 2-18 给出了每种寻址模式的操作数如何识别。MIPS 寻址模式如下所示：

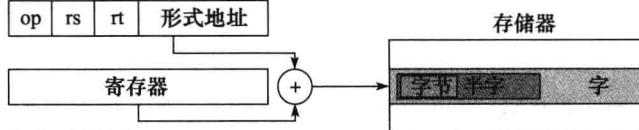
1. 立即数寻址



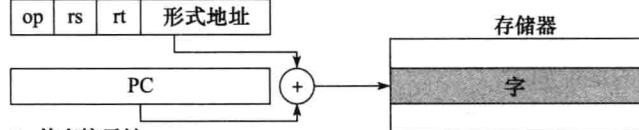
2. 寄存器寻址



3. 基址寻址



4. PC 相对寻址



5. 伪直接寻址

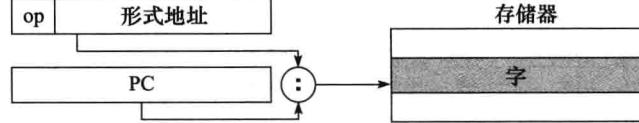


图 2-18 MIPS 5 种寻址模式的说明。阴影部分为操作数。模式 3 的操作数在内存中，而模式 2 的操作数是寄存器。注意，读数和存数对字节、半字或字有多种版本。模式 1 的操作数是指令自身的 16 位字段。模式 4 和模式 5 寻址的指令在内存中，模式 4 把 16 位地址左移 2 位与 PC 相加，而模式 5 把 26 位地址左移 2 位与 PC 计数器的高 4 位相连。注意，一种操作可能可以使用多种寻址模式，例如，加法可以使用立即数寻址（addi）和寄存器寻址（add）。

② 寻址模式：根据对操作数和/或地址的使用不同加以区分的多种寻址方式中的一种。

- 1) 立即数寻址 (immediate addressing)，操作数是位于指令自身中的常数。
- 2) 寄存器寻址 (register addressing)，操作数是寄存器。
- 3) 基址寻址 (base addressing) 或偏移寻址 (displacement addressing)，操作数在内存中，其地址是指令中基址寄存器和常数的和。
- 4) PC 相对寻址 (PC-relative addressing)，地址是 PC 和指令中常数的和。
- 5) 伪直接寻址 (pseudodirect addressing)，跳转地址由指令中 26 位字段和 PC 高位相连而成。

116

01 硬件/软件接口 虽然我们把 MIPS 系统结构按 32 位地址描述，但是几乎所有的微处理器（包括 MIPS）都能进行 64 位地址扩展（见附录 E 和 2.18 节）。这些扩展主要是针对大型程序的需要。指令集的扩展使得体系结构发展的同时，保持软件和下一代体系结构的向上兼容性。

117

2.10.4 机器语言解码

有时候必须通过逆向工程将机器语言恢复到最初的汇编语言，比如检查“核心转储”(core dump)时。图 2-19 描述了 MIPS 机器语言对各个字段的编码。该图可用于汇编语言和机器语言之间的手动翻译。

01 例题·机器码解码

下面这条机器指令对应的汇编语言语句是什么？

00af8020hex

01 答案

第一步是将十六进制转换到二进制，以便找到操作码字段：

(Bits: 31 28 26	5 2 0)
0000 0000 1010 1111 1000 0000 0010 0000	

我们查看操作码字段来决定指令的操作类型。参照图 2-19，当 31~29 位是 000 且 28~26 位也是 000 时，它是 R 型指令。参照图 2-20，将该二进制指令按照 R 型指令字段重新排列：

op	rs	rt	rd	shamt	funct
000000	00101	01111	10000	00000	100000

op(31:26)

28~26 31~29	0(000)	1(101)	2(010)	3(011)	4(100)	5(101)	6(110)	7(111)
0(000)	R 型	Bltz/gez	跳转	跳转并链接	分支 eq	分支 ne	blez	bgtz
1(001)	立即数加法	addiu	小于立即数置位	小于无符号立即数时置位	andi	ori	xori	取立即数高位
2(010)	TLB	FIpt						

图 2-19 MIPS 指令解码。该标记根据行和列确定字段的值。例如，图的顶部在第 4 行（指令的第 31~29 位为 100_2 ）第 3 列（指令的第 28~26 位为 011_2 ）描述了取字指令，因此相应操作码字段（第 31~26 位）的 (R 型) 值是 100011_2 。下划线表示该字段在其他地方被使用。例如，第 0 行第 0 列 ($op = 000000_2$) 的 R 型在图的底部定义。因此，底部第 4 行第 2 列的 subtract 意味着指令 funct 字段（第 5~0 位）是 100010_2 而操作码字段（第 31~26 位）是 000000_2 。第 2 行第 1 列的 FIpt 在第三章的图 3-18 中定义。Bltz/gez 是附录 B 中 4 条指令的操作码：bltz、bgez、bltzal 和 bgezal。附录 A 涵盖所有的指令

op(31:26)								
3(011)								
4(100)	取字节	取半字	lw1	取字	取无符号字节	取无符号半字	lwr	
5(101)	存字节	存半字	sw1	存字			swr	
6(110)	取链接字	lwc1						
7(111)	存条件字	swc1						

op(31:26) = 010000(TLB), rs(25:21)								
23 ~ 21 25 ~ 24	0(000)	1(001)	2(010)	3(011)	4(100)	5(101)	6(110)	7(111)
0(00)	mfc0		cfc0		mtc0		ctc0	
1(01)								
2(10)								
3(11)								

op(31:26) = 000000(R型), funct(5:0)								
2 ~ 0 5 ~ 3	0(000)	1(001)	2(010)	3(011)	4(100)	5(101)	6(110)	7(111)
0(000)	逻辑左移		逻辑右移	sra	sllv		srlv	sraw
1(001)	jump register	jalr			syscall	break		
2(010)	mfhi	mthi	mflo	mtlo				
3(011)	mult	multu	div	divu				
4(100)	add	addu	subtract	subu	and	or	xor	not or(nor)
5(101)			set l.t.	set l.t. 无符号操作				
6(110)								
7(111)								

图 2-19 (续)

名称	字段						备注
字段大小	6 位	5 位	5 位	5 位	5 位	6 位	所有 MIPS 指令都是 32 位
R 型	op	rs	rt	rd	shamt	funct	算术指令型
I 型	op	rs	rt	地址/立即数			传输、分支和立即数型
J 型	op	目标地址					跳转指令型

图 2-20 MIPS 指令的格式

图 2-19 的底部确定了 R 型指令的操作。在本例中，5~3 位是 100，2~0 位是 000，因此该二进制指令为 add 指令。

下面我们通过查找字段值来解码指令的剩余部分。rs 字段的十进制值是 5，rt 是 15，rd 是 16（shamt 未使用）。图 2-14 说明这些数字表示寄存器 \$a1、\$t7 和 \$s0。现在可以给出转换后的汇编指令：

```
add $s0,$a1,$t7
```

图 2-20 给出了所有 MIPS 指令的格式。第 2.2 节的图 2-1 汇总了本章出现的所有汇编指令。其他 MIPS 指令主要处理算术运算和实数，将在第 3 章介绍。□

01 小测验

- I. 在 MIPS 中条件分支的地址范围 ($K = 1024$) 是多大?
1. 地址在 $0 \sim 64K - 1$ 之间
 2. 地址在 $0 \sim 256K - 1$ 之间
 3. 分支前后地址范围各大约 $32K$
 4. 分支前后地址范围各大约 $128K$
- II. 在 MIPS 中跳转和跳转链接指令的地址范围 ($M = 1024K$) 是多大?
1. 地址在 $0 \sim 64M - 1$ 之间
 2. 地址在 $0 \sim 256M - 1$ 之间
 3. 分支前后地址范围各大约 $32M$
 4. 分支前后地址范围各大约 $128M$
 5. 由 PC 提供高 6 位地址的 $64M$ 大小的块中任意地址
 6. 由 PC 提供高 4 位地址的 $256M$ 大小的块中任意地址
- III. 机器指令 $0000\ 0000_{16}$ 对应的 MIPS 汇编语言指令是什么?
1. j
 2. R 型
 3. addi
 4. sll
 5. mfc0
 6. 未定义的操作码：没有对应 0 的合法指令

118

120

2.11 并行与指令：同步

当任务之间相互独立的时候，任务的并行执行是比较容易的。但往往任务之间需要相互协作，这种协作通常意味着某些任务写的结果是其他任务需要读取的值。这时执行读任务的一方要知道写任务什么时候完成了写操作，才能安全地读回数据。就是说，任务之间需要同步 (synchronize)，否则就有发生数据竞争 (data race) 的危险，导致读数据错误而引起程序运行结果的改变。

数据竞争：假如来自不同线程的两个访存请求访问同一个地址，它们连续出现，并且至少其中一个是一个写操作，那么这两个存储访问形成数据竞争。

例如，回忆第 1 章 1.8 节所提到的 8 个记者共同写作一个故事的例子。假设一个记者要写总结，他要阅读所有之前的章节。因此，他必须知道其他记者什么时候可以完成各自的章节，然后他再撰写总结，这样他就不用担心写好总结后其他记者再对各自章节进行修改。所以，他们就需要很好地同步各个章节撰写和阅读的过程，这样总结才能和前面章节中所写的内容相一致。

在计算中，同步机制要依赖硬件提供的同步指令，这些指令可由用户调用。本节我们重点讨论加锁 (lock) 和解锁 (unlock) 同步操作的实现。采用加锁和解锁可以直接创立一个仅允许单个处理器操作的区域，叫作互斥 (mutual exclusion) 区。更复杂的同步机制实现也与此类似。

在多处理器中实现同步需要一组硬件原语，提供对存储单元进行原子读和原子写的能力，使得在进行存储器原子读或原子写操作时任何其他操作都不得插入。如果没有这样的硬件原语，那么建立同步机制的代价将会变得很高，并且随着处理器数量的增加情况将更为恶化。

建立基本硬件原语有若干可选的方案，这些方案都可以实现原子读和原子写的功能，并能

用某种方法表示这些操作是否为原子操作。通常，体系结构设计人员并不希望基本硬件原语被用户使用，而是希望这些原语被系统程序员用来建立同步库，建立同步库的过程通常很复杂且难度较大。

我们用原子交换原语（atomic exchange 或 atomic swap）来演示如何建立基本同步机制。这个原语是将寄存器中的一个值和存储器中的一个值相互交换。

为了展示该原语建立同步原理的基本过程，假定使用存储器中某个单元来表示一个锁变量：其数值为 0 时表示解锁，为 1 时表示加锁。一个处理器尝试对锁单元加锁，方法是用一个寄存器中的 1 与该锁单元的值进行交换。交换以后该锁单元的新值为 1，返回值（锁单元的原值）如果是 1，表明这个锁已被其他处理器占用；否则返回值为 0，表示锁是自由的，尝试加锁成功。此时锁单元已被修改成 1，以防止任何其他处理器再来占用。
121

例如，考虑有两个处理器同时尝试进行交换操作，它们的竞争关系就会被破坏。因为其中只能有一个处理器先执行交换操作，并且返回 0。那么第二个处理器执行完交换操作的时候返回值就变成了 1。用交换原语实现同步的关键是操作的原子性：交换操作是不可分割的，并且由硬件对两个同时执行的交换操作进行排序。有可能两个处理器同时尝试置位同步变量，但这两个处理器认为它们同时成功设置了同步变量是不可能的。

实现单个的原子存储器操作给处理器的设计者带来了若干挑战，因为这要求存储器的读、写操作都是有单条不可被中断的指令完成。

一种可行的方法是采用指令对，其中第二条指令返回一个表明这对指令是否原子执行的标志值。假如处理器的操作都是在这对指令之前或之后执行，这对指令就是原子的。因此，当一个指令对是原子的，没有哪个处理器能改变这两个指令执行之间的数据值。

在 MIPS 处理器中这一指令对包括一条叫作链接取数（load linked）的特殊取数指令和一条叫作条件存数（store conditional）的特殊存数指令。我们顺序地使用这两条指令：如果链接取数指令所指定的锁单元的内容在相同地址的条件存数指令执行前已被改变，那么条件存数指令就执行失败。我们定义条件存数指令完成以下功能：保存寄存器的值，并且如果执行成功则将寄存器的值修改为 1，如果失败则修改为 0。因为链接取数指令返回锁单元的原始值，条件存数指令执行成功的时候才返回 1，下面的指令序列实现了存储器单元的原子交换。存储器单元的地址由 \$s1 中的值指出。

```
again: addi $t0,$zero,1      ;copy locked value
      li      $t1,0($s1)    ;load linked
      sc      $t0,0($s1)    ;store conditional
      beq    $t0,$zero,again ;branch if store fails
      add    $s4,$zero,$t1    ;put load value in $s4
```

在 `li` 和 `sc` 两条指令之间的任何时候有处理器插入，并修改了该锁单元的值，指令 `sc` 都会将 `$t0` 置为 0，引起这段指令序列重新执行。在指令序列的最后，寄存器 `$s4` 中的值和 `$s1` 指向的锁单元的值发生了原子交换。

01 精解 尽管我们讲述的同步是在多处理器系统中的，但是原子操作对于单个处理器上运行的操作系统在处理多个进程时也是十分有用的。在单处理器中，为了保证执行不被任何事件所干扰，条件存数指令在处理器两条指令之间进行上下文切换（context switch）时也会失败（见第 5 章）。
122

链接取数/条件存数机制的优点是：可以通过它们来构造其他的诸如原子比较和交换（atomic compare and swap）或者原子取后加（atomic fetch-and-increment）等同步原语。这些同步原语可以被用在一些并行编程模型中。这些同步原语的实现需要在 `li` 指令和 `sc` 指令之间插入更多的指令，但不需要太多。

因为在链接取数指令执行之后，任何试图修改锁单元值的操作或者任何异常都将导致条件存数指令执行失败，所以在选择 `ii` 和 `sc` 之间的指令时就要格外注意。特别需要注意的是，允许使用的并且不会造成问题的只有寄存器 - 寄存器指令，而处理器可能由于重复的页错误而导致始终无法完成 `sc` 指令，从而使处理器处于一种死锁的状态。另外，链接取数和条件存数之间的指令数一定要尽可能少，这样才可以减少不相关的事件或者竞争资源的处理器所引起条件存数指令执行失败的频率。

01 小测验

什么时候才会用到像链接取数（load linked）和条件存数（store conditional）这样的原语？

- 当一个并行程序中相互协作的线程需要同步以获得对共享数据的正确的读写行为时
- 当运行在单处理器上的相互协作的处理过程需要同步以获得对共享数据的正确的读写行为时

2.12 翻译并执行程序

本节描述了将存储在硬盘文件中的 C 程序转换为可执行程序的 4 个步骤，图 2-21 所示是语言翻译的层次。尽管某些系统可能合并部分步骤以减少转换时间，但从逻辑上讲，这 4 个步骤是程序转换流程所必经的 4 个阶段。本节将根据这种翻译层次进行描述。

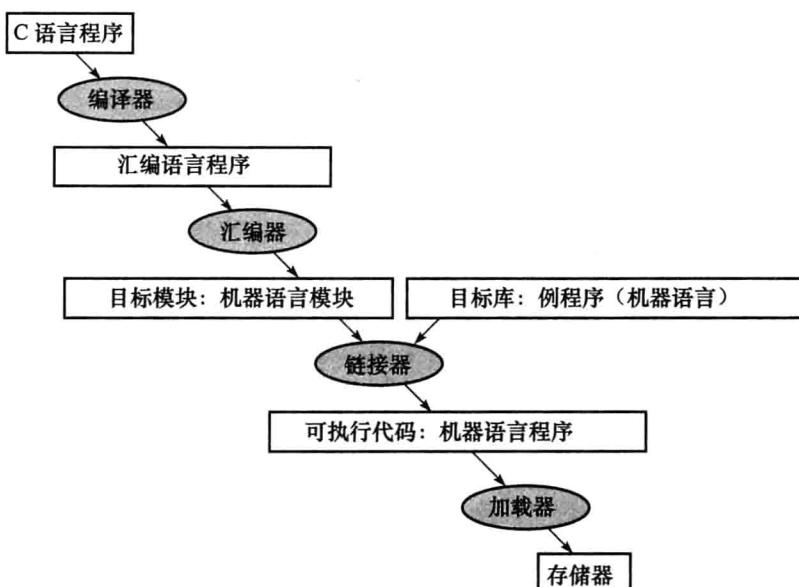


图 2-21 C 语言的翻译层次。用高级语言编写的程序首先需要被编译成为汇编语言，然后被汇编成机器语言组成的目标模块。链接器将多个模块和库程序组合在一起解析所有的引用。加载器将可执行程序加载到内存的适当位置，然后处理器就可以执行了。为了加快翻译的速度，某些步骤被跳过或和其他步骤组合在一起。一些编译器直接产生目标模块，一些系统使用带链接功能的加载器直接完成后面两步。为了确定文件的类型，UNIX 使用文件的后缀，`x.c` 代表 C 源文件，`x.s` 表示汇编文件，`x.o` 表示目标文件，`x.a` 表示静态链接库，`x.so` 表示动态链接库，默认情况下，`a.out` 表示可执行文件。MS-DOS 使用后缀 `.C, .ASM, .OBJ, .LIB, .DLL` 和 `.EXE` 来完成同样的功能。

2.12.1 编译器

编译器将 C 程序转换成一种机器能理解的符号形式的汇编语言程序（assembly language）

program)。高级语言编写的程序比使用汇编语言编写的代码少得多，所以程序员效率更高。

1975 年，因为存储器容量较小并且编译器效率不高，所以许多操作系统和汇编器都用汇编语言 (assembly language) 编写。如今单 DRAM 芯片容量增长 500 000 倍，减轻了人们对程序大小的关注，并且今天优化的编译器能够产生出几乎与一个汇编语言专家所写的程序一样好的汇编程序，对于大型程序有时甚至效果更好。

● 汇编语言：一种符号语言，能被翻译成二进制的机器语言。

2.12.2 汇编器

因为汇编语言对于高层次软件是一个接口，所以汇编器也能够处理一些机器语言指令的常见变种，就像这些变种是它自己的指令一样。硬件不需要实现这些指令，然而它们在汇编语言中的存在简化了程序转换和编程。这类指令称为伪指令 (pseudoinstruction)。

● 伪指令：汇编语言指令的一个变种，通常被看作一条汇编指令。

如前所述，MIPS 硬件确保寄存器 \$zero 保持 0 值。即一旦使用寄存器 \$zero，它都提供 0，而且程序员不能修改寄存器 \$zero 的值。寄存器 \$zero 用于生成汇编语言指令 move，move 的功能是将一个寄存器中的内容复制到另一个中。因此即使 MIPS 体系结构中不存在这条指令，MIPS 汇编器也能够识别它：

```
move $t0,$t1      # register $t0 gets register $t1
```

汇编器将这条汇编语言指令转换成功能等价的如下机器语言指令：

```
add $t0,$zero,$t1 # register $t0 gets 0 + register $t1
```

在 2.7.1 节的例子中提到，MIPS 汇编器将 blt (branch on less than，小于则分支) 转换成两条指令：slt 和 bne。其他例子包括 bgt、bge 和 ble。它也将一个到远距离的分支指令拆成一个分支指令和一个跳转指令。如前所述，MIPS 汇编器允许将 32 位常量加载到一个寄存器中，不用考虑立即数指令的 16 位限制。

总的来说，伪指令使 MIPS 拥有比硬件所实现的更为丰富的汇编语言指令集。唯一的代价是保留了一个由汇编器使用的寄存器 \$at。如果你打算写汇编程序，请使用伪指令来简化你的任务。为了理解 MIPS 体系结构并保证获得最好的性能，可以学习图 2-1 和图 2-19 中真正的 MIPS 指令。

汇编器同样接受不同基数的数字。除了二进制和十进制，它们通常还使用比二进制更为紧凑而又容易转化为位模式的基数。MIPS 汇编器使用十六进制。

这种特性相当方便，但是汇编器的主要任务是汇编成机器代码。汇编器将汇编语言程序转换成目标文件 (object file)，它包括机器语言指令、数据和指令正确放入内存所需要的信息。

为了产生汇编语言程序中每条指令对应的二进制表示，汇编器必须处理所有标号对应的地址。汇编器将分支和数据传输指令中用到的标号都放入一个符号表 (symbol table) 中。正如你所想的，这个表由标号和地址成对构成。

● 符号表：一个用来匹配标记名和指令所在内存字的地址的列表。

UNIX 系统中的目标文件通常包含以下 6 个不同的部分：

- 目标文件头，描述目标文件其他部分的大小和位置。
- 代码段，包含机器语言代码。
- 静态数据段，包含在程序生命周期内分配的数据。（UNIX 系统允许程序使用静态数据，它

存在于整个程序中；也允许使用动态数据，它随程序的需要而增长或缩小。见图 2-13。)

- 重定位信息，标记了一些在程序加载进内存时依赖于绝对地址的指令和数据。
- 符号表，包含未定义的剩余标记，如外部引用。
- 调试信息，包含一份说明目标模块如何编译的简明描述，这样，调试器能够将机器指令关联到 C 源文件，并使数据结构也变得可读。

下一小节描述了如何链接已经汇编完成的子程序，如库程序。

2.12.3 链接器

到目前为止我们所描述的内容表明，对于源程序任意一行代码的修改都需要重新编译和汇编整个程序。全部重新翻译是对计算资源的严重浪费。这种重复对于标准库程序尤为浪费，因为程序员要编译和汇编那些在定义上几乎从未改变过的过程。另一种方法是单独编译和汇编每个过程，以使得某一行代码的改变只需要编译和汇编一个过程。这种方法需要一个新的系统程序，称为链接编辑器或（link editor）链接器（linker），它把所有独立汇编的机器语言程序“拼接”在一起。

- 链接器：也称链接编辑器。它是一个系统程序，把各个独立汇编的机器语言程序组合起来并且解决所有未定义的标记，最后生成可执行文件。

链接器的工作分 3 个步骤：

- 1) 将代码和数据模块象象征性地放入内存。
- 2) 决定数据和指令标签的地址。
- 3) 修补内部和外部引用。

链接器使用每个目标模块中的重定位信息和符号表，来解析所有未定义标签。这种引用发生在分支指令、跳转指令和数据寻址处，所以这个程序的工作非常像一个编辑器：它寻找所有旧地址并用新地址取代它们。编辑是“链接编辑器”或链接器名字的简称。采用链接器的原因是修补代码比重新编译和汇编要快得多。

如果所有外部引用都解析完，链接器接着决定每个模块将要占用的内存位置。回忆 2.8.4 节的图 2-13，它描述了 MIPS 在内存中为程序和数据分配空间的方式。因为文件是单独汇编的，所以汇编器不可能知道该模块的指令和数据相对于其他模块而言将会被放到哪里。当链接器将一个模块放到内存中的时候，所有绝对引用（absolute reference），即与寄存器无关的内存地址必须重定位以反映它的真实地址。

链接器产生一个可执行文件（executable file），它可以在一台计算机上运行。通常，这个文件与目标文件具有相同的格式，但是它不包含未解决的引用。具有部分链接的文件是可能的，如库程序，在目标文件中仍含有未解决的地址。

- 可执行文件：一个具有目标文件格式的功能程序，不包含未解决的引用。它可以包含符号表和调试信息。“剥离的可执行程序”不包含这些信息，可能包含加载器所需的重定位信息。

例题·目标文件的链接

将下面的两个目标文件链接。给出最终可执行文件中前几条指令对应的更新过的地址。为了便于理解，我们使用汇编语言来表示指令，在实际文件中，这些指令由数字表示。

注意目标文件中，我们已将必须在链接进程中更新的地址和标记高亮显示了，分别是引用过程 A 和过程 B 的地址的指令，以及引用数据字 X 和 Y 的地址的指令。

目标文件头				
代码段	名字	过程 A		
	正文大小	100_{16}		
	数据大小	20_{16}		
数据段	地址	指令		
	0	<code>lw \$a0,0(\$gp)</code>		
	4	<code>jal 0</code>		
		
重定位信息地址	0	(X)		
		
符号表	地址	指令类型	依赖	
	0	<code>lw</code>	X	
	4	<code>jal</code>	B	
目标文件头	标记	地址		
	X	—		
	B	—		
代码段				
	名字	过程 B		
	正文大小	200_{16}		
数据段	数据大小	30_{16}		
	地址	指令		
	0	<code>sw \$a1,0(\$gp)</code>		
重定位信息地址	4	<code>jal 0</code>		
		
	0	(Y)		
		
符号表	地址	指令类型	依赖	
	0	<code>sw</code>	Y	
	4	<code>jal</code>	A	
目标文件头	标记	地址		
	Y	—		
	A	—		

127

01 答案

过程 A 需要找到 load 指令中标号为 X 的变量的地址和 jal 指令中过程 B 的地址。过程 B 需要找到 store 指令中标号为 Y 的变量的地址和 jal 指令中过程 A 的地址。

从 2.8.4 节的图 2-13 中，我们可以看到代码段从地址 $40\ 0000_{16}$ 开始而数据段从地址 $1000\ 0000_{16}$ 开始。过程 A 的正文被放置在第一个地址而它的数据被放置在第二个地址。过程 A 的目标文件头表明其代码段大小是 100_{16} 字节而数据段大小是 20_{16} 字节，这样过程 B 的代码段开始地址就是 $400\ 100_{16}$ ，数据段开始地址是 $1000\ 0020_{16}$ 。

可执行文件头			可执行文件头	
	正文大小	300_{16}		$0040\ 0104_{16}$
	数据大小	50_{16}		...
代码段	地址	指令	数据段	地址
	$0040\ 0000_{16}$	<code>lw \$a0,8000(\$gp)</code>		$1000\ 0000_{16}$
	$0040\ 0004_{16}$	<code>jal 40 0100</code>		...
...		$1000\ 0020_{16}$
	$0040\ 0100_{16}$	<code>sw \$a1,8020(\$gp)</code>		...

图 2-13 也表明了代码段的起始地址是 $40\ 0000_{16}$ ，数据段的起始地址是 $1000\ 0000_{16}$ 。过程 A 的正文被放置在第一个地址而它的数据被放置在第二个地址。过程 A 的目标文件头表明其代码段大小是 100_{16} 字节而数据段大小是 20_{16} 字节，这样过程 B 的代码段开始地址就是 400100_{16} ，数据段开始地址是 10000020_{16} 。[⊖]

现在链接器更新了指令的地址字段。它使用指令类型字段得到待编辑地址的格式。这里共有两种类型：

1) jal 类型比较简单。因为它们使用伪直接寻址。对于地址 $40\ 0004_{16}$ 处的 jal，其地址字段是 $40\ 0100_{16}$ （程序 B 的地址），而地址 $40\ 0104_{16}$ 处的 jal 的地址字段是 $40\ 0000_{16}$ （程序 A 的地址）。

2) 存取数指令对应的地址更为复杂，因为它们和基址寄存器有关。本例使用全局指针作为基址寄存器。图 2-13 表明 \$gp 的初始值为 10008000_{16} 。为了得到地址 10000000_{16} （字 X 的地址），我们设置位于地址 400000_{16} 处的 lw 的地址字段中为 8000_{16} 。同样，为了得到地址 10000020_{16} （字 Y 的地址），可以设置位于地址 400100_{16} 处的 sw 的地址字段中为 8020_{16} 。 □

128

01 精解 回忆前面讲过 MIPS 指令是按字对齐的。所以 jal 指令丢弃最右侧 2 位来增加指令寻址范围。这样，它就可以使用 26 位来产生一个 28 位的字节地址。因此，本例中 jal 指令的低 26 位存放的实际地址是 $10\ 0040_{16}$ ，而不是 $40\ 0100_{16}$ 。

2.12.4 加载器

现在可执行文件已经在磁盘中，操作系统可以将其读入内存并启动执行它。在 UNIX 系统中，加载器（loader）按照如下步骤工作：

- 1) 读取可执行文件头来确定代码段和数据段的大小。
- 2) 为正文和数据创建一个足够大的地址空间。
- 3) 将可执行文件中的指令和数据复制到内存中。
- 4) 把主程序的参数（如果存在）复制到栈顶。
- 5) 初始化机器寄存器，将栈指针指向第一个空位置。
- 6) 跳转到启动例程，它将参数复制到参数寄存器并且调用程序的 main 函数。当 main 函数返回时，启动例程通过系统调用 exit 终止程序。

加载器：把目标程序装载到内存中以准备运行的系统程序。

附录 A 中的 A.3 节和 A.4 节更加详细地描述了链接器和加载器。

2.12.5 动态链接库

事实上，计算机科学中的每个问题可以在其他层次上间接地解决。

——David Wheeler

本节的第一部分将描述程序运行前链接库文件的传统方法。尽管这种静态的方法是最快的调用库程序的办法，但它有以下缺点：

- 库程序成为可执行代码的一部分。这样如果发布新版本的库以修正一些错误或支持新的硬件设备，静态链接的程序中使用的还是旧版本。
- 在程序运行时，尽管可能不会使用库中的所有部分，但它们还是会全部加载进来。相对程序而言，库可能会很大，例如，标准的 C 库有 2.5MB。

[⊖] 原书中表格前后的文字除开头外一模一样。此处按原书翻译。——译者注

这些不足导致了动态链接库（dynamically linked library, DLL）的产生，也就是说，直到程序运行的时候，这些库例程才会被链接并加载。程序和库例程都会在非局部的过程和名字中保存额外的信息。在最初版本的 DLL 中，加载器调用一个动态链接器，使用文件中的额外信息来找到适当的库并且更新所有外部引用。

129 动态链接库：在程序执行过程中才被链接的库例程。

最初版本 DLL 的缺点是它仍链接库中所有在程序运行时可能调用的例程，而不是仅仅链接程序运行时实际调用的例程。由此产生 DLL 的晚过程链接（lazy procedure linkage）版本，该版本中每个例程只有在它被调用后才被链接。

就像这个领域中的许多创新一样，这个技巧采用了一种间接的方法。图 2-22 展示了该技术。它以一个非局部例程开始，该例程的末尾调用了一组虚例程，每个非局部例程都有一个人口。每个虚入口都包含一个间接跳转。

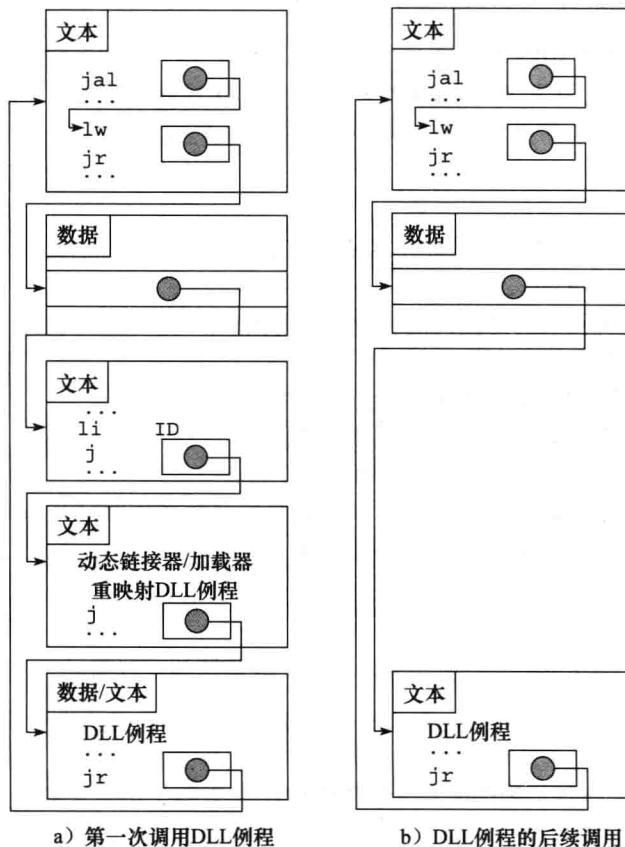


图 2-22 通过晚过程链接方式链接动态链接库。a) 第一次调用 DLL 的步骤；b) 在随后的调用中，查找例程、重映射例程和链接例程被跳过。我们将在第 5 章看到，操作系统通过虚拟内存管理方式来重映射例程以避免复制所需例程

第一次调用库例程的时候，程序首先调用虚入口，然后执行间接跳转。它通过将一个数字放入寄存器来识别所需的库例程，然后跳转到动态链接器或加载器。链接器或加载器找到所需的例程，将其重映射并改变间接跳转位置的地址，使其指向这个例程。然后跳转到这个例程。这个例程完成时，将返回到初始调用点。此后，它都会间接跳转到这个例程而不去执行额外的中间过程。

总的来说，DLL 需要额外的空间来存储动态链接的信息，但是不需要复制或链接整个库。仅仅在例程的第一次调用时开销较大，此后就只需一个间接跳转。注意，从库返回的操作不需要额外的开销。微软的 Windows 广泛地依赖动态链接库，如今在 UNIX 系统中程序执行的默认方式也是使用动态链接库。

2.12.6 启动一个 Java 程序

前面讨论了程序执行的传统模式，重点是以一个特定的指令集体系结构甚至这个体系结构的特定实现为目标的程序的快速执行。实际上，可以像 C 那样来执行 Java 程序。然而，Java 是为了不同的目标而发明的，其中之一就是能够安全地运行在每台计算机上，尽管这可能延长执行时间。

图 2-23 展示了典型的 Java 翻译和运行步骤。Java 程序会首先被编译成易于解释的指令序列——Java 字节码（Java bytecode）指令集（见 2.15 节），而不是编译成目标计算机可识别的汇编语言。这个指令集被设计得非常接近 Java 语言，这样，编译步骤相对简单，事实上它没有做任何优化。就像 C 语言编译器那样，Java 编译器会检查数据类型并且为每种类型提供正确的操作。Java 程序将转化成这些字节码的二进制形式。

- Java 字节码：为了解释 Java 程序而设计的指令集中的指令。

一个叫作 Java 虚拟机（Java Virtual Machine, JVM）的软件解释器能够执行 Java 字节码文件。解释器是一个用来模拟指令集体系结构的程序。例如，本书所使用的 MIPS 模拟器就是一个解释器。由于翻译非常简单，所以地址可以由编译器填写或在运行时被 JVM 发现，不需要再单独进行汇编。

- Java 虚拟机：解释 Java 字节码的程序。

解释的优势是可移植性。软件实现的 Java 虚拟机的可用性意味着在 Java 公布以后，大部分人都可以立即编写和运行 Java 程序。今天 Java 虚拟机可以用在从手机到网络浏览器等数亿的设备中。

解释的不足是性能较差。20 世纪 80 年代和 90 年代解释在执行性能上的飞速提高使它可用于很多重要的应用程序，但是与传统的编译好的 C 程序相比，10 倍的性能差距使 Java 对一些应用程序毫无吸引力。

为了既保持可移植性又提高执行速度，开发 Java 的下一阶段目标是实现程序执行的同时可以进行翻译的编译器。这个即时编译器（Just In Time compiler）通过记录运行的程序来找到称为“热点”的方法，然后将它们直接编译成 Java 虚拟机运行的宿主机的指令序列，编译过的部分保存起来以便下次程序运行时调用，这样，以后每次运行会更快。解释和编译的平衡随着时间的推移逐步形成，届时，经常运行的 Java 程序的解释开销变得非常小。

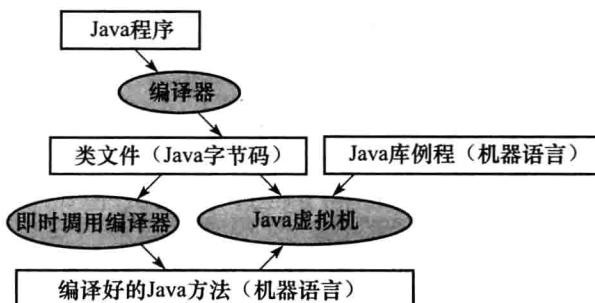


图 2-23 Java 的翻译层次。一个 Java 程序首先被编译成一个二进制版本的 Java 字节码形式，其中由编译器定义所有的地址。此时，Java 程序已可在解释器上运行，称为 Java 虚拟机（JVM）。在程序运行的时候，JVM 链接 Java 库中一些需要调用的方法。为了得到更好的性能，JVM 能够调用即时（just in time, JIT）编译器，在运行它的机器上能够选择性地把一些方法编译成宿主机上的本地机器语言

- 即时编译器：一类通用编译器的名称，编译器能够在运行时将解释的代码段翻译成宿主计算机上的机器语言。

随着计算机的速度越来越快，编译器能做的事情也越来越多。而随着研究者不断地发明更好的技术来编译 Java 程序，Java 与 C 或 C++ 在性能上的差距越来越小。2.15 节将进一步介绍 Java 程序、Java 字节码、JVM 和 JIT 编译器。

01 小测验

对 Java 设计者来说，你认为与翻译器相比，解释器在哪些方面的优点是最重要的？

1. 解释器便于编写。
2. 更准确的错误消息。
3. 更少的目标代码。
4. 机器独立性。

2.13 以一个 C 排序程序作为完整的例子

以片断的方式展示汇编代码的危险之处在于，你无法知道整个汇编语言程序的全貌。本节，我们给出了两个 C 过程对应的 MIPS 代码：一个用于交换（swap）数组的元素，另一个用于对数组元素排序（sort）。

2.13.1 swap 过程

我们从图 2-24 中的过程 swap 开始。这个过程简单地交换内存中两个位置的内容。我们按照以下常见的步骤把它从 C 程序手动翻译为汇编程序：

- 1) 为程序变量分配寄存器。
- 2) 为过程体生成汇编代码。
- 3) 保存过程调用间的寄存器。

本小节将按照这三个步骤描述 swap 程序，在最后把它们总结在一起。

1. 为 swap 分配寄存器

如 2.8 节所述，在 MIPS 中，实现参数传递通常使用寄存器 \$a0、\$a1、\$a2、\$a3。由于 swap 只需要两个参数，v 和 k，它们将被分配在寄存器 \$a0 和 \$a1 中。由于 swap 是一个叶过程（见 2.8.2 节），所以我们为唯一的剩余变量 temp 分配寄存器 \$t0。这些寄存器的分配与图 2-24 中的 swap 过程的第一部分变量的声明相对应。

2. 为 swap 过程体生成代码

swap 剩余部分的 C 代码如下所示：

```
temp = v[k];
v[k] = v[k+1];
v[k+1] = temp;
```

回忆一下 MIPS 是按字节在内存中寻址的，字由 4 字节组成。因此我们需要把 k 乘以 4，再与地址相加。忘记连续的字之间的地址相差 4 而不是 1，是汇编语言程序设计中常见的错误。因此获得 v [k] 地址的第一步就是通过左移 2 位来使 k 乘以 4：

```
void swap(int v[], int k)
{
    int temp;
    temp = v[k];
    v[k] = v[k+1];
    v[k+1] = temp;
}
```

图 2-24 一个交换内存中两个不同位置所存的数值的 C 过程。本小节要在排序的例子中使用这个过程

```
sll    $t1, $a1,2      # reg $t1 = k * 4
add    $t1, $a0,$t1    # reg $t1 = v + (k * 4)
                  # reg $t1 has the address of v[k]
```

接下来使用 \$t1 来取 v [k] 的值，在使 \$t1 加 4 得到 v [k+1] 的地址：

```
lw     $t0, 0($t1)    # reg $t0 (temp) = v[k]
lw     $t2, 4($t1)    # reg $t2 = v[k + 1]
                  # refers to next element of v
```

最后将 \$t0 和 \$t2 存储到需要交换数据的地址中：

```
sw     $t2, 0($t1)    # v[k] = reg $t2
sw     $t0, 4($t1)    # v[k+1] = reg $t0 (temp)
```

至此，我们已经为该过程分配了寄存器并翻译好了程序体的代码。保存在 swap 中使用的保存寄存器的代码还没有完成。但是，由于这是一个叶过程，并没有使用保存寄存器，所以没有需要保留的东西。

3. 完整的 swap 程序

现在我们已经得到完整的例程了，包括程序标号和返回的跳转。为了方便读者的理解，在图 2-25 中，我们标明了过程中每个代码块的目的。

过程体
<pre>swap: sll \$t1, \$a1,2 # reg \$t1 = k * 4 add \$t1, \$a0,\$t1 # reg \$t1 = v + (k * 4) # reg \$t1 has the address of v[k] lw \$t0, 0(\$t1) # reg \$t0 (temp) = v[k] lw \$t2, 4(\$t1) # reg \$t2 = v[k + 1] # refers to next element of v sw \$t2, 0(\$t1) # v[k] = reg \$t2 sw \$t0, 4(\$t1) # v[k+1] = reg \$t0 (temp)</pre>
过程返回
<pre>jr \$ra # return to calling routine</pre>

图 2-25 图 2-24 中 swap 过程的 MIPS 汇编代码

2. 13.2 sort 过程

为保证你能够认识到汇编语言编程的严格性，我们提供了第二个更长的例子。在这个例子中，我们将编写一个调用 swap 过程的例程。这个例程对数组中的整数进行排序，使用的是冒泡或交换排序算法，这种排序算法虽然不是最快的，但却是最简单的。图 2-26 给出了该程序的 C 代码。我们还是使用几个步骤来演示翻译的过程，最后再把它们总结到一起。

```
void sort (int v[], int n)
{
    int i, j;
    for (i = 0; i < n; i += 1) {
        for (j = i - 1; j >= 0 && v[j] > v[j + 1]; j -= 1) {
            swap(v, j);
        }
    }
}
```

图 2-26 一个对数组 v 中元素进行排序的 C 程序

1. sort 的寄存器分配

为过程 sort 的两个参数 v 和 n 分配参数寄存器 \$a0 和 \$a1，为变量 i 和 j 分别分配寄存器 \$s0 和 \$s1。

2. 为 sort 过程体生成代码

过程体包含两个嵌套的 for 循环和一个有参数的 swap 调用。我们将从外到内来展开代码。第一步来翻译最外面的 for 循环。

```
for (i = 0; i < n; i += 1) {
```

回忆 C 语言中 for 的声明有三个参数：初始值、循环判断条件和迭代增量。for 语句的第一部分是将 i 初始化为 0，这需要一条指令，

```
move $s0, $zero # i = 0
```

(请记住 move 是为了方便汇编程序员而由汇编器提供的伪指令，见 2.12.2 节。) for 语句的最后一部分，需要一条语句来增加 i：

```
addi $s0, $s0, 1 # i += 1
```

循环要在条件 $i < n$ 非真的时候退出，换句话说，当 $i \geq n$ 时循环退出。如果 $\$s0 < \$a1$ ，那么小于则置位指令将 $\$t0$ 置 1，否则置 0。因为我们要测试 $\$s0 \geq \$a1$ ，所以当寄存器 $\$t0$ 为 0 时，执行分支指令。这需要两条指令：

```
for1st:slt $t0, $s0, $a1 # reg $t0 = 0 if $s0 >= $a1 (i >= n)
beq $t0, $zero, exit1 # go to exit1 if $s0 >= $a1 (i >= n)
```

循环的底部仅仅需要跳回循环判断的地方：

```
j for1st # jump to test of outer loop
exit1:
```

第一个 for 循环的框架代码为

```
move $s0, $zero # i = 0
for1st:slt $t0, $s0, $a1 # reg $t0 = 0 if $s0 >= $a1 (i >= n)
beq $t0, $zero, exit1 # go to exit1 if $s0 >= $a1 (i >= n)
.
.
.
(body of first for loop)
.
.
.
addi $s0, $s0, 1 # i += 1
j for1st # jump to test of outer loop
exit1:
```

(后面的练习将会进一步探索为类似的循环编写更快的代码。)

第二个 for 循环的 C 语句如下：

```
for (j = i - 1; j >= 0 && v[j] > v[j + 1]; j -= 1) {
```

这个循环的初始化部分仍然是一条指令：

```
addi $s1, $s0, -1 # j = i - 1
```

循环末尾 j 的自减（减 1）也是一条指令：

```
addi $s1, $s1, -1 # j -= 1
```

循环判断由两个部分组成。任何一个条件为假就退出循环，所以第一个条件如果为假 ($j < 0$) 就要退出循环：

```
for2tst: slti $t0, $s1, 0 # reg $t0 = 1 if $s1 < 0 (j < 0)
bne $t0, $zero, exit2 # go to exit2 if $s1 < 0 (j < 0)
```

这将跳过第二个条件测试，如果没有跳过，则 $j \geq 0$ 。

第二个测试条件当 $v[j] > v[j + 1]$ 非真的时候退出，或 $v[j] \leq v[j + 1]$ 时退出。为得到地址，我们首先将 j 乘以 4（我们需要字节地址），然后将它与 v 的基址相加：

```
sll $t1, $s1, 2 # reg $t1 = j * 4
add $t2, $a0, $t1 # reg $t2 = v + (j * 4)
```

现在取 $v[j]$ ：

```
lw $t3, 0($t2) # reg $t3 = v[j]
```

因为我们知道第二个元素恰好是下一个字，所以我们将寄存器 $\$t2$ 值加 4，得到 $v[j + 1]$

135

136

的地址：

```
lw    $t4, 4($t2)  # reg $t4 = v[j + 1]
```

测试 $v[j] \leq v[j+1]$ 与测试 $v[j+1] \geq v[j]$ 相同，所以测试退出的两条指令如下：

```
slt  $t0, $t4, $t3  # reg $t0 = 0 if $t4 > $t3  
beq  $t0, $zero, exit2 # go to exit2 if $t4 > $t3
```

循环末尾跳回到内层循环测试处：

```
j    for2tst  # jump to test of inner loop
```

将这些片段组合到一起，可得第二个 for 循环的框架如下：

```
addi $s1, $s0, -1      # j = i - 1  
for2tst: slti $t0, $s1, 0      # reg $t0 = 1 if $s1 < 0 (j < 0)  
        bne $t0, $zero, exit2 # go to exit2 if $s1 < 0 (j < 0)  
        sll $t1, $s1, 2      # reg $t1 = j * 4  
        add $t2, $a0, $t1      # reg $t2 = v + (j * 4)  
        lw   $t3, 0($t2)      # reg $t3 = v[j]  
        lw   $t4, 4($t2)      # reg $t4 = v[j + 1]  
        slt $t0, $t4, $t3      # reg $t0 = 0 if $t4 > $t3  
        beq $t0, $zero, exit2 # go to exit2 if $t4 > $t3  
        . . .  
        (body of second for loop)  
        . . .  
        addi $s1, $s1, -1      # j -= 1  
        j   for2tst          # jump to test of inner loop  
exit2:
```

3. sort 中的过程调用

下一步翻译第二个 for 循环的循环体：

```
swap(v,j);
```

调用 swap 很容易：

```
jal   swap
```

4. sort 中的参数传递

当我们想传递参数时问题出现了，因为 sort 过程需要使用寄存器 \$a0 和 \$a1 中的值，而 swap 过程需要将它的参数放入这些寄存器。一种解决办法是在过程执行的早期将 sort 的参数复制到其他的寄存器中，使 swap 过程可以使用寄存器 \$a0 和寄存器 \$a1。（这个复制的过程比在栈中保存后再取回要快得多。）在过程中我们首先将寄存器 \$a0 和 \$a1 的值复制到寄存器 \$s2 和 \$s3。

```
move $s2, $a0      # copy parameter $a0 into $s2  
move $s3, $a1      # copy parameter $a1 into $s3
```

然后用下面两条指令将参数传递给 swap

```
move $a0, $s2      # first swap parameter is v  
move $a1, $s1      # second swap parameter is j
```

5. 在 sort 中保留寄存器

仅剩保存和恢复寄存器值的代码了。因为 sort 是一个过程并且它要递归使用，所以很明显需要用寄存器 \$ra 保存返回地址。sort 过程还使用了 \$s0、\$s1、\$s2 和 \$s3 保存寄存器，它们的值也必须被保存。所以 sort 过程头如下：

```
addi $sp,$sp,-20  # make room on stack for 5 registers  
sw   $ra,16($sp)  # save $ra on stack  
sw   $s3,12($sp)  # save $s3 on stack  
sw   $s2, 8($sp)   # save $s2 on stack  
sw   $s1, 4($sp)   # save $s1 on stack  
sw   $s0, 0($sp)   # save $s0 on stack
```

过程末尾只需反向执行这些指令，然后为了返回加上 jr 指令。

6. 完整的 sort 过程

现将所有片段合起来放入图 2-27，注意 for 循环中对寄存器 \$a0 和 \$a1 的引用已经被替换成对寄存器 \$s2 和 \$s3 的引用。为了方便阅读，我们再一次将过程中每一块的用途标了出来。本例中，9 行 C 语言编写的 sort 过程被翻译成 35 行的 MIPS 汇编语言代码。

保存寄存器值	
	<pre>sort: addi \$sp, \$sp, -20 # make room on stack for 5 registers sw \$ra,16(\$sp) # save \$ra on stack sw \$s3,12(\$sp) # save \$s3 on stack sw \$s2,8(\$sp) # save \$s2 on stack sw \$s1,4(\$sp) # save \$s1 on stack sw \$s0,0(\$sp) # save \$s0 on stack</pre>
过程体	
移动参数	<pre>move \$s2, \$a0 # copy parameter \$a0 into \$s2 (save \$a0) move \$s3, \$a1 # copy parameter \$a1 into \$s3 (save \$a1)</pre>
循环外部	<pre>move \$s0, \$zero # i = 0 forltst: slt \$t0, \$s0, \$s3 # reg \$t0 = 0 if \$s0 < \$s3 (i < n) beq \$t0, \$zero, exit1 # go to exit1 if \$s0 < \$s3 (i < n)</pre>
循环内部	<pre>addi \$s1, \$s0, -1 # j = i - 1 for2tst: slti \$t0, \$s1, 0 # reg \$t0 = 1 if \$s1 < 0 (j < 0) bne \$t0, \$zero, exit2 # go to exit2 if \$s1 < 0 (j < 0) sll \$t1, \$s1, 2 # reg \$t1 = j * 4 add \$t2, \$s2, \$t1 # reg \$t2 = v + (j * 4) lw \$t3, 0(\$t2) # reg \$t3 = v[j] lw \$t4, 4(\$t2) # reg \$t4 = v[j+1] slt \$t0, \$t4, \$t3 # reg \$t0 = 0 if \$t4 < \$t3 beq \$t0, \$zero, exit2 # go to exit2 if \$t4 < \$t3</pre>
传递参数和调用	<pre>move \$a0, \$s2 # 1st parameter of swap is v (old \$a0) move \$a1, \$s1 # 2nd parameter of swap is j jal swap # swap code shown in Figure 2.25</pre>
循环内部	<pre>addi \$s1, \$s1, -1 # j -= 1 j for2tst # jump to test of inner loop</pre>
循环外部	<pre>exit2: addi \$s0, \$s0, 1 # i += 1 j forltst # jump to test of outer loop</pre>
恢复寄存器的值	
	<pre>exit1: lw \$s0,0(\$sp) # restore \$s0 from stack lw \$s1,4(\$sp) # restore \$s1 from stack lw \$s2,8(\$sp) # restore \$s2 from stack lw \$s3,12(\$sp) # restore \$s3 from stack lw \$ra,16(\$sp) # restore \$ra from stack addi \$sp, \$sp, 20 # restore stack pointer</pre>
过程返回	
	<pre>jr \$ra # return to calling routine</pre>

图 2-27 图 2-26 中 sort 过程的 MIPS 汇编版本

01 精解 这个例子可以使用的一种优化方法是内联过程（procedure inlining）。在代码中调用 swap 过程的地方，编译器将 swap 的过程体的代码复制过来，而不是通过传递参数并通过 jal 指令来调用这段代码。本例中使用内联可以省掉 4 条指令。使用内联优化的缺点是如果内联过程需要在多个地方调用，编译后产生的代码将会变多。如果这种代码扩展导致 cache 的缺失率上升，将导致性能的下降（见第 5 章）。

01 理解程序性能 图 2-28 展示了编译器优化对排序程序的性能、编译时间、时钟周期、指令数和 CPI 的影响。注意没有优化的代码具有最好的 CPI，使用 O1 优化的代码具有最少的指令数，但是 O3 优化的执行速度最快，这告诉我们执行时间是准确衡量程序性能的唯一指标。

图 2-29 比较了编程语言、编译执行或解释执行和算法对排序程序性能的影响。第四列表明在执行冒泡排序时没有优化的 C 程序比解释型的 Java 程序快 8.3 倍。使用即时编译器可以使 Java 比没有优化的 C 程序快 2.1 倍，比最佳优化的 C 代码慢不到 1.13 倍。（2.15 节将给出关于解释执行和编译执行 Java 的更多细节以及冒泡排序的 Java 和 MIPS 代码。）在第五列中，快速排序的性能比就沒那么接近了，这大概是因为在这样短的执行时间内分摊运行时编译的时间是非常困难的。最后一列展示了更好的算法带来的影响，当对 100 000 个元素进行排序时，性能达到了 3 个数量级的提升。即第五列中解释执行的 Java 与第四列中最优化的 C 代码相比，快速排序法要比冒泡法快 50 倍 (0.05×2468 或者用 $123/2.41$)。

gcc 优化选项	相对性能	时钟周期（百万）	指令数（百万）	CPI
无	1.00	158 615	114 938	1.38
O1（中等）	2.37	66 990	37 470	1.79
O2（完全）	2.38	66 521	39 993	1.66
O3（过程集成）	2.41	65 747	44 993	1.46

图 2-28 冒泡排序中编译器优化对性能、指令数、CPI 的影响比较。程序对含有 100 000 个字的被初始化为随机数的数组进行排序。程序运行在 3.06GHz 的奔腾 4 处理器上，前端系统总线是 533MHz，具有 2GB 的 PC2100 DDR SDRAM。操作系统使用 Linux 2.4.20

编程语言	执行方式	优化选项	冒泡排序 相对性能	快速排序 相对性能	快速排序相对冒泡 排序加速比
C	编译器	无	1.00	1.00	2 468
	编译器	O1	2.37	1.50	1 562
	编译器	O2	2.38	1.50	1 555
	编译器	O3	2.41	1.91	1 955
Java	解释器	—	0.12	0.05	1 050
	即时编译器	—	2.13	0.29	338

图 2-29 两个排序算法的性能比较。算法分别用 C 和 Java 实现，Java 分别使用解释执行和优化编译来与未优化的 C 版本比较。最后一列是快速排序比冒泡排序在每种语言和执行方式下速度提高多少。这些程序运行的系统与图 2-28 相同。JVM 是 Sun 的 1.3.1 版本，JIT 是 Sun Hotspot 的 1.3.1 版本

01 精解 MIPS 的编译器总是在栈上为参数保留空间以便它们得以保存，所以实际上 \$sp 总是减 16 来给 4 个参数寄存器（16 字节）分配空间。这样做的原因是 C 提供一个 vararg 选项，该选项允许选择一个指针，例如过程的第三个参数。当编译器遇到这种少见的 vararg 时，它就将 4 个参数寄存器的值都复制到栈上已经保留的位置中。

2.14 数组与指针

理解指针对任何一个 C 程序新手来说都是具有挑战的。通过对比使用数组和数组标记的汇编代码和使用指针的汇编代码，可以从本质上理解指针。本节将展示 C 和 MIPS 汇编版本的两个清除内存中连续字的过程：一个使用数组标记；另一个使用指针。图 2-30 给出了这两个 C 过程。

```
clear1(int array[], int size)
{
    int i;
    for (i = 0; i < size; i += 1)
        array[i] = 0;
}
clear2(int *array, int size)
{
    int *p;
    for (p = &array[0]; p < &array[size]; p = p + 1)
        *p = 0;
}
```

图 2-30 两个将数组清零的 C 过程。`clear1` 使用下标，而 `clear2` 使用指针。对不熟悉 C 的人，第二个过程需要做一些解释。变量的地址使用 `&` 表示，指针所指向的对象用 `*` 表示。声明部分说明 `array` 和 `p` 都是指向整数的指针。`clear2` 的 `for` 循环中第一个部分将 `array` 的第一个元素的地址赋值给指针 `p`。`for` 循环的第二部分判断这个指针是否指向了 `array` 的最后一个元素之外。`for` 循环的最后一部分，对这个指针每次递增（增 1），意味着将指针移到它声明的空间中的下一个对象。由于 `p` 是一个指向整数的指针，编译器将会产生 MIPS 指令，让 `p` 按照 4 递增，4 是 MIPS 中整数的字节数目。循环体中将 0 赋值给 `p` 所指向的对象

本节的目的是展示指针是如何映射到 MIPS 指令的，而不是赞同这种过时的编程风格。我们在本节的末尾将看到现代编译器的优化对这两个过程带来的影响。

2.14.1 用数组实现 clear

我们从数组版本的 `clear1` 开始，主要关注循环体，而忽略过程链接相关的代码。假设两个参数 `array` 和 `size` 分别在寄存器 `$a0` 和 `$a1` 中，`i` 保存在 `$t0` 中。

for 循环的第一部分，初始化变量 `i`：

```
move $t0,$zero      # i = 0 (register $t0 = 0)
```

为了将 `array [i]` 清 0，我们首先需要得到它的地址。首先把 `i` 乘以 4 得到字节地址：

```
loop1: sll $t1,$t0,2      # $t1 = i * 4
```

因为数组的起始地址在寄存器中，所以我们必须将它与下标相加以得到 `array [i]` 的地址，使用下面的加法指令：

```
add $t2,$a0,$t1      # $t2 = address of array[i]
```

然后，我们就将 0 保存在这个地址：

```
sw $zero, 0($t2)      # array[i] = 0
```

这条指令是循环体最后一条指令，下一步是增加 `i` 值（加 1）：

```
addi $t0,$t0,1      # i = i + 1
```

循环测试条件检测 `i` 是否小于 `size`：

```
slt $t3,$t0,$a1      # $t3 = (i < size)
bne $t3,$zero,loop1  # if (i < size) go to loop1
```

现在，我们已经得到过程所有的片断。下面则是使用数组下标对数组清零的 MIPS 汇编编码：

```

move $t0,$zero      # i = 0
loop1: sll $t1,$t0,2    # $t1 = i * 4
       add $t2,$a0,$t1    # $t2 = address of array[i]
       sw  $zero, 0($t2)   # array[i] = 0
       addi $t0,$t0,1      # i = i + 1
       slt $t3,$t0,$a1     # $t3 = (i < size)
       bne $t3,$zero,loop1 # if (i < size) go to loop1

```

(只要 size 大于 0, 这些代码就能正确工作; ANSI C 需要在循环前测试 size 值, 但是我们跳过了这个。)

142

2.14.2 用指针实现 clear

第二个过程是使用指针的, 该过程将两个参数 array 和 size 分配到寄存器 \$a0 和 \$a1, 将 p 分配到寄存器 \$t0。在第二个过程开始时需要将数组的首地址赋值给指针 p:

```
move $t0,$a0          # p = address of array[0]
```

接下来的代码将是 for 循环体, 它仅仅是简单地将 0 存到地址 p:

```
loop2: sw $zero,0($t0)  # Memory[p] = 0
```

这条指令实现了循环体, 所以下一条指令将是迭代子自增, 即改变 p 使其指向下一个字:

```
addi $t0,$t0,4        # p = p + 4
```

在 C 中将指针加 1 意味着将指针指向序列中下一个对象。因为 p 是一个指向整数的指针, 整数占用 4 字节, 编译器将对 p 加 4。

接着就是循环测试。首先计算 array 最后一个元素的地址。先将 size 乘以 4 得到字节地址。

```
sll $t1,$a1,2          # $t1 = size * 4
```

然后, 将乘积与数组的首地址相加以获得数组后面第一个字的地址:

```
add $t2,$a0,$t1        # $t2 = address of array[size]
```

循环测试仅仅是简单地判断 p 是否比 array 最后一个元素的地址小:

```
slt $t3,$t0,$t2        # $t3 = (p < &array[size])
bne $t3,$zero,loop2    # if (p < &array[size]) go to loop2
```

所有的代码片段都已经完成, 现在我们可以看到指针版本的数组清零了:

```

move $t0,$a0          # p = address of array[0]
loop2: sw $zero,0($t0)  # Memory[p] = 0
       addi $t0,$t0,4      # p = p + 4
       sll $t1,$a1,2        # $t1 = size * 4
       add $t2,$a0,$t1      # $t2 = address of array[size]
       slt $t3,$t0,$t2      # $t3 = (p < &array[size])
       bne $t3,$zero,loop2  # if (p < &array[size]) go to loop2

```

与第一个例子一样, 这段代码也假定 size 大于 0。

注意, 尽管数组的末地址一直保持不变, 但是这个程序循环的每次迭代都要计算它。一种快速的执行方式是将数组末地址的计算放到循环体外面:

```

move $t0,$a0          # p = address of array[0]
sll $t1,$a1,2          # $t1 = size * 4
add $t2,$a0,$t1        # $t2 = address of array[size]
loop2: sw $zero,0($t0)  # Memory[p] = 0
       addi $t0,$t0,4      # p = p + 4
       slt $t3,$t0,$t2      # $t3 = (p < &array[size])
       bne $t3,$zero,loop2  # if (p < &array[size]) go to loop2

```

143

2.14.3 比较两个版本的 clear

将两段代码放在一起进行比较可以说明数组下标和指针的不同 (指针版本带来的变化被高

亮显示)：

```

move $t0,$zero      # i = 0
loop1:sll $t1,$t0,2    # $t1 = i * 4
add  $t2,$a0,$t1    # $t2 = &array[i]
sw   $zero,0($t2)  # array[i] = 0
addi $t0,$t0,1      # i = i + 1
slt  $t3,$t0,$a1    # $t3 = (i < size)
bne $t3,$zero,loop1# if () go to loop1
move $t0,$a0      # p = &array[0]
sll $t1,$a1,2      # $t1 = size * 4
add  $t2,$a0,$t1    # $t2 = &array[size]
loop2:sw  $zero,0($t2) # Memory[p] = 0
addi $t0,$t0,4      # p = p + 4
slt  $t3,$t0,$t2    # $t3=(i<&array[size])
bne $t3,$zero,loop2# if () go to loop2

```

左边的版本必须在循环中有“乘”和加操作，因为 *i* 值增加了，每个地址都将从新下标开始被重新计算。右边存储器指针版本的代码直接增加指针 *p*。指针版本通过把一些操作拿到循环外部，将每次迭代执行的指令从 6 条减少到 4 条。这种手动的优化与编译器的强度减少(用移位代替乘)和变量消除(消除循环中的数组地址计算)是一致的。2.15 节叙述了这两种优化和其他一些优化。

01 精解 正如前面提到的，C 编译器需要增加测试来保证 *size* 一定大于 0。一个方法是在循环的第一条指令之前加入一条跳转到 *slt* 的跳转指令。

01 理解程序性能 以往经常教育人们要在 C 中使用指针来获得数组所无法获得的更高的效率。然而，“使用指针，甚至会使你自己都无法理解代码的含义。”现代的优化编译器可以为数组版本产生同样好的代码。现在大部分程序员更喜欢让编译器去做更繁重的工作。

2.15 高级内容：编译 C 语言和解释 Java 语言

本节将简要概述 C 编译器如何工作和 Java 是如何执行的。因为编译器将对计算机的性能产生重要影响，所以理解编译器技术是理解性能的关键。要知道“编译器的构建”课程的学习一般需要 1 个或 2 个学期，所以我们这里将仅仅介绍一些基本内容。

本节的第二部分是为对面向对象语言(objected oriented language)(例如 Java)在 MIPS 体系结构上执行感兴趣的读者准备的。本节将展示被用于解释执行的 Java 字节码和前面章节中用 C 编写的程序段的 Java 版本的 MIPS 代码，包括冒泡排序。本节将包括 Java 虚拟机和即时编译器。

本节的剩余内容在配套网站上。

- ② 面向对象语言：一种针对对象而不是动作的编程语言，或者针对数据而不是逻辑的编程语言。

2.16 实例：ARMv7 (32 位) 指令集

在嵌入式设备领域中最流行的指令集体系结构是 ARM，2011 年有超过 90 亿部各种各样的设备使用 ARM 处理器，并且以每年 20 亿的数量增长。ARM 最初代表 Acorn RISC Machine，稍后被改为 Advanced RISC Machine。ARM 与 MIPS 处理器在同年发布并遵循相同的设计哲学。图 2-31 列出了 ARM 与 MIPS 的相似性。它们二者的主要区别是 MIPS 有更多的寄存器，而 ARM 有更多的寻址模式。

图 2-32 展示了 MIPS 与 ARM 在算术逻辑和数据传输指令方面具有相似的核心指令集。

	ARM	MIPS
发布时间	1985	1985
指令大小（位）	32	32
寻址空间（大小，模式）	32 位，平坦	32 位，平坦
数据对齐	对齐	对齐
数据寻址模式	9	3
整数寄存器（个数，模式，大小）	15 通用寄存器 × 32 位	31 通用寄存器 × 32 位
I/O	存储器映射	存储器映射

图 2-31 ARM 和 MIPS 指令集的相同点

指令名	ARM	MIPS
寄存器 - 寄存器	加法	add
	加法（溢出捕获）	adds; swivs
	减法	sub
	减法（溢出捕获）	subs; swivs
	乘法	mul
	除法	—
	与	and
	或	orr
	异或	eor
	取寄存器高位	—
	逻辑左移	lsl ¹
	逻辑右移	lsr ¹
	算术右移	asr ¹
	比较	cmp, cmn, tst, teq
数据传输	取有符号字节	ldr sb
	取无符号字节	ldr b
	取有符号半字	ldr sh
	取无符号半字	ldr h
	取字	ldr
	存字节	str b
	存半字	str h
	存字	str
	读、写特殊寄存器	mrs, msr
	原子交换	swp, swpb

图 2-32 ARM 的寄存器 - 寄存器指令和数据传输指令与 MIPS 核心指令是等价的。横线表示体系结构不支持该操作或不能用一些指令来实现该操作。如果有几条可供选择的指令都与 MIPS 核心指令等价，那么用逗号分隔这些指令。ARM 中每条数据操作指令都有移位的部分，所以移位指令用了上标 1，它们基本是 move 指令的变种，例如 lsr¹。注意 ARM 中没有除法指令

2.16.1 寻址模式

图 2-33 展示了 ARM 支持的数据寻址模式。不同于 MIPS，ARM 不需要使用专门的寄存器来保存 0 这个数值。尽管 MIPS 仅有 3 种简单的数据寻址模式（见图 2-18），ARM 却有 9 种寻址模式之多，包括十分复杂的计算的寻址模式。例如，ARM 的一种寻址模式可以把一个寄存器中的数移动任意位，将移位后得到的数与另外一个寄存器中的值相加产生地址，然后将产生

的新地址存入一个寄存器中。

寻址模式	ARM	MIPS
寄存器操作数	×	×
立即数操作数	×	×
寄存器 + 偏移（转移或基地址）	×	×
寄存器 + 寄存器（下标）	×	—
寄存器 + 寄存器倍乘（倍乘）	×	—
寄存器 + 偏移和更新寄存器	×	—
寄存器 + 寄存器和更新寄存器	×	—
自增，自减	×	—
相对 PC 的数据	×	—

图 2-33 数据寻址模式的总结。ARM 具有分离的寄存器间接寻址和寄存器 + 偏移寻址模式，而不是仅仅在后一种模式的偏移地址上填 0。为了增加寻址范围，如果是对半字或字进行操作，ARM 对偏移左移 1 位或 2 位

2.16.2 比较和条件分支

MIPS 使用寄存器中的值来决定条件分支是否执行。而 ARM 使用传统的存储在程序状态字中的 4 位条件码来决定条件分支是否执行。这 4 个条件码是：负值（negative）、零（zero）、进位（carry）和溢出（overflow）。这些条件码可以被任何算术或逻辑指令设置，不同于早期的体系结构，这些设置功能是每条指令的可选功能。明确的选项会使流水化的实现变得更加容易。ARM 使用条件分支来测试条件码以判断所有有符号和无符号的关系。

CMP 指令用一个操作数减去另一个操作数，用它们的差设置条件码。CMN 指令将一个操作数与另一个操作数相加，用它们的和来设置条件码。TST 指令将两个操作数进行逻辑与，然后设置除溢出位外其他的条件码。TEQ 指令是用异或结果来设置条件码的前三位。

ARM 具有这样一个不寻常的特点，每条指令都有一个可选的执行条件，这个条件决定于条件码。每条指令开始的 4 位字段决定这条指令将执行空操作（nop）还是执行真实的指令操作，这种选择也取决于条件码。因此，条件分支也可以被认为是有条件的执行无条件分支指令。条件执行指令可以取代仅为了跳过一条指令的分支指令，不仅占用的代码空间更少，而且也会节省运行时间。

图 2-34 展示了 ARM 和 MIPS 的指令格式。它们之间的主要区别有两点：每条指令的 4 位条件执行字段不同；ARM 因为只用 MIPS 一半数量的寄存器，所以具有相对较小的寄存器字段。

2.16.3 ARM 的特色

图 2-35 列举了 ARM 处理器所特有的一些算术逻辑指令，这些指令在 MIPS 中是不存在的。由于没有专门的寄存器用来存储 0，所以 ARM 需要单独的操作码来完成一些在 MIPS 中可以简单使用 \$zero 来完成的操作。另外，ARM 支持多个字的算术操作。

ARM 解释 12 位立即数字段的方式非常新颖。首先将右侧低 8 位的有效位填 0 扩展到 32 位，然后将所得的数循环右移，移动的位数由高 4 位的值乘以 2 决定。这种解释方式的优点是可以在 32 位字的范围内表达所有 2 的幂次。为什么这种分割所表示的数字多于简单的 12 位字段是一个有趣的问题。

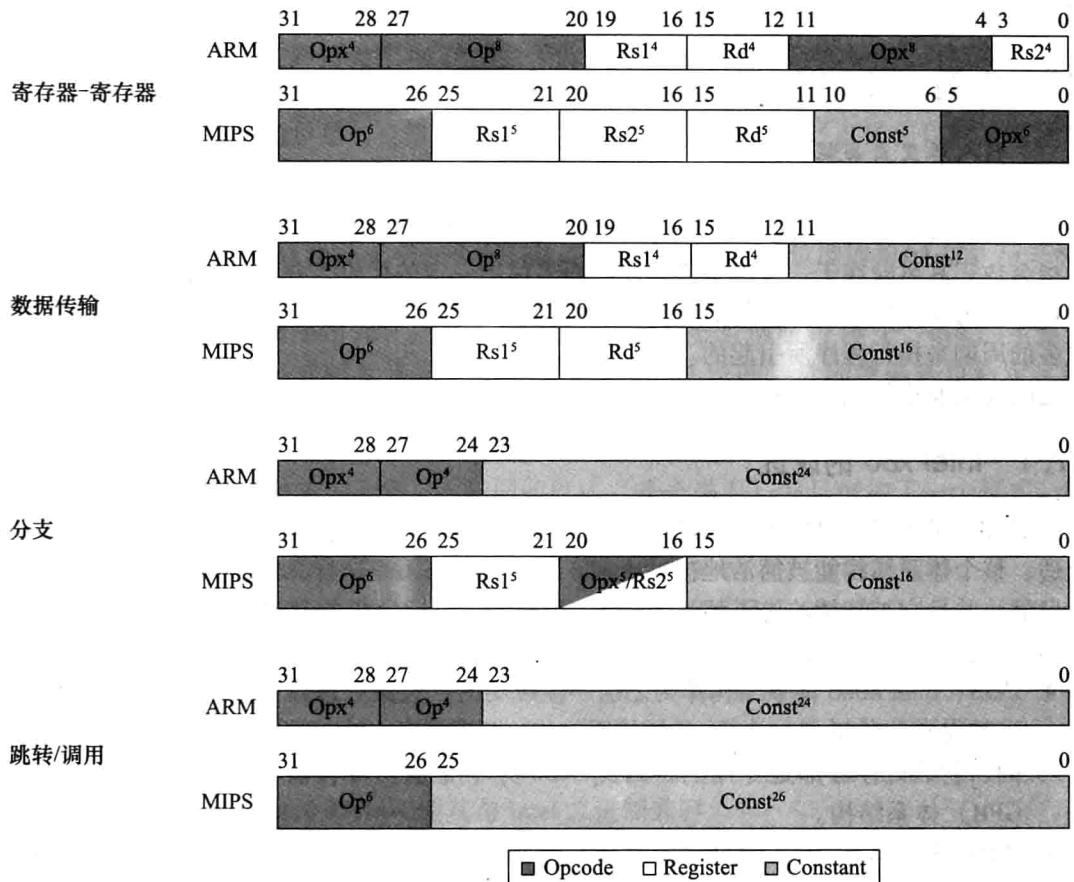


图 2-34 ARM 和 MIPS 的指令格式。区别在于体系结构中是有 16 个还是 32 个寄存器

名字	定义	ARM	MIPS
取立即数	$Rd = Imm$	mov	addi \$0,
非	$Rd = \sim(Rs1)$	mvn	nor \$0,
移动	$Rd = Rs1$	mov	or \$0,
循环右移	$Rd = Rsi >> i$ $Rd_{0...i-1} = Rs_{31-i...31}$	ror	
寄存器与另一寄存器的非进行与操作	$Rd = Rs1 \& \sim(Rs2)$	bic	
反向减	$Rd = Rs2 - Rs1$	rsb, rsc	
支持多个整数字的加	CarryOut, $Rd = Rd + Rs1 + OldCarryOut$	adcs	—
支持多个整数字的减	CarryOut, $Rd = Rd - Rs1 + OldCarryOut$	sbs	—

图 2-35 MIPS 中没有的 ARM 算术/逻辑指令

对操作数的移位并不仅限于立即数。所有算术和逻辑运算操作的第二个寄存器操作数都可以在执行操作之前进行移位。可选的移位方式是逻辑左移、逻辑右移、算术右移和循环右移。

ARM 还对寄存器组的操作提供了指令支持，这些指令叫作块加载和存储（block loads and stores）。在指令的 16 位掩码的控制下，16 个寄存器中的任意组合都可以被一条指令加载或存储到内存中。这些指令可以保存和恢复程序调用和返回时的寄存器。这些指令也可以被用于存

储器块的复制，现在这些存储器块的复制是对这些指令的主要应用。

2.17 实例：x86 指令集

情人眼里出西施。

——Margaret Wolfe Hungerford, 《Molly Bawn》, 1877

指令集的设计者有时提供比 ARM 和 MIPS 更强大的操作。这样做的目的是减少程序需要执行的指令数。其风险在于，在设备简单性方面需付出一定的代价，并且可能使程序执行时间变长，这是因为指令执行需要更长的时间。这可能是由于时钟周期变长或者是比更简单的序列需要更多的周期来执行程序所引起的。

通向复杂操作的道路困难重重。2.19 节将阐述复杂性的陷阱。

2.17.1 Intel x86 的改进

ARM 和 MIPS 都是由单独的小组在 1985 年推出的。这种体系结构的每部分配合在一起非常合适，整个体系结构能被简洁地描述出来。但是 x86 却不是这样，它是由一些相互独立的小组开发的，并且它被持续改进了超过 35 年，不断在原来指令集的基础上增加新的特性，这就像有些人往包装好的包里添加衣服。下面是 x86 发展的一些重要的里程碑。

149

- 1978：Intel 8086 体系结构作为之前一款成功的 8 位微处理器的汇编语言的可兼容的扩展被发布。8086 是一个 16 位的体系结构，所有内部的寄存器都是 16 位长。与 MIPS 不同，它的寄存器都是专用的，因此 8086 并不是通用寄存器（general-purpose register, GPR）体系结构。
- 1980：Intel 8087 浮点协处理器发布。这个体系结构在 8086 的基础上增加了 60 条浮点指令。它通过栈来代替寄存器（见 2.21 节和 3.7 节）。
- 1982：80286 在 8086 的基础上把地址空间扩展到 24 位，并设计了精妙的内存映射和保护模式（见第 5 章），还增加了一些指令去丰富整个指令集以及控制保护模式。
- 1985：80386 在 80286 体系结构的基础上将地址空间扩展到 32 位。除了 32 位的寄存器和 32 位的地址空间，80386 也增加了一些新的寻址模式和额外的操作。增加的指令使得 80386 几乎就是通用寄存器的处理器。80386 还增加了对页的支持并提供了段寻址（参见第 5 章）。与 80286 一样，80386 也提供能运行不经修改的 8086 程序的模式。
- 1989 ~ 1995：接下来在 1989 年发布了 80486，1992 年发布 Pentium 处理器，1995 年发布 Pentium Pro 处理器。这些处理器都是以获得更高的性能为目的的，仅有 4 个指令被增加到用户可见的指令集中，其中 3 个有助于多处理技术（参见第 6 章），另一个是条件传送指令。
- 1997：在 Pentium 和 Pentium Pro 销售后，Intel 公司宣称他们将用多媒体扩展 MMX（Multi Media Extension）来扩展 Pentium 和 Pentium Pro 的体系结构。这个新指令集包含 57 条指令，使用浮点栈来加速多媒体和通信应用程序。MMX 通过传统的单指令多数据（single instruction, multiple data, SIMD）的方式来一次处理多个短的数据元素（参见第 6 章）。Pentium II 没有引入任何新的指令。
- 1999：Intel 添加了另外 70 条指令，将 SSE（Streaming SIMD Extension）作为 Pentium III 的一部分。主要的变化是添加了 8 个独立的寄存器，把它们的长度增加到 128 位，并且增加了一个单精度浮点数据类型。因此，4 个 32 位的浮点操作就可以并行进行。为了改进内存性能，SSE 还包括 cache 的预取指令，以及可以绕过缓冲器直接写内存的流存储指令。

- 2001：Intel 公司增加了另外 144 条指令。这次命名为 SSE2。增加的新的数据类型是双精度算术，它允许并行操作 64 位浮点型数据对。这 144 条指令几乎都对应着一些已经存在的 MMX 和 SSE 指令，这些指令并行操作 64 位数据。这种变化不仅允许更多的多媒体操作，并且与单独的栈架构相比，编译器多了一个新的浮点操作目标。编译器可以使用 8 个 SSE 寄存器来充当浮点寄存器。这种改进大大增强了第一个包括 SSE2 指令集的微处理器 Pentium 4 的浮点性能。
- 2003：这次是 AMD 改进了 x86 体系结构，把地址空间从 32 位增加到 64 位。与 1985 年在 80386 上从 16 位到 32 位的转变类似，AMD64 把所有的寄存器都拓宽到 64 位，并且把寄存器的数目增加到 16，把 128 位的 SSE 寄存器数目增加到 16 个。ISA 的主要变化是新增加了一个模式叫长模式（long mode），用 64 位的地址和数据来重新定义所有 x86 指令的执行。为了寻址更多的寄存器，给指令增加了新前缀。根据计算方式，长模式还添加了 4~10 条新的指令并且去掉了 27 条旧指令。PC 相对数据寻址是另一个扩展。AMD64 仍然有一个和 x86 相同的模式（遗产模式）并且增加了一个模式，以限制用户程序使用 x86 模式，但是却允许操作系统使用 AMD64 模式（兼容模式）。这些模式使它成为比 HP/Intel IA-64 更好地从 32 位过渡到 64 位寻址的处理器。
- 2004：Intel 屈服并吸纳了 AMD64，重新标记为 Extended Memory64 Technology (EM64T)，主要的区别是 Intel 增加了 128 位的原子比较和交换指令，这个本应在 AMD64 上可能具有的指令。同时，Intel 发布了新一代媒体扩展。SSE3 添加了 13 条指令来支持复杂算术，包括在结构数组上进行的图形操作、视频编码、浮点转换以及线程同步（见 2.11 节）。AMD 会在以后的芯片中提供对 SSE3 的支持。而且它几乎肯定能够把原先没有的原子交换指令添加到 AMD64 使其与 Intel 二进制兼容。
- 2006：作为 SSE4 的一部分扩展，Intel 发布了 54 条新指令。这些扩展都是针对像如下影响性能的因素：绝对差求和、数组结构的点积计算、窄数据到较宽的数据的符号或零扩展，序列中非零的数目统计等。还增加了对虚拟机的支持（见第 5 章）。
- 2007：作为 SSE5 的一部分，AMD 发布了 170 条指令，包括为 46 条基本指令集中的指令增加了像 MIPS 的 3 操作数的版本。
- 2011：Intel 发布了高级向量扩展，同时将 SSE 寄存器从 128 位扩展到 256 位，因此重新定义了 250 条指令并新增了 128 条指令。

② 通用寄存器：可用于存储任何指令的地址或数据的寄存器。

这段历史说明了兼容性这个“金手铐”对 x86 的影响，体系结构的改变不允许对已有的软件产生任何的危害。

无论 x86 结构有多失败，该指令集一直对个人计算机的更新换代起着很大的推动作用，在后 PC 时代占据着很大的份额。表面上看起来，3.5 亿 x86 芯片的年产量相对于 ARMv7 芯片的 90 亿片要小很多，但是许多公司都想去控制这个市场。无论如何，这个多变的家族带来的是一个难以解释并且不讨人喜欢的体系结构。

请鼓起勇气来面对你将要看到的内容！不要带着需要编写 x86 程序的担心来阅读这一节，实际上，本节的目的是让你熟悉这一世界上最流行的台式机体系结构的优缺点。

本节我们主要关心的是 80386 的 32 位指令子集，而不是整个 16 位、32 位和 64 位指令集。我们从寄存器和寻址模式开始说明，接下来是整数操作，最后考虑指令编码。

2.17.2 x86 寄存器和数据寻址模式

80386 的寄存器展示了指令集的进化（如图 2-36 所示）。80386 把 16 位寄存器（除了段寄

[152] 存器) 扩展为 32 位。并用前缀 E 来标示 32 位版本。它们通常被称为通用寄存器。80386 只有 8 个通用寄存器，这意味着 MIPS 程序使用 4 倍数量的寄存器，而 ARMv7 可以使用 2 倍数量的寄存器。

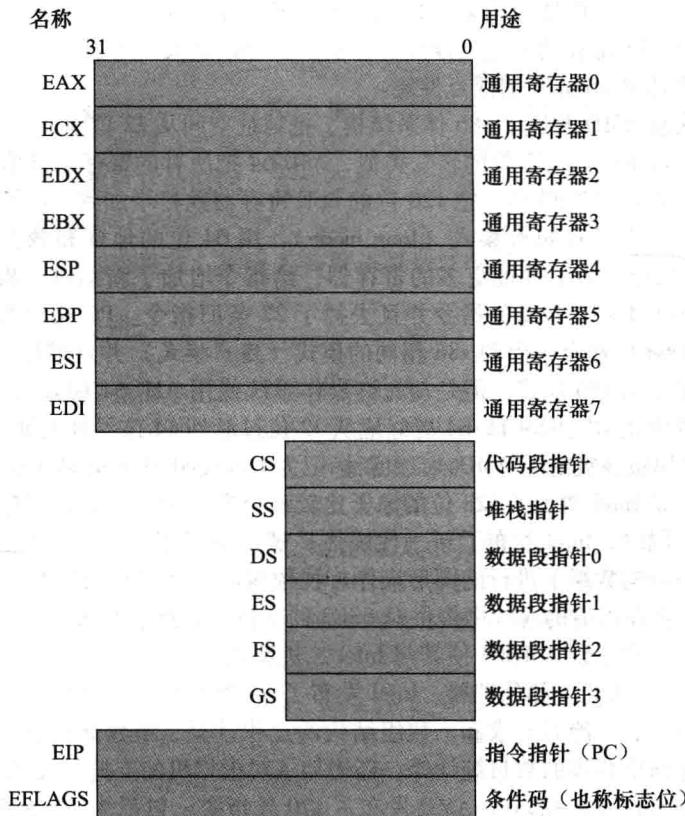


图 2-36 80386 寄存器组。从 80386 开始，上面的 8 个寄存器扩展到 32 位并可以当做通用寄存器使用

图 2-37 展示了两个操作数的算术、逻辑和数据传输指令。它们有两个重要的不同之处。首先 x86 的算术和逻辑指令中的一个操作数必须既是源操作数又是目的操作数，而 ARMv7 和 MIPS 的源操作数和目的操作数是不同的寄存器。这种限制给有限的寄存器带来更大的压力，因此一个源寄存器必须被改变。第二个重要的不同之处在于一个操作数可以在存储器中。这样，实质上任何指令都可能有一个操作数在存储器中。这与 ARMv7 和 MIPS 不同。

源/目标操作数类型	第二个源操作数
寄存器	寄存器
寄存器	立即数
寄存器	存储器
存储器	寄存器
存储器	立即数

图 2-37 算术、逻辑和数据传输指令的指令格式。x86 所允许的组合见上表。唯一的限制是没有存储器 - 存储器模式。立即数可以是 8 位、16 位或 32 位；寄存器可以是图 2-36 中 14 个主要的寄存器（不能是 EIP 或 EFLAGS）的任意一个

后面将会详细阐述数据的存储器寻址模式，在指令中提供两种位长的地址。这种所谓的偏移（displacements）既可能是 8 位也可能是 32 位。

尽管存储器操作数可以使用任何寻址模式，但是每种模式使用哪些寄存器是有限制的。

图 2-38 展示了 x86 寻址模式和每种模式下哪个 GPR 是不允许使用的，并说明如何使用 MIPS 指令集来达到相同效果。

模式	描述	寄存器限制	等价的 MIPS
寄存器间接寻址	地址在寄存器中	不能为 ESP 或 EBP	<code>lw \$s0,0(\$s1)</code>
8 位或 32 位偏移寻址模式	地址是基址寄存器与偏移量之和	不能为 ESP	<code>lw \$s0,100(\$s1) #<=16 bit # displacement</code>
基址加比例下标寻址	地址是 基址 + (2 ^{比例} × 下标) 比例是 0, 1, 2 或 3	基址：任何 GPR 下标：不能为 ESP	<code>mul \$t0,\$s2, add \$t0,\$t0,\$s1 lw \$s0,0(\$t0)</code>
8 位或 32 位偏移量的基址 + 比例下标寻址	地址是 基址 + (2 ^{比例} × 下标) + 偏移量 比例是 0, 1, 2 或 3	基址：任何 GPR 下标：不能为 ESP	<code>mul \$t0,\$s2,4 add \$t0,\$t0,\$s1 lw \$s0,100(\$t0) #<=6-bit # displacement</code>

图 2-38 x86 有寄存器使用限制的 32 位寻址模式及等价的 MIPS 代码。ARM 和 MIPS 所没有的，基址加比例下标寻址模式，包含在 x86 中以避免将寄存器中的下标乘 4（使用比例因子 2）变成字节地址（见图 2-25 和图 2-27）。比例因子 1 用于 16 位数据，3 用于 64 位数据。比例因子 0 意味着这个地址不需要按比例增加。在第二种或第四种模式中如果偏移量比 16 位长，等价的 MIPS 需要额外的两条指令：lui 取偏移量的高 16 位，add 将高 16 位与寄存器 \$s1 相加。（Intel 的基址寻址模式还有另外的名字基址和下标，但是它们本质上是等同的，我们在这里将它们合并。）

2.17.3 x86 整数操作

8086 提供对 8 位（字节）和 16 位（字）数据类型的支持。80386 在 x86 结构中加入了 32 位的地址和数据（双字）。（AMD64 又增添了 64 位的地址和数据，叫作四字；本小节我们将关注 80386。）数据类型的不同也造成了寄存器操作和存储器访问的不同。

几乎所有操作都能在 8 位和一个更长的数据上进行。这个最长的数据大小取决于运行的模式，可能是 16 位也可能是 32 位。

显然，有些程序希望操作所有三种长度的数据，于是 80386 系统结构提供一种不用明显增加代码长度的方便途径来指定每一种形式。它们认为大多数程序中 16 位或 32 位数据占绝大多数，于是设定一个默认的较长长度是有意义的。这个默认的数据长度由代码段寄存器中的一位指定。若要改变默认数据长度，需在指令前附加 8 位前缀告诉机器这条指令使用其他数据长度。

使用前缀是从 8086 借鉴过来的，8086 可使用多种前缀来改变指令的行为。最初的三个前缀包括忽略默认的段寄存器，给总线加锁来支持同步（见 2.11 节），或重复后面的指令直到寄存器 ECX 减少到 0。最后一个前缀要配合一个字节传送指令使用以便传送可变数目的字节。80386 还加入一个前缀以改变默认的地址长度。

x86 整数操作可以分为 4 个主要的类：

- 1) 数据传送指令，包括 move、push 和 pop。
- 2) 算术和逻辑指令，包括测试、整数和小数算术运算。
- 3) 控制流，包括条件分支、无条件跳转、调用和返回。
- 4) 字符串指令，包括字符串传送和字符串比较。

除了算术和逻辑操作指令的结果既可以保存在寄存器也可以保存在存储器地址外，前两个种类没有值得关注之处。图 2-39 展示了典型的 x86 指令和它们的功能。

x86 的条件分支像 ARMv7 一样基于条件码（condition code）或标志位（flag）。条件码是作为一些操作的副作用被设置的，大部分被用作将结果与 0 比较，然后使用分支指令测试条件码。PC 相对分支地址必须以字节数来指定，这与 ARMv7 和 MIPS 不同，80386 的指令不都是 4 字节长的。

指令	功能
je name	if equal (condition code) {EIP = name}; EIP - 128 <= name < EIP + 128
jmp name	EIP = name
call name	SP = SP - 4; M[SP] = EIP + 5; EIP = name;
movw EBX,[EDI + 45]	EBX = M[EDI + 45]
push ESI	SP = SP - 4; M[SP] = ESI
pop EDI	EDI = M[SP]; SP = SP + 4
add EAX,#6765	EAX = EAX + 6765
test EDX,#42	Set condition code (flags) with EDX and 42
movs l	M[EDI] = M[ESI]; EDI = EDI + 4; ESI = ESI + 4

图 2-39 x86 的一些典型指令和它们的功能。常用操作的列表在图 2-40 中。CALL 将下一条指令的 EIP 保存在栈上。(EIP 是 Intel 的程序计数器。)

字符串指令是 x86 的祖先 8080 的一部分，在大部分程序中都不使用。它们常常比同等功能的软件例程要慢（见 2.19 节的谬误）。

图 2-40 列出了一些 x86 的整数指令。这些指令大部分都同时有字节和字格式。

指令	含义
控制指令	条件和无条件分支
jnz,jz	条件成立跳转到 EIP + 8 位偏移量；JNE (for JNZ), JE (for JZ) 两者之一
jmp	无条件跳转——8 位或 16 位偏移量
call	过程调用——16 位偏移量；返回地址压入栈中
ret	从栈中弹出返回地址并跳转到该地址处
loop	循环分支——递减 ECX；如果 ECX 非零，则跳转到 EIP + 8 位偏移处
数据传输	在寄存器之间或寄存器和存储器之间传递数据
move	在两个寄存器之间或寄存器和存储器之间传递数据
push,pop	将源操作数压栈；将栈顶数据取到寄存器中
les	从存储器中取 ES 和一个 GPR
算术、逻辑	使用数据寄存器和存储器的算术和逻辑操作
add,sub	将源操作数与目的操作数相加；从目的操作数中减去源操作数；寄存器 - 存储器格式
cmp	比较源和目的操作数；寄存器 - 存储器格式
shl,shr,rcr	左移；逻辑右移；循环右移并用条件码填充
cbw	将 EAX 最右 8 位字节转换成 EAX 最右 16 位字
test	将源操作数和目的操作数进行逻辑与，并设置条件码
inc,dec	递增目的操作数，递减目的操作数
or,xor	逻辑或；异或；寄存器 - 存储器格式
字符串	在字符串操作数之间移动；由重复前缀给出长度
movs	通过递增 ESI 和 EDI 从源字符串复制到目的字符串；可能使用重复
lod\$	从字符串中取字节、字或双字到寄存器 EAX

图 2-40 一些典型的 x86 操作。很多操作使用寄存器 - 存储器格式，这种格式要求源操作数或目的操作数可以是存储器，另一个操作数可以是寄存器或立即数。

2.17.4 x86 指令编码

把最糟的放在最后——80386 的指令编码是非常复杂的，有多种不同指令格式。当没有操作数的时候，80386 的指令可以是 1 字节，最长到 15 字节。

图 2-41 展示了图 2-39 中几条指令的格式。操作码字节中通常有一位用来表明操作数是 8 位还是 32 位。一些指令的操作码可能还包含寻址模式和寄存器，例如，很多的指令具有如下形式“寄存器 = 寄存器操作立即数”。其他指令使用寻址模式的“后置字节”或额外的操作码字节，标记为“mod, reg, r/m”（模式，寄存器，寄存器/存储器）。这个后置字节在寻址存储器的很多指令中都被用到。基址加比例下标的寻址模式需要使用第二个后置字节，标记为“sc, index, base”（比例，下标，基址）。

a.JE EIP + displacement

4	4	8
JE	条件	偏移量

b.CALL

8	32
CALL	位移量

c.MOV EBX, [EDI + 45]

6	1	1	8	8
MOV	d	w	r/m	偏移量

d.PUSH ESI

5	3
PUSH	Reg

e.ADD EAX, #6765

4	3	1	32
ADD	Reg	w	立即数

f.TEST EDX, #42

7	1	8	32
TEST	w	寻址方式字节	立即数

图 2-41 典型的 x86 指令格式。图 2-42 给出后置字节（postbyte）的编码。很多指令包含 1 位的 w 段，这个字段说明操作的是一个字节还是一个双字。MOV 中 d 字段用于从存储器中传出或传入数据的指令并指明传输方向。ADD 指令需要 32 位的立即数字段，因为在 32 位模式下，立即数或者是 8 位或者是 32 位。TEST 中的立即数字段也是 32 位长，是因为在 32 位模式下没有 8 位的立即数要判断。总的来说，指令长度可以从 1 字节到 15 字节变化。较长的长度产生于额外的 1 字节前缀，该长度具有 4 字节的立即数和 4 字节的偏移地址，使用 2 字节的操作码，并使用比例下标模式说明符，这还需要一个额外的字节。

图 2-42 展示了 16 位和 32 位模式的两个后置字节地址指定的编码。不幸的是，为了全面理解哪个寄存器和哪种寻址模式可用，你需要看所有寻址模式的编码，有时甚至需要看指令编码。

reg	w = 0	w = 1	r/m	mod = 0		mod = 1		mod = 2		mod = 3
		16b	32b		16b	32b	16b	32b		
0	AL	AX	EAX	0	addr = BX + SI = EAX	same	same	same	same	same
1	CL	CX	ECX	1	addr = BX + DI = ECX	addr as	addr as	addr as	addr as	as
2	DL	DX	EDX	2	addr = BP + SI = EDX	mod = 0	mod = 0	mod = 0	mod = 0	reg
3	BL	BX	EBX	3	addr = BP + SI = EBX	+ disp8	+ disp8	+ disp16	+ disp32	field
4	AH	SP	ESP	4	addr = SI = (sib)	SI + disp8	(sib) + disp8	SI + disp8	(sib) + disp32	"
5	CH	BP	EBP	5	addr = DI = disp32	DI + disp8	EBP + disp8	DI + disp16	EBP + disp32	"
6	DH	SI	ESI	6	addr = disp16 = ESI	BP + disp8	ESI + disp8	BP + disp16	ESI + disp32	"
7	BH	DI	EDI	7	addr = BX = EDI	BX + disp8	EDI + disp8	BX + disp16	EDI + disp32	"

图 2-42 x86 的第一个地址说明符的编码：mod，reg，r/m。前 4 列表示 3 位的 reg 字段，它依赖于操作码中的 w 位以及机器是工作在 16 位（8086）模式还是 32 位（80386）模式。余下的列解释了 mod 和 r/m 字段。3 位的 r/m 字段依赖于 2 位的 mod 字段和地址的大小。用于地址计算的寄存器列在第六和第七列中，mod = 0 时依赖于寻址模式，mod = 1 时加上 8 位的偏移量，mod = 2 时加上 16 位或 32 位的偏移量。例外的情况有以下几种：1) 当 mod = 1 或 mod = 2，在 16 位模式时，r/m = 6 选择 BP 加上偏移。2) 当 mod = 1 或 mod = 2，在 32 位模式时，r/m = 5 选择 EBP 加上偏移量。3) 当 mod 不等于 3，在 32 位模式时，r/m = 4，(sib) 代表使用图 2-38 中的比例下标模式。当 mod = 3 时，r/m 字段指定一个寄存器，与 w 位组合在一起和 reg 字段的编码相同

2.17.5 x86 总结

Intel 的 16 位微处理器比它的竞争对手的更优秀的体系结构（如 Motorola 68000）早两年问世，这个领先使得 IBM 选用 8086 作为其 PC 的 CPU。Intel 的工程师普遍认识到 x86 要比 ARMv7 和 MIPS 的计算机更难制造，但是巨大的市场意味着 AMD 和 Intel 可以投入更多的资源来克服这些额外的复杂性。数量上的巨大优势弥补了风格上的缺点，这使得 x86 前景美好。

x86 中最常使用的体系结构组成部分是不难实现的，从 1978 年开始 AMD 和 Intel 就展示了整数程序性能的快速改进。为了获得这样的性能，编译器必须避免那些难于实现快速执行的体系结构部分。

然而，在后 PC 时代，虽然有大量的体系结构和制造专家基于 x86 做工作，但是 x86 在个人移动设备里面还不具有竞争力。

2.18 实例：ARMv8（64 位）指令集

在一个指令集所具有的所有潜在问题中，最不可能解决的就是地址空间太小的问题。x86 是第一个扩展为 32 位地址的，并且是第一个扩展为 64 位地址的指令集，许多其他的指令系统都被落在了后面。例如，虽然具有 16 位地址的 MOStek 6502 指令集统治了 Apple II，但是 Apple II 即使是第一个成功的商用个人计算机的领头羊，却也由于其地址空间上的缺陷饱受诟病。

虽然 ARM 体系结构遇到了 32 位地址空间的限制，在 2007 年开始设计具有 64 位地址的 ARM，并最终在 2013 年完成。与 x86 中为了使寄存器加宽为 64 位只做了很小改变不同，ARM 作了完全的改进。如果你了解 MIPS，那就非常容易了解 64 位版本的 ARMv8。

首先，与 MIPS 相比，ARM 舍弃了 v7 中并不常用的一些特性：

- v8 中没有条件执行字段，而在 v7 中几乎每条指令都有该字段。
- 立即数字段仅仅是一个 12 位的常数，而在 v7 中是产生一个常数的函数的输入。
- ARM 舍弃了 Load Multiple 和 Store Multiple 指令。
- PC 不再是一个寄存器，因此如果对其进行写操作将会导致非预期的分支转移。

其次，ARM 添加了一些 MIPS 中有用的特征：

- v8 有 32 个通用寄存器，编译器设计者非常喜欢该特点。与 MIPS 相同，一个寄存器永远存放 0，虽然在 load 和 store 指令中该寄存器将由栈指针替代。
- ARMv8 的寻址方式是用于所有的字长，而在 ARMv7 中并非如此。
- 它包含了 ARMv7 中省掉的除法指令。
- 它增加了 MIPS 中的相等或不等的条件分支指令。

由于 v8 相对于 v7 而言，其指令集更像 MIPS，因此我们的结论是 ARMv7 和 ARMv8 的主要相同点仅仅是名字。

2.19 谬误与陷阱

谬误：更强大的指令意味着更高的性能。

x86 的一个强大的地方是可以通过前缀来改变后续指令的执行。某个前缀可以重复执行后面的指令直到一个计数器减少至 0。因此，为了在存储器中传输数据，看起来最自然的指令序列应该是使用加了重复前缀的 move 指令来实现 32 位的存储器到存储器的传输。

另外一种方法是使用所有计算机上都有的标准指令，将数据取到寄存器后再存回存储器。这种形式通过代码复制来减少循环开销，复制操作大约快 1.5 倍。第三种方式，使用更大的浮点寄存器代替 x86 的整数寄存器，复制操作比使用复杂指令快 2 倍。

谬误：使用汇编语言编程来获得最高的性能。

在一段时间内，编程语言的编译器经常产生很低级的指令序列。通过不断改进，编译器产生的代码与手工编写的代码在性能上的差距正在快速缩小。事实上，为了与当今编译器竞争，汇编程序员需要深刻理解第 4 章和第 5 章中的计算机体系结构概念（包括处理器流水线和存储器层次）。

编译器和汇编程序员之间的斗争正在逐渐消失。例如，C 为程序员提供一个指示编译器把变量保存在寄存器中而不是换出到存储器中的机会。当编译器在寄存器分配上能力较差时，这种指示对性能至关重要。事实上，一些较老的 C 语言课本花费大量的时间给出了有效的寄存器指示的例子。今天的 C 语言编译器通常忽略这种指示，因为编译器能比程序员更好地分配寄存器。

即使手工编写会产生更快的代码，汇编语言编写还是存在很多危险：需要更多时间编码和调试，可移植性差，难于维护。软件工程中少数几个被广泛接受的公理之一是编写的程序行数越多所花时间也越多。很明显使用汇编语言编写的程序比 C 或 Java 更长。一旦代码写好，下一个危险将是它会变成一个流行的程序。这种程序存在的时间总是比预期要长，意味着程序员需要每隔几年就更新一下代码使新的版本可以运行在新的操作系统和新机器上。高级语言而不是汇编语言编写的程序不仅可以使未来的编译器为未来的机器生成代码，还可以使软件易于维护并运行在其他类型的计算机上。

谬误：商用计算机二进制兼容的重要性意味着成功的指令集不需改变。

在向后的二进制兼容是神圣不可侵犯的同时，图 2-43 显示了 x86 指令集的快速发展。在 35 年中，平均每个月至少增加一条新的指令。

陷阱：忘记在字节寻址的机器中，连续的字地址相差不是 1。

很多汇编程序员假定下一个字地址可以通过将寄存器的值加 1 来获得，而不是增加一个字的字节数，这使他们犯下很多错误。提前注意以便有所准备！

陷阱：在自动变量的定义过程外，使用指针指向该变量。

处理指针的常见错误是使用指向一个过程中局部数组的指针，从该过程传出结果。遵从图 2-12 中的栈规则，当过程返回时，包含局部数组的存储器将立即被重新使用。指向自动变量的指针会造成混乱。

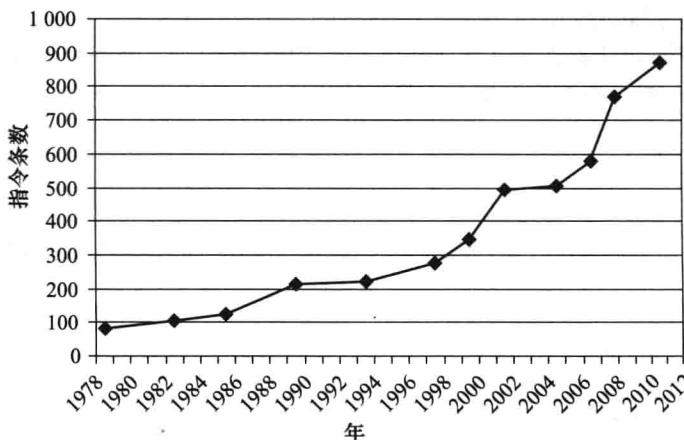


图 2-43 随时间推移 x86 指令集的增长。这种扩展是有一定的技术价值的，迅速的变化也增加了其他公司试图做兼容处理器的难度

2.20 本章小结

少就是多。

——Robert Browning, 《Andrea del Sarto》, 1855

存储程序计算机的两个准则是指令的使用与数字没有区别，以及使用可修改的存储器。这些准则使一台计算机可以在不同的领域辅助环境科学家、经济顾问和小说家。选择机器可以理解的指令集需要精妙的平衡程序执行需要的指令数目、指令执行所需的时钟周期数和时钟的速度。就像本章所描述的，在做精妙平衡时有 3 条准则可以指导设计者：

1) 简单源于规整。规整性使 MIPS 指令集具有很多特点：所有指令长度统一、算术指令总是需要三个寄存器操作数和寄存器字段在每种指令格式的位置相同。

2) 越小越快。对速度的要求导致 MIPS 只有 32 个寄存器而不是更多。

3) 优秀的设计需要好的折中。一个 MIPS 例子是在指令中提供更大地址与常数，并且保持所有的指令具有相同的长度之间的折中。

与计算机体系结构相同，在指令集中也会看到“加速大概率事件”的伟大思想。该思想在 MIPS 中的体现包括条件分支的 PC 相对寻址和大常数操作数的立即数寻址。

机器语言之上是人们可读的汇编语言。汇编器将翻译为机器可以理解的二进制数，它甚至通过创造硬件中没有的符号指令来“扩展”指令集。例如，较大的常量和地址被切割成合适的大小，常用的指令变体都有它们自己的名字，等等。图 2-44 列举了到目前为止我们讲过的 MIPS 指令，包括实际指令和伪指令。在更高级别隐藏细节是伟大思想“抽象”的另外一个例子。

每一类 MIPS 指令与编程语言中出现的结构相关：

- 算术指令对应于赋值语句中的运算。
- 传输指令很可能发生在处理像数组和结构体这样的数据结构时。
- 条件分支被用于 if 语句和循环。
- 无条件分支被用于过程调用和返回以及 case/switch 语句。

这些指令出现频率不相等，少数指令出现频率较大。例如，图 2-45 展示了 SPEC CPU 2006 中每类指令出现的频率。指令出现频率的不同在数据通路、控制通路和流水线的特征分析中扮演重要角色。

MIPS 指令	名称	格式	MIPS 伪指令	名称	格式
加	add	R	移位	move	R
减	sub	R	乘	mult	R
加立即数	addi	I	乘立即数	multi	I
取字	lw	I	取立即数	li	I
存字	sw	I	小于时跳转	blt	I
取半字	lh	I	小于或等于时跳转	ble	I
取无符号半字	lhu	I	大于时跳转	bgt	I
存半字	sh	I	大于或相等时跳转	bge	I
取字节	lb	I			
取无符号字节	lbu	I			
存字节	sb	I			
取链接字	ll	I			
存条件字	sc	I			
取立即数高位	lui	I			
与	and	R			
或	or	R			
或非	nor	R			
与立即数	andi	I			
或立即数	ori	I			
逻辑左移	sll	R			
逻辑右移	srl	R			
相等时跳转	bne	I			
不相等时跳转	bne	I			
小于时置位	slt	R			
小于立即数时置位	slti	I			
小于无符号立即数时置位	sltiu	I			
跳转	j	J			
跳转至寄存器所指位置	jr	R			
跳转和链接	jal	J			

图 2-44 到目前为止介绍过的 MIPS 指令集，左侧是真实的 MIPS 指令，右侧是伪指令。附录 A (A.10 节) 描述了完整的 MIPS 体系结构。图 2-1 展示了与本章相关的更细致的 MIPS 体系结构。这里给出的信息可在 MIPS 参考数据卡的第 1 和第 2 列查到

指令类别	MIPS 范例	相应的高级语言	出现频率	
			整型	浮点
算术	add, sub, addi	赋值语句中的操作	16%	48%
数据传输	lw, sw, lb, lbu, lh, lhu, sb, lui	对数据结构的引用，例如数组	35%	36%
逻辑	and, or, nor, andi, ori, sll, srl	赋值语句中的操作	12%	4%
条件分支	beq, bne, slt, slti, sltiu	if 语句和循环	34%	8%
跳转	j, jr, jar	过程调用，返回，case/switch 语句	2%	0%

图 2-45 MIPS 指令分类、范例以及相应的高级编程语言结构和 SPEC CPU 2006 测试程序执行时定、浮点指令所占的比例。第 3 章中的图 3-26 展示了每条 MIPS 指令执行时所占的平均比例

在第 3 章解释计算机算术运算之后，我们将继续揭示 MIPS 指令集体系结构。

2.21 历史观点和拓展阅读

本节概述了指令集体系结构 (ISA) 的历史，我们介绍了编程语言和编译器的简短历史。

ISA 包括累加器体系结构、通用寄存器体系结构、栈体系结构和 ARM 及 x86 的简史。我们还回顾了高级语言计算机体系结构中的争议问题和精简指令集体体系结构。编程语言的历史包括 Fortran、Lisp、Algol、C、Cobol、Pascal、Simula、Smalltalk、C++ 和 Java。编译器的历史包括重要的里程碑和实现它们的先驱。本节剩余部分在配套网站中的 2.21 节中。

2.22 练习题

附录 A 描述了对这些练习有帮助的 MIPS 的模拟器。尽管模拟器可以接受伪指令，但是在要求产生 MIPS 代码的习题中，尽量不要使用伪指令。你的目的是学习实际的 MIPS 指令集，如果问你指令数，你所给出的答案必须反映实际执行的指令数而不是伪指令。

有些情况必须使用伪指令（例如，当汇编时不知道真实值时，使用 `la` 指令）。还有些情况下，使用伪指令会更方便并使代码可读性变好（例如，`li` 和 `move` 指令）。如果你因为这些原因选择使用伪指令，请在伪指令开始的地方加上一两句话，说明你使用伪指令的原因。

- 2.1** [5] <2.2> 下面的 C 语言表达式对应的 MIPS 汇编语言代码是什么？假设给定变量 `f`、`g`、`h` 和 `i`，像在 C 程序中声明的一样它们都是 32 位的整数，使用最少的 MIPS 汇编指令。

`f = g + (h - 5);`

- 2.2** [5] <2.2> 下面的 MIPS 汇编语言程序段对应的 C 语言表达式是什么？

```
add  f, g, h
add  f, i, f
```

164

- 2.3** [5] <2.2, 2.3> 下面的 C 语言表达式对应的 MIPS 汇编代码是什么？假设变量 `f`、`g`、`h`、`i` 和 `j` 分别赋值给寄存器 `$s0`、`$s1`、`$s2`、`$s3` 和 `$s4`。假设数组 `A` 和 `B` 的基址分别在寄存器 `$s6` 和 `$s7` 中。

`B[8] = A[i-j];`

- 2.4** [5] <2.2, 2.3> 下面的 MIPS 汇编语言程序段对应的 C 语言表达式是什么？假设变量 `f`、`g`、`h`、`i` 和 `j` 分别赋值给寄存器 `$s0`、`$s1`、`$s2`、`$s3` 和 `$s4`。假设数组 `A` 和 `B` 的基址分别在寄存器 `$s6` 和 `$s7` 中。

```
sll  $t0, $s0, 2      # $t0 = f * 4
add  $t0, $s6, $t0    # $t0 = &A[f]
sll  $t1, $s1, 2      # $t1 = g * 4
add  $t1, $s7, $t1    # $t1 = &B[g]
lw   $s0, 0($t0)     # f = A[f]
addi $t2, $t0, 4
lw   $t0, 0($t2)
add  $t0, $t0, $s0
sw   $t0, 0($t1)
```

- 2.5** [5] <2.2, 2.3> 在不改变功能的前提下，重写习题 2.4 中的 MIPS 程序使其指令数目尽可能少。

- 2.6** 下表表示在主存中存放的一个数组的 32 位数据。

Address	Data
24	2
38	4
32	3
36	6
40	1

- 2.6.1** [5] <2.2, 2.3> 基于上表中数据在存储器中的位置，编写一段 C 代码，将数据从小到大排序，最小的数放在地址最低的位置。（假设这段数据代表了 C 的一个 Int 型数组 `Array`，并且这台特别的机器是按照字节寻址的，且一个字包含 4 字节。）

- 2.6.2** [5] <2.2, 2.3> 基于上表中数据在存储器中的位置，编写一段 MIPS 代码，将数据从小到大排序，最小的数放在地址最低的位置。（使用最少的 MIPS 汇编指令，假设 `Array` 的基址保存在寄存器 `$s6` 中。）

- 2.7 [5] <2.3> 分别画出数据 0xabcdef12 在大端编址和小端编址的机器上是如何分布在存储器中的。(假定数据从地址 0 开始存储。)
- 2.8 [5] <2.4> 将 0xabcdef12 转化为十进制。
- 2.9 [5] <2.2, 2.3> 把下面的 C 代码翻译为 MIPS 代码。假定变量 f、g、h、i 和 j 分别赋值给寄存器 \$s0、\$s1、\$s2、\$s3 和 \$s4。假定数组 A 和数组 B 的基址分别存放在 \$s6 和 \$s7 中。假定数组 A 和数组 B 中的元素均为 4 字节的字：
B[8] = A[i] + A[j];
- 2.10 [5] <2.2, 2.3> 把下面的 MIPS 代码翻译为 C 代码。假定变量 f、g、h、i 和 j 分别赋值给寄存器 \$s0、\$s1、\$s2、\$s3 和 \$s4。假定数组 A 和数组 B 的基址分别存放在 \$s6 和 \$s7 中。

```
addi $t0, $s6, 4
add $t1, $s6, $0
sw $t1, 0($t0)
lw $t0, 0($t0)
add $s0, $t1, $t0
```

- 2.11 [5] <2.2, 2.5> 对于每条 MIPS 指令，写出操作码 (OP)、源操作数 (RS) 和目标操作数 (RT) 的值 (value)。对于 I 型指令，写出立即数字段的值。对于 R 型指令，写出目的寄存器 (RD) 字段的值。

- 2.12 假定寄存器 \$s0 和 \$s1 分别存放数值 0x80000000 和 0xD0000000。

- 2.12.1 [5] <2.4> 下面汇编代码的 \$t0 的值是多少？

```
add $t0, $s0, $s1
```

- 2.12.2 [5] <2.4> \$t0 中的结果是期望的结果还是发生溢出后的结果？

- 2.12.3 [5] <2.4> 对于上面定义的寄存器 \$s0 和 \$s1 的内容，下面汇编代码的 \$t0 的值是多少？

```
sub $t0, $s0, $s1
```

- 2.12.4 [5] <2.4> \$t0 中的结果是期望的结果还是发生溢出后的结果？

- 2.12.5 [5] <2.4> 对于上面定义的寄存器 \$s0 和 \$s1 的内容，下面汇编代码的 \$t0 的值是多少？

```
add $t0, $s0, $s1
add $t0, $t0, $s0
```

- 2.12.6 [5] <2.4> \$t0 中的结果是期望的结果还是发生溢出后的结果？

- 2.13 假定 \$s0 中的值为 128_{10} 。

- 2.13.1 [5] <2.4> 对于指令 add \$t0, \$s0, \$s1，求使结果产生溢出的 \$s1 的值的范围。

- 2.13.2 [5] <2.4> 对于指令 sub \$t0, \$s0, \$s1，求使结果产生溢出的 \$s1 的值的范围。

- 2.13.3 [5] <2.4> 对于指令 sub \$t0, \$s1, \$s0，求使结果产生溢出的 \$s1 的值的范围。

- 2.14 [5] <2.2, 2.5> 写出下面的二进制数值对应的类型和汇编语言指令：

```
0000 0010 0001 0000 1000 0000 0010 00002
```

- 2.15 [5] <2.2, 2.5> 给出下面指令的类型和十六进制表示： sw \$t1, 32 (\$t2)

- 2.16 [5] <2.5> 写出用下面 MIPS 字段描述的指令的类型、汇编语言指令和二进制表示：

```
op=0, rs=3, rt=2, rd=3, shamt=0, funct=34
```

- 2.17 [5] <2.5> 写出用下面 MIPS 字段描述的指令的类型、汇编语言指令和二进制表示：

```
op=0x23, rs=1, rt=2, const=0x4
```

- 2.18 假设可以将 MIPS 寄存器文件扩展到 128 个寄存器，并将指令集中的指令数扩展为原来的 4 倍。

- 2.18.1 [5] <2.5> 这将如何影响 R 型指令的每个位字段的大小？

- 2.18.2 [5] <2.5> 这将如何影响 I 型指令的每个位字段的大小？

- 2.18.3 [5] <2.5, 2.10> 在提出的这两种变化中，每种变化如何减少一个 MIPS 汇编程序的大小？另一方面，如何增大一个 MIPS 汇编程序的大小？

- 2.19 假设如下寄存器内容：

```
$t0 = 0xAAAAAAAA, $t1 = 0x12345678
```

- 2.19.1 [5] <2.6> 对于以上的寄存器内容，执行下面的指令序列后 \$t2 的值是多少？

166

167

```
sll $t2, $t0, 44
or $t2, $t2, $t1
```

- 2.19.2** [5] <2.6> 对于以上的寄存器内容，执行下面的指令序列后 \$t2 的值是多少？

```
sll $t2, $t0, 4
andi $t2, $t2, -1
```

- 2.19.3** [5] <2.6> 对于以上的寄存器内容，执行下面的指令序列后 \$t2 的值是多少？

```
srl $t2, $t0, 3
andi $t2, $t2, 0xFFE
```

168

- 2.20** [5] <2.6> 找出完成如下功能的最短的 MIPS 指令序列：从寄存器 \$t0 中提取第 16 位到第 11 位，然后使用这些位替换寄存器 \$t1 的第 31 位到第 26 位，保持其他位不变。

- 2.21** [5] <2.6> 写出可用来实现下面伪指令的 MIPS 指令集的最小子集：

```
not $t1, $t2 // bit-wise invert
```

- 2.22** [5] <2.6> 对于下面的 C 语言表达式，写一个能够完成同样操作的最短 MIPS 汇编指令程序段。

假设 \$t1 = A, \$t2 = B, \$s1 是 C 的基地址。

```
A = C[0] << 4;
```

- 2.23** [5] <2.7> 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
j DONE
ELSE: addi $t2, $t2, 2
DONE:
```

- 2.24** [5] <2.7> 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？

- 2.25** MIPS 指令集不包含下面的指令：

```
rpt $t2, loop # if(R[rs]>0) R[rs]=R[rs]-1, PC=PC+4+BranchAddr
```

- 2.25.1** [5] <2.7> 如果要在 MIPS 指令集中实现该指令，哪种指令格式最合适？

- 2.25.2** [5] <2.7> 能够实现相同操作的最短 MIPS 指令序列是什么？

- 2.26** 考虑如下的 MIPS 循环：

```
LOOP: slt $t2, $0, $t1
      beq $t2, $0, DONE
      subi $t1, $t1, 1
      addi $s2, $s2, 2
      j LOOP
DONE:
```

- 2.26.1** [5] <2.7> 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？

- 2.26.2** [5] <2.7> 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。

- 2.26.3** [5] <2.7> 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？

- 2.27** [5] <2.7> 将下面的 C 代码翻译为 MIPS 汇编代码。要求使用的指令数目最少。假设值 a、b、i 和 j 分别存放在寄存器 \$s0、\$s1、\$t0 和 \$t1 中。另外假设寄存器 \$s2 中存放着数组 D 的基地址。

```
for(i=0; i<a; i++)
    for(j=0; j<b; j++)
        D[4*j] = i + j;
```

- 2.28** [5] <2.7> 实现习题 2.27 中的 C 代码用了多少条 MIPS 汇编指令？如果变量 a 和 b 分别初始化为 10 和 1，并且 D 中所有元素初始化为 0，将整个循环执行完成时，一共执行了多少条 MIPS 指令？

- 2.29** [5] <2.7> 将下面的循环翻译成 C 代码。假定寄存器 \$t1 中存放 C 语言级的整数 i，\$s2 中存放 C 语言级的整数 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

```

170

- 2.30** [5] <2.7> 将习题 2.29 中的循环重写以减少执行的 MIPS 指令。
- 2.31** [5] <2.8> 使用 MIPS 汇编实现下面的 C 代码。该函数一共执行了多少条 MIPS 指令？
- ```

int fib(int n){
 if (n==0)
 return 0;
 else if (n == 1)
 return 1;
 else
 return fib(n-1) + fib(n-2);
}

```
- 2.32** [5] <2.8> 函数经常被编译器实现为内联“in-line”的形式。内联函数是将函数体复制到程序空间中，以消除函数调用的开销。对于上面的函数，请用 MIPS 汇编实现内联版本的 C 代码。请问实现这个函数总共可以减少多少条 MIPS 汇编指令？（假设 C 的变量 n 被初始化为 5。）
- 2.33** [5] <2.8> 对于每一次函数调用，画出调用后栈的内容。（假定栈指针被初始化为 0x7fffffff，寄存器的使用情况和图 2-11 相同。）
- 2.34** 将下面的函数翻译成 MIPS 汇编语言。如果需要使用寄存器 \$t0 到 \$t7，请从编号小的寄存器开始使用。假设函数 func 的声明为 “int f (int a, int b);”，函数 f 的代码如下：
- ```

int f(int a, int b, int c, int d){
    return func(func(a,b),c+d);
}

```
- 171
- 2.35** [5] <2.8> 请问这个函数可以使用尾调用优化吗？如果不能，请说明原因。如果能，请说明优化前后执行 f 的指令数的差别。
- 2.36** [5] <2.8> 在习题 2.34 中函数 f 返回之前，我们可以知道寄存器 \$t5、\$s3、\$ra 和 \$sp 的内容吗？（注意，我们知道函数 f 的全部，但是我们只知道函数 func 的声明。）
- 2.37** [5] <2.9> 用 MIPS 汇编语言写一段代码将包含十进制正整数和负整数的 ASCII 码的数串转换成整数。在程序中使用寄存器 \$a0 处理由数字 0~9 组成的非空串的地址。程序应该计算与这个数字串等值的整数，并将这个整数存放在寄存器 \$v0 中。如果在字符串的任意位置出现非数字字符，程序停止并将 -1 存入 \$v0。例如，如果寄存器 \$a0 指向 3 字节的序列 50₁₀, 52₁₀, 0₁₀（非终结的字符串“24”），当程序停止的时候，寄存器 \$v0 中的值应该是 24₁₀。
- 2.38** [5] <2.9> 对于如下代码：
- ```

lbu $t0, 0($t1)
sw $t0, 0($t2)

```
- 假设寄存器 \$t1 中存放地址 0x1000 0000，寄存器 \$t2 中存放地址 0x1000 0010。注意 MIPS 体系结构使用大端地址。假设地址 0x1000 0000 的数据是 0x11223344。寄存器 \$t2 指向的地址中存放的数值是多少？
- 2.39** [5] <2.10> 请编写能产生 32 位常数 0010 0000 0000 0001 0100 1001 0010 0100<sub>2</sub> 的 MIPS 代码，并将值存储到寄存器 \$t1 中。
- 2.40** [5] <2.6, 2.10> 如果当前 PC 值是 0x00000000，可以使用单独的跳转指令跳转到练习题 2.39 中所指定的 PC 地址吗？
- 2.41** [5] <2.6, 2.10> 如果当前 PC 值是 0x00000600，可以使用单独的分支指令跳转到练习题 2.39 中所指定的 PC 地址吗？
- 2.42** [5] <2.6, 2.10> 如果当前 PC 值是 0x1FFF f000，可以使用单独的分支指令跳转到练习题 2.39 中所指定的 PC 地址吗？
- 172

- 2.43** [5] <2.11> 写出实现下面 C 代码的 MIPS 汇编代码:

```
lock(1k);
shvar=max(shvar,x);
unlock(1k);
```

假设变量 1k 的地址在 \$a0 中, 变量 shvar 的地址在 \$a1 中, 变量 x 的地址在 \$a2 中。你所编写的这个重要部分的代码不能包含任何函数调用。使用 ll/sc 指令实现 lock() 操作, 而 unlock() 操作可以简单地使用存数指令。

- 2.44** [5] <2.11> 重新解决练习题 2.43 中的问题, 不过这次使用 ll/sc 直接完成 shvar 变量的原子更新操作, 不使用 lock() 和 unlock()。注意这个问题中没有变量 1k。

- 2.45** [5] <2.11> 以练习题 2.43 中的代码为例, 解释当两个处理器同时执行这段临界区域时, 将发生什么情况? 假设每个处理器执行一条指令正好需要一个周期。

- 2.46** 假设给定处理器的算术指令的 CPI 是 1, 取数/存数指令的 CPI 是 10, 分支指令的 CPI 是 3。假设一个程序由 5 亿条算术指令、3 亿条取数/存数指令和 1 亿条分支指令组成。

- 2.46.1** [5] <2.19> 假设向指令集中添加了新的、功能更强的算术指令。通过使用这些功能更强大的算术指令平均可以减少程序执行所需要的 25% 的算术指令, 而时钟周期的开销增长了 10%。请问这是好的设计选择吗? 为什么?

- 2.46.2** [5] <2.19> 假设我们找到一种可以使算术指令性能达到原来两倍的方法。请问我们机器的整体加速是多少? 假设我们找到一种可以使算术指令性能达到原来 10 倍的方法, 那么机器的性能整体加速又是多少?

- 2.47** 假设一给定程序共执行了 70% 的算术指令、10% 的取数/存数指令和 20% 的分支指令。

- 2.47.1** [5] <2.19> 假设执行一条算术指令、取数/存数指令和分支指令分别需要 2 个周期、6 个周期和 3 个周期, 求平均 CPI。

- 2.47.2** [5] <2.19> 在取数/存数指令和分支指令执行时间不变的情况下, 如果要使性能提升 25%, 则算术运算指令的平均执行时间应该为多少?

- 2.47.3** [5] <2.19> 在取数/存数指令和分支指令执行时间不变的情况下, 如果要使性能提升 50%, 则算术运算指令的平均执行时间应该为多少?

## 01 小测验答案

**2.2** MIPS, C, Java

**2.3** 2. 非常慢

**2.4** 2.  $-8_{10}$

**2.5** 4. sub \$t2, \$t0, \$t1

**2.6** 都可以。将“逻辑与”和全“1”的掩码一起使用会导致除了想要的区域之外, 都变成 0。正确的左移位操作将左边的位数都移走。合适的右移将一个字最右边的区域都移走, 将 0 留在字中。注意到“逻辑与”操作会保留原始的值, 移位操作对将需要的区域移动到字的最右边。

**2.7** I. 全对, II. 1。

**2.8** 两个都正确。

**2.9** I. 1 和 2, II. 3。

**2.10** I. 4. + -128K, II. 6. 一个 256M 的块, III. 4. sll。

**2.11** 两个都正确。

**2.12** 4. 与机器无关。