第五章

转移指令的寻址方式

①段内直接转移：JMP NEAR PTR L2

②段内间接转移：JMP BX，JMP WORD PTR [BX]

③段间直接转移：JMP FAR PTR L3

④段间间接转移：JMP DWORD PTR [DI]

控制转移指令

•无条件转移指令

- 条件转移指令
- 循环指令
- 子程序调用指令
- 中断指令

JMP（JuMP）

格式：JMP 目标地址

无条件地转移到指令指定的地址去执行该地址开始的指令。

JMP 含上面所讲的5中寻址方式（加上段内直接短转移）

条件转移指令

条件转移指令的寻址方式是**相对寻址方式**(短转移)

目标地址在本指令的下一条指令的-128～127之间，操作数是一个8位的二进制补码。

单个标志的条件转移指令

JZ（JE） JNZ（JNE） ZF为0/1

JS JNS SF=1/0 有/无符号跳转

JO JNO 溢出跳转

JP（JPE） JNP（JPO）偶校验跳转/奇校验跳转 PF= 1/0

JC JNC 进位跳转

无符号数的条件转移指令

•这是根据两个条件（标志位CF和ZF）同时测试的条件转移指令。

•格式及执行的操作同单个标志位的条件转移指令
JB（JNAE，JC） 小于跳转

JNB（JAE） 不小于跳转

JBE（JNA）小于等于跳转

JNBE（JA）大于跳转

带符号数的条件转移指令

比较两个有符号数，根据比较结果转移

JL（JNGE）小于跳转

JNL（JGE）不小于跳转

JLE（JNG）小于或等于跳转

JNLE（JG）大于跳转

测试CX转移指令

格式： JCXZ OPR

测试条件：（CX）=0
当CX=0时，则转移到OPR指出的转移地址去执行。

循环指令

•LOOP 循环指令

格式：LOOP OPR

测试条件：CX<>0

•LOOPZ/LOOPE 为零或相等时循环指令

格式：LOOPZ OPR 或LOOPE OPR

测试条件：ZF=1且CX<>0

•LOOPNZ/LOOPNE 不为零或不相等时循环指令

格式：LOOPNZ OPR 或LOOPNE OPR

测试条件：ZF=0且CX<>0

子程序调用和返回指令

•CALL子程序调用指令

段内直接调用

段内间接调用

段间直接调用

段间间接调用

•RET从子程序返回指令

段内返回

段内带立即数返回

段间返回

段间带立即数返回

段内直接调用

格式： CALL DST

其中，DST是子程序入口地址的符号地址。

执行的操作： 先SP =SP-2，IP入栈

再转到子程序的入口地址继续执行。

段内间接调用

格式： CALL DST

其中，DST是寄存器操作数和内存操作数， 当然不允许立即数和段寄存器。

执行的操作： 先SP =SP-2，IP入栈

再IP =（EA），转入。

段间直接调用

格式： CALL DST

或 CALL FAR PTR DST

其中，DST是子程序入口地址的符号地址。

执行的操作： 先SP =SP-2，CS入栈

SP =SP-2，IP入栈

再转到子程序的入口地址继续执行。

段间间接调用

格式： CALL DST

其中，DST只能是内存操作数。

执行的操作： 先SP ÜSP-2，CS入栈

SP =SP-2，IP入栈

再IP =（EA）， CS =（EA+2）

转入。

段内返回指令

格式： RET

执行的操作： 先IP =(SP+1)(SP)， SP =SP+2

返回主程序继续执行。

与段内调用子程序指令相对应

段内带立即数返回指令

格式： RET EXP

其中，EXP是表达式，其结果为常数。

执行的操作： 先IP =(SP+1)(SP)， SP =SP+2

（返回主程序继续执行）

再SP =SP+D16

例如：RET 4

段间返回指令

格式： RET

执行的操作： 先IP Ü(SP+1)(SP)， SP ÜSP+2

CS Ü(SP+1)(SP)， SP ÜSP+2 返回主程序继续执行。

与段间调用子程序指令相对应。