3.1.10指令

An instruction is a statement that becomes executable when a program is assembled. Instructions are translated by the assembler into machine language bytes, which are loaded and executed by the CPU at runtime. An instruction contains 4 basic parts:

* Lable(optional)
* Instruction mnemonic(required)
* Operand(s)(usually required)
* Comment(optional)

This is the basic syntax:

[label:]mnemonic[operands][;comment]

3.5.1等号伪指令

当前地址计数器：最重要的符号之一被称为当前地址计数器（current location counter），表示为$。下面语句声明了一个变量selfPtr,并将其初始化为该该变量的偏移量：

SelfPtr DWORD $

5.2.1PROC伪指令

过程定义（非正式）：由返回语句结束的已命名的语句块。

Main PROC

Statement

Main ENDP

当在启动过程之外创建一个过程时，就用RET指令来结束它，RET强制CPU返回到该过程被调用的位置：

Sample PROC

Statement

RET

Sample endp

过程标号jmp destination，到只在被定义的过程中可见，全局标号定义destination::(两个顿号)

6.2.1 CPU flags

操作结果等于0，零标志位1

操作使目标操作数的最高位有进位时，进位标志位1

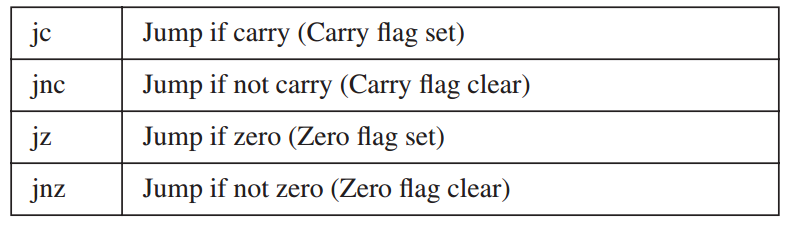
The sign flag is a copy of the high bit of the destination operand, indicating that it is negative if set and positive if clear.

The overflow flag is set when an instruction generates an invalid signed result.

The parity flag is set when an instruction generates an even number of 1 bits in the low byte of the destination operand.

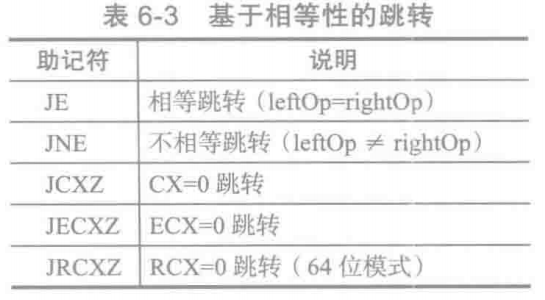
6.3.2 Jcond指令

当状态标志条件为真时，条件跳转指令就分支到目标标号；否则，当标志位条件为假，立即执行条件跳转后面的指令。



CPU status flags are most commonly set by arithmetic, comparison and boolean instructions. Conditional jump instructions evaluate the flag state, using them to determine whether or not jumps should be taken.









8.高级过程

调用程序向子程序传递的数值被称为实际参数（arguments），而被调用的子程序要接受的数值被称为形式参数（parameters）。

8.2.7 LEA指令

LEA指令返回间接操作数的地址。由于间接操作数中包含一个或多个寄存器，因此会在运行时计算这些操作数的偏移量。

注：不能用OFFSET获取堆栈参数的地址，因为OFFSET只适用于编译时已知的地址，下面语句无法汇编：mov esi,OFFSET [ebp-30]

10章

