3 月 5 日《计算机系统》理论课—汇编进阶

课堂要点

本次课堂教学重点进一步介绍汇编语言的重点内容，包括：**压栈与弹栈操作、基本与特殊的运算操作指令、条件码、无条件跳转、条件跳转、条件传送、标志位设定、循环指令。**需要指出的是，目前的内容都只是做**简单介绍**，让学生对上述内容有简单了解，能够在阅读代码时知道该指令执行的操作即可，**暂不要求明白其操作的原理**。

1. **压栈与弹栈**是非常重要的机器操作，本次学习中特别要注意的是：

   栈的特点：向下增长，栈顶地址最小；

   压栈就是 1）拉开抽屉（esp 减小要压入数据的字节数）2）放入数据（高位数据放入高地址，低位数据放入低地址）。

   弹栈就是：1）拿出数据（字节数取决于 pop 后缀或者目的寄存器，同时高地址数据放入目的寄存器高位）；2）关上抽屉（esp 增加对应字节数）

2. **基本与特殊的运算操作指令**只需要**记住名称和具体操作**，尤其是**操作的顺序**（例如减法是后面减前面，结果放入后面）；

3. 最重要的**四个条件码**：

   1）CF: 将运算看做“无符号数运算”，如果有进/借位，则置 1；

   2）OF：将运算看做“有符号数运算”，如果产生溢出，则置 1；

   3）SF: 如果运算结果最高位是 1，则置 1；

   4）ZF: 如果运算结果是 0，则置 1.

4. **无条件跳转 jmp；直接跳转到指定的地址**，即：将其操作数作为地址写入%eip，实现 CPU 指令执行的改变。**四种方式**：

   jmp LABEL 直接使用 LABEL 所在的地址

   jmp *LABEL 使用 LABEL 地址中存的地址（间接）

   jmp 0x8048056 直接使用立即数作为跳转的地址

   jmp *%eax 将%eax 中的内容作为跳转的地址

5. **条件跳转**：依据条件码的不同组合，可以判定大小关系，依据大小关系来决定的跳转就是条件跳转。指令符形式为 **J 后面接表示判定结果的后缀**，例如：JGE，就是：jump if greater or equal—当大于或等于时跳转。

6. **cmov（条件传送）**，功能与格式和 mov 完全相同，不同在于它和条件跳转一样有后缀，满足后缀表示的比较关系才进行数据传送，例如：

comvge %ax,%bx 当大于或等于时才将%ax 的内容传给%bx

7. **标志位设定指令（set）**是将后面跟着的操作数(一个字节)设为 1，前提是判定结果满足其后缀，例如：setge %al 表示当大于或等于时将%al 置 1。这样，比较的结果就以一个字节 1 的形式保留下来。

8. **循环在机器中就是通过条件跳转来实现的**。后面的学习中我们将看到各种不同的循环模式在机器中的具体实现。本节课只要求大家人知道条件跳转是如何实现循环的。

循环体执行后，进行判定（循环变量，或者其它循环结束条件），不满足条件，直接跳转到循环体外的下一条指令地址处；满足条件，跳转回循环体开始阶段。