**《微机原理及应用》实验报告**

实验一：调试程序debug.exe的使用

专业班级： 计科20-02

学生学号： 542001020223

学生姓名： 原彬贺

指导教师： 韩继辉

成 绩：

1、实验目的

正文使用小四号宋体，1.15倍行间距。插图大小要合适，图和表需标明题注。

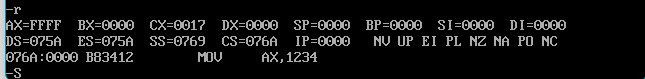
1、掌握debug.exe常用命令的功能；

2、通过debug.exe编写指令序列，并能够调试简单的程序。

2、实验环境、内容及要求

1、内容、要求

1）启动DEBUG（开始菜单->cmd），用“R”命令显示各寄存器值,记录并说明DEBUG的初始工作环境。

初始工作环境除了ds ip es ss cs地址寄存器外，其他通用寄存器的值均为0，如图表1所示

图表 1 初始寄存器状态

2）认真学习"D"命令、“E”命令、“R”命令的功能、应用、命令格式、各种显示信息及含义，自行设计操作进行，掌握它们的用法，要求做到能对不同地址中的内容和寄存器进行熟练的检查和修改。记录练习的操作和过程，解释结果；说明各个寄存器的初值以及段地址、偏移地址的意义，确实掌握地址与其中存放的数据之间的关系。

3）阅读下列源程序指令，填写运行结果。再用“A”命令输入这些源程序指令(运行结果部分不输入):

地址 目标代码 源程序指令运行结果

076A：0000 MOV AX, 1234； AX:\_1234\_

076A：0003 INC AX； AX:1235 CF:\_0\_ ZF:0 SF:\_1

076A：0004\_ DEC AH； AH：11 CF:0 ZF:0 SF:1

076A：0006 ADD AH,78； AH：89 CF 1 ZF:0 OF:0 SF:1

076A：0009 AND AH,C8； AH:51 PF:\_1\_ ZF:\_0\_

076A：000c OR AL,9F； AL: bf\_PF:\_0\_ ZF:\_0\_

076A：000e XOR AL,59； AL: e6\_PF:\_1\_ ZF:0\_\_

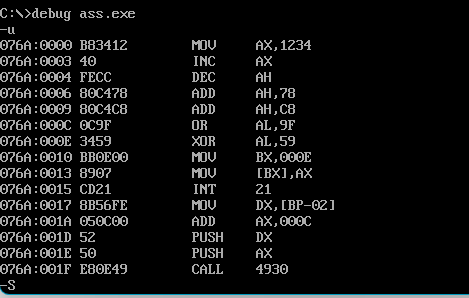
076A：0010 MOV BX,000E； BX:\_000e\_

076A：0013 MOV [BX],AX； DS:000EH

076A：0015 INT 20； ;程序终止

说明：程序中的段地址CS和DS，由DEBUG确定，不另外设置。

1. 用“U”命令反汇编这段程序，再与原输入指令对照检查，记录并解释两者差别。

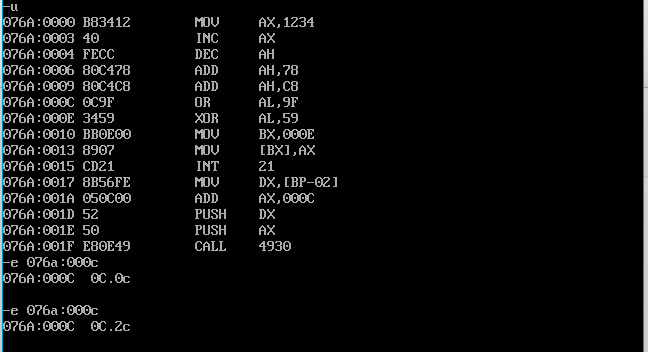
通过图表2看到，编写的代码转化为二进制指令后再进行反汇编，其形式内容是一样的，二进制指令的末尾默认增加了一些指令，用以保存返回值并返回到其主程序。

图表 2 U命令查看

B. 根据汇编结果，将各条指令的存放地址及目标代码分别填入上面的地址和目标代码栏中，分析目标代码，体会操作码与操作数之间的关系。

C. 用“T”命令单步执行这段程序，核对运行结果和各标志位的设置，熟悉它们的表示形式。

D. 设置IP到程序开始地址，用“G”命令设置断点（任选），执行这段程序，检测运行结果。改变不同断点方式多次重复这一步，总结体会断点选择的目的性与应用技巧。

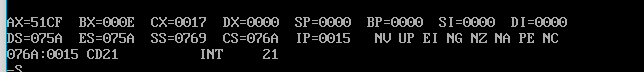
E. 将 OR AL，9FH 指令修改为 SUB AL,9FH（提示：这两条指令的机器码长度相同，可以查看其机器码的区别，用内存单元修改指令“E”进行修改），比较指令代码和运行结果的不同。

图表 3修改指令

更改前结果，如图表4所示：

图表 4 更改前执行结果

更改后结果，如图表5所示：



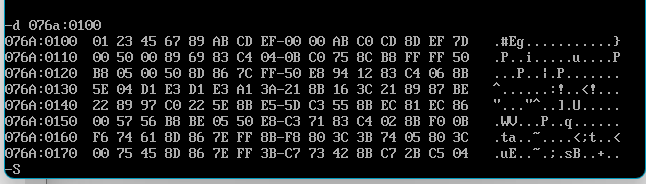
图表 5更改后执行结果

通过对比可以发现，只有al变化了，由原本的E6变为了CF。

F. 根据反汇编和程序运行过程IP的变化，详细分析指令地址、目标代码、程序指令、指令代码存放规律之间的关系，深入理解程序存储原理与控制器自动控制执行的机理。

程序指令由指令代码和伪指令组成，其一般是更高层次的语言，较为容易阅读。程序指令通过编译形成二进制指令即目标代码，但是此时其不同文件中指令的地址用符号代替的，并未形成一个整体，当通过链接操作后，不同文件中地址形成了关联，形成逻辑地址。当运行时，指令中的地址再变为物理地址。指令地址便是上一条指令地址加上一条指令所占的字节，在运行时确定。

4）自编指令段，学习每一种寻址方式的传送指令，算术、逻辑运算指令及对标志位的影响。记录指令的设计、目的及结果。

5）用“E”命令从cs:0100开始设置一段字符数据“0123456789ABCDEF0000”，再用“U”命令反汇编这一段数据，分析并体会计算机中程序与数据之间、数据与字符之间的关系。

图表 6 插入数据段

可以看到在程序cs：0100到cs：0109，是该段字符数据“0123456789ABCDEF0000”。

在程序中，程序就是二进制的数据，而字符也是数据，去本质均是二进制的数据，只是处理器对他们的解析方式不同，造成了不同的结果。

2、实验安排方式：每组1人，独立完成上机实验

4、实验总结

通过本次实验，我学会了使用masm先对asm文件进行编译，再使用link文件对其进行链接操作，之后再使用debug生成的可执行文件进行调试操作。

同时，在进行debug调试的过程中，我也学会了许多debug的命令，比如-R查看寄存器内容，-T进行单步执行操作，-D进行内存内容查看，-E进行内存内容的替换，而-U进行代码的反汇编，同时还有G的断点操作，使我在debug的过程中对于程序状态的了解更加得心应手。这次实验使我收获很大，使我对于程序从汇编到机器指令的过程有了更加深入的理解。