《汇编语言程序设计实验》注意事项

请大家在网站上下载实验报告样例和实验报告评分原则，上机前做好准备，需要完成实验报告中除上机实验记录和体会以外的全部内容。上机时主要是验证所做结果是否正确，记录实验中看到的现象（如果截图，必须对截图中反映的信息给出文字说明），分析各种现象的内在原理，找出错误的原因，以促进对课本知识的理解。

到机房上机要签到、以班级为单位安排座位、检查实验报告预习情况；提前完成的需经过老师检查后方可离开机房。

请大家参考配套的《80X86汇编语言程序设计上机指南》（华中科技大学出版社2007年）相关内容。

上机使用的相关软件请从汇编教学网站上下载（比如MASM60TD的压缩包等）。自备U盘带相关软件和电子版实验报告，实验报告文件名格式：

CS1401\_ U201412345张三丰\_1.DOC

实验课程成绩=实验报告（70%）+现场实验操作表现（20%）+现场问答讨论（10%）

其中，最终提交的实验报告是8次实验报告的整合，作为终结成绩（每次实验后只需要提交电子版的实验报告，注意，为避免没有收到邮件，学生必须收到回复邮件后才算确认提交成功。8次实验完毕后，提交纸质报告，是8个报告的合订本，外加一个统一的封面）。实验报告评分中包括实验完成质量与撰写质量。

《汇编语言程序设计实验》

第一次上机实验任务

实验名称：实验一 简单程序设计，DOS功能调用，上机操作与TD的使用。

一．实验目的和要求

(1) 掌握汇编源程序编辑工具、汇编程序、连接程序、调试工具的使用；

(2) 理解数、符号、寻址方式等在计算机内的表现形式；

(3) 理解指令执行与标志位改变之间的关系；

(4) 熟悉常用的DOS功能调用。

二．实验内容

任务1. 《80X86汇编语言程序设计》教材中 P31的 1.14题。

要求：(1) 直接在TD中输入指令，完成两个数的求和、求差的功能（可以省略实验报告中的程序框图）。求和/差后的结果放在(AH)中。

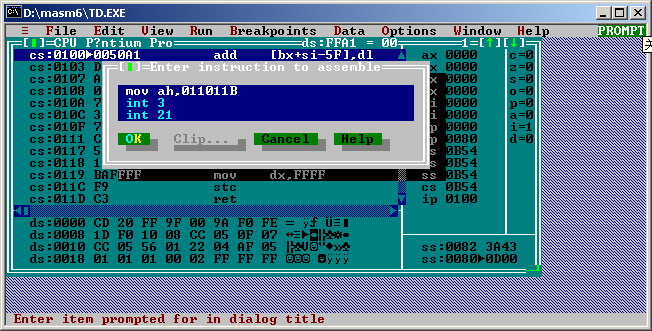
(2) 请事先指出执行指令后(AH)、标志位 SF、OF、CF、ZF的内容。

(3) 记录上机执行后的结果，与（2）中对应的内容比较。

(4)求差运算中，若将A、B视为有符号数，且A>B, 标志位有何特点？

若将A、B视为无符号数，且A>B, 标志位又有何特点？

**在TD中输入指令语句的操作提示：**将TD中的代码显示区置为当前区域，光标移到期望修改的行后，直接输入汇编指令；当输入了第一个字符时，TD自动弹出如下图所示的指令编辑窗口。每输入完一条指令，按回车键，这时输入的指令即可出现在光标处，同时光标自动下移一行，以便输入下一条指令。



任务2. 《80X86汇编语言程序设计》教材中 P45的 2.3题。

要求：（1）可以省略实验报告中的程序框图和源程序。

（2）分别记录执行到“MOV CX，10”和“INT 21H”之前的(BX), (BP),(SI),(DI)各是多少。

（3）记录程序执行到退出之前数据段开始40个字节的内容，指出 程序运行结果是否与设想的一致。

(4)在标号LOPA前加上一段程序，实现新的功能：先显示提示信息“Press any key to begin!”, 然后，在按了一个键之后继续执行LOPA处的程序。

**操作提示：**使用TD.EXE调试程序时，应先单步执行各个语句，每执行一条语句，都应观察数据段中的内容以及相应寄存器的变化。首先注意观察对DS寄存器的赋值过程，并在TD的数据窗口定位待观察的数据区位置。其次，单步执行循环体两遍且正确理解了循环体语句的含义后，可在“MOV AH, 4CH”处设置断点，然后直接执行到断点处，回答(2)和(3)的问题。

任务3. 《80X86汇编语言程序设计》教材中 P45的 2.4题的改写。

要求：(1) 实现的功能不变，对数据段中变量访问时所用到的寻址方式中的寄存器改成32位寄存器。

(2) 内存单元中数据的访问采用变址寻址方式。

(3) 记录程序执行到退出之前数据段开始40个字节的内容，检查 程序运行结果是否与设想的一致。

(4)在TD代码窗口中观察并记录机器指令代码在内存中的存放形式，并与TD中提供的反汇编语句及自己编写的源程序语句进行对照，也与任务2做对比。（相似语句记录一条即可，重点理解机器码与汇编语句的对应关系，尤其注意操作数寻址方式的形式）。

（5）观察连续存放的二进制串在反汇编成汇编语言语句时，从不同字节位置开始反汇编，结果怎样？理解 IP/EIP指明指令起始位置的重要性。

**操作提示：**同任务2。

**上述任务中，重要操作环节（纳入到学生自己写的实验步骤中）提示：**

本次实验中需要学生尝试体会的操作可分为三类：

1. TD的操作（直接在TD内输入指令，设置断点、单步执行程序、运行到断点、运行到指定的指令、查看寄存器的内容、查看标志寄存器的某个标志位的值、查看指定的存储单元的值、查看整个程序在内存中的存放方式）；

2. 将一个汇编源程序生成一个可执行文件的步骤，包括如何读懂汇编源程序在汇编过程中产生的错误信息；编辑工具的使用（使用Edit， notepad等需要注意的问题）；

3. 操作数寻址方式的改变，对目标码产生的影响； DOS系统功能调用中应注意的问题。

各实验任务中的上述三类操作的具体提示如下表：

|  |  |  |
| --- | --- | --- |
| 任务编号 | 序号 | 学生尝试的操作 |
| 任务1 | 1 | 打开TD之后，如何在代码区输入一条指令，并且执行这条指令？ |
| 2 | 如何在代码区输入若干条指令后，再从输入的第一条指令开始执行？ |
| 3 | 在输入一条指令中的数据时，若以16进制输入，需要注意什么问题？ |
| 4 | 输入指令MOV AH, -128并执行 查看AH寄存器的内容 |
| 5 | 任务1中的(1)~(4) |
| 6 | 执行一条指令后，如何查看寄存器的值（含32位寄存器）？如何修改寄存器的值？ |
| 7 | 执行一条指令后，如何查看标志寄存器的值？ |
| 8 | 经过6，7后，总结加减法对标志寄存器的影响？ |
| 任务2和任务3 | 1 | 如何将一可执行程序调入TD，并查看代码区？理解机器码与汇编指令之间的对应关系？ |
| 2 | 如何设置断点并运行到断点？ |
| 3 | 如何使程序运行到光标的当前点？（假设活动光标在代码区，指向某一条指令） |
| 4 | 如何单步执行一条指令？（多种方法） |
| 5 | 在数据区找到数据段的方法？思考：是否可以用这一方法查看代码段甚至整个程序?（至少有三种方法：(1)goto，DS：偏移地址，(2)goto, 直接输入：段寄存器的值：偏移地址；(3)直接在数据区用光标移动查找） |
| 6 | 修改某个指定的存储单元的值，如任务2中的BUF2 |
| 7 | 如何查看堆栈？ |
| 8 | 如何汇编一个汇编源程序并链接产生可执行代码？ |
| 9 | 如何读懂源程序在汇编过程中产生的错误？ |
| 10 | 使用DOS系统功能调用前应注意保存AX寄存器的值？ |
| 11 | 查看BUF2等变量在TD中的表示形式并总结？ |
| 12 | 查看寄存器间接寻址、变址寻址的汇编源程序经汇编、链接后在TD中的表示形式？总结源程序的指令和TD中的指令差异。 |
| 13 | 单步执行循环体2遍，查看数据段的变化? |