《汇编语言程序设计实验》注意事项

请大家在课堂群或答疑群里下载“2020实验报告样例”，仔细阅读其中的相关说明。

网课期间，课内学时上机时段仍要签到。课内学时上机前需要做好一定的准备，即：对该次4学时上机时段内希望完成的每个任务，需要完成实验报告中 “实验记录与分析”之前的全部内容（称之为预习报告，预习报告不要求很完善，后续可以修改）。课内上机学时开始前要将该预习报告通过邮件发给指导老师。**预习报告**电子版文件名格式：

CS1801\_ U201812345张三丰\_P1.DOC

课内学时上机时，主要是在预习报告的基础上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），分析讨论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。完成某次实验后的实验报告电子版提交时间是当次实验课的课时全部结束后的次日，推迟提交将影响成绩。

**实验报告**电子版文件名格式：

CS1801\_ U201812345张三丰\_1.DOC

注意：预习报告文件名中的“\_P1”表示第1次上机4学时对应的预习报告，“\_P8”表示第8次上机4学时（最后一次上机）对应的预习报告，而实验报告文件名中的“\_1”表示实验一做完之后的实验报告，“\_5”表示最后一个实验五做完之后的实验报告。实验报告是对预习报告完善之后的结果。无论是预习报告还是实验报告，后一次的报告都是接着前一次的报告后面写的，不要把前一次报告的内容删掉了。

注意：签到考勤将影响课程综合评分，无故缺勤1/3以上课内上机实验学时者，实验课程成绩为不及格。

全部实验（8次上机完成5个实验）完成之后要提交含有5次实验内容的实验报告的纸质版，作为终结成绩（平时在每个实验结束后只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。5个实验完毕后，提交纸质版实验报告的同时，还需要将实验报告电子版、每次实验的所有源程序、执行程序一起打包提交。

另外请注意，从实验报告评分要求可以看出，汇编语言程序设计实验更强调实验的过程与思考，而不是把某个功能的程序调通了就完事。一个如实记录了实验过程及进行了深入分析思考的实验报告的成绩，就算程序没有调通，都可能比一个程序没有问题但没有什么过程记录与思考的实验报告成绩高很多。 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（例如：虚拟机DOSBOX，汇编程序MASM60，调试工具TD；混合编程时采用BC31或VS2019；WIN32编程采用MASM32或VS2019，跟踪程序时的反汇编工具OLLYDBG等）请从QQ群或网上下载。

《汇编语言程序设计实验》

实验一任务

实验名称：编程基础

本实验课内学时4+4，即占用两周课内实验课时，该部分实验报告的电子版在第二次课内学时完成后的次日提交。

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TD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. 熟悉操作系统的常用功能调用，如常用的DOS功能调用；
5. 熟悉分支、循环程序的结构及控制方法，掌握分支、循环程序的调试方法；
6. 加深对转移指令及一些常用的汇编指令的理解；
7. 掌握设计实现一个原型系统的基本方法。

二．实验内容

（上机实验环境说明：计算机配置较好时使用VMWare Workstation的虚拟机环境，或者DOSBox虚拟机；在普通便携计算机上建议使用DOSBox虚拟机。源程序编辑工具可以使用记事本、EDIT、或C语言的编辑器；汇编程序使用MASM 6.0;连接程序使用LINK；调试工具使用TD；具体介绍可参见教材第7章及《80X86汇编语言程序设计上机指南》）

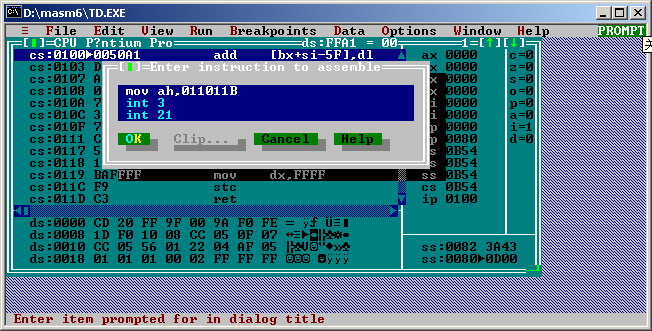
**任务1.1 《80X86汇编语言程序设计》教材中 P31的 1.14题。要求：**

(1) 直接在TD中输入指令（不需要编写完整程序），完成两个数的求和、求差的功能。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。

**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1.2 《80X86汇编语言程序设计》教材中 P45的 2.3题。要求：**

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

（2）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。

**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(1)和(2)的问题。

**任务1.3 《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，但对数据段中变量访问时所用到的变址寄存器采用32位寄存器。

(2) 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。

(3)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1.2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编码形式，比如寄存器间接寻址、变址寻址、32位寄存器与16位寄存器编码的不同、段前缀在代码里是如何表示的等）。

（4）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：**要让TD从任意指定地址开始反汇编，需要使用TD在代码显示区的Goto功能，即鼠标选中代码显示区，点击右键将显示带有Goto的菜单，选中Goto菜单项，输入CS:XXXX即可（XXXX是你希望录入的偏移地址）。

**任务1.4 设计实现一个网店商品信息管理系统。**

该系统的基本需求见“2020实验报告样例”文档中的“实验任务的总体描述”。

根据系统的基本需求，可以制定如下的数据段的定义（供参考）：

BNAME DB ‘ZHANG SAN’,0 ；老板姓名（本实验要求必须是自己名字的拼音）

BPASS DB ‘test’，0，0 ，0 ；密码

AUTH DB 0 ；当前登录状态，0表示顾客状态

GOOD DB/DW … ；当前浏览商品名称或地址（自行确定）

N EQU 30

SNAME DB ‘SHOP’,0 ；网店名称，用0结束

GA1 DB ‘PEN’, 7 DUP(0) ，10 ；商品名称及折扣

DW 35，56，70，25，？ ； 推荐度还未计算

GA2 DB ‘BOOK’, 6 DUP(0) ，9 ； 商品名称及折扣

DW 12，30，25，5，？ ；推荐度还未计算

GAN DB N-2 DUP( ‘TempValue’ ,0,8，15，0，20，0，30，0，2，0，？，？) ;除了2个已经具体定义了的商品信息以外，其他商品信息暂时假定为一样的。

本次实验主要是利用分支、循环程序的结构，实现该系统的基本功能，并能熟悉全周期、全流程地设计实现一个原型系统的基本方法。本次实验要具体实现的功能要求如下：

0.主菜单界面

完整显示“实验任务的总体描述”中给出的界面信息。等待用户输入数字（可使用1号DOS系统功能调用）。对用户输入的字符进行判断，看是否是1~9的数字；是的话就转移到对应功能的程序标号，不是的话就提示错误，回到主菜单界面。

1.登录/重新登录

（1）先后分别提示用户输入姓名和密码（可使用9号DOS系统功能调用）。

（2）分别获取输入的姓名和密码（可使用10号DOS系统功能调用）。输入的姓名字符串放在以in\_name为首址的存储区中，密码放在以in\_pwd为首址的存储区中。

（3）若输入姓名时只是输入了回车，则将0送到AUTH字节变量中，回到主菜单界面。

（4）进行身份认证：

（a）使用循环程序结构，比较姓名是否正确。若不正确，则跳到（c）。

（b）若正确，再比较密码是否相同，若相同，跳到（d）。

（c）若名字或密码不对，则提示登录失败，并转到“（3）”的位置。

（d）若名字和密码均正确，则将1送到AUTH变量中，回到主菜单界面。

**提示：**字符串比较时，当采用输入串的长度作为循环次数时，若因循环次数减为0而终止循环，则还要去判断网店中定义的字符串的下一个字符是否是结束符0，若是，才能确定找到了（这样做是为了避免输入的字符串仅仅是数据段中所定义字符串的子集的误判情况）。

2.查找指定商品并显示其信息

（1）提示用户输入商品名称。

（2）在商店中寻找是否存在该商品。

（3）若存在，则将商品名称或地址记录到GOOD字段中。商品信息的显示暂时不做。返回到主菜单界面。

（4）若没有找到，提示没有找到，返回到主菜单界面。

3.下订单

（1）判断当前浏览商品是否有效（GOOD不为空），若有效，判断其剩余数量是否为0，不为0则将已售数量加1，重新计算所有商品的推荐度（目前不是用子程序实现的，所以，跳转之前，要把返回地址送到指定变量中），返回主菜单界面。

（2）若无效或剩余数量为0，则提示错误，回到主菜单界面。

4.计算商品推荐度

按照给出的公式计算所有商品的推荐度，返回到指定的位置（JMP 含返回地址的指定变量）。

**要求尽量避免溢出。**结果只保留整数部分。

5.排名

暂不实现，直接返回主菜单界面。

6.修改商品信息

暂不实现，直接返回主菜单界面。

7.迁移商店运行环境

暂不实现，直接返回主菜单界面。

8.显示当前代码段首址

将当前代码段寄存器CS里面的内容按照16进制的方式显示到屏幕上，返回主菜单界面。

9.退出

退出本系统（可使用4CH号DOS系统功能调用）

***--------------实验内容描述完毕。以下是相关说明，请认真阅读------------***

* 进度提示：

第一次上机学时必须完成任务1.1至1.3，可以完成任务1.4的部分功能；第二次上机学时完成全部任务。

* 学生自主变更提示：

学生可以自行调整实验内容，但自选的内容要能完成实验目的与要求，并经老师同意。任务1.4的内容不宜自行更改太多，因后续实验还会用到。

* 需要解决的问题提示：

**在完成上述任务过程中，需要大家按照下面的提示检查自己是否还存在未搞清楚的问题，鼓励大家自行设置新的问题并通过实验观察来解决。（这些问题可按照合适的方式纳入到自己写的实验步骤、记录与分析以及总结中）**

本次实验中需要学生尝试体会与解决的操作及问题可分为三类：

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。

各实验任务中的具体提示如下表：

|  |  |  |
| --- | --- | --- |
| 任务编号 | 序号 | 学生尝试的操作 |
| 任务1.1 | 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 | 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？ |
| 6 | 执行一条指令后，如何查看标志寄存器的值？ |
| 7 | 将A、B视为有符号数，运算后得到的结果、所有标志位信息，与将A、B视为无符号数，再次做同样运算后得到的结果、所有标志位信息进行比较，有何不同？ |
| 8 | 总结加减法对标志寄存器的影响？ |
| 任务1.2和任务1.3 | 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（包括找到某个变量在哪里）？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1.2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（包括在定义的地方、使用的地方等处的表现形式） |
| 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 |

**任务1.4中，需要探究的问题提示：**

|  |  |  |
| --- | --- | --- |
|  | 序号 | 学生尝试的操作 |
| 任务1.4 | 1 | 如何让9号功能调用显示的信息放在自己希望的位置？ |
| 2 | 如果在9号功能调用时，带显示字符串的结尾没有“$”结束符会怎样？ |
| 3 | 如果在9号功能调用前，未对DS赋值，或者未对DX给予正确的值，结果会如何？ |
| 4 | 10号功能调用时，输入的字符数超过定义的数量时，它是如何处理的？ |
| 5 | 匹配姓名时，如何提高匹配速度？ |
| 6 | 循环或转移时，是否有多种指令的组合方式实现？ |
| 7 | 注意观察转移指令机器码的编码方法，观察对应标号的偏移地址与该编码之间的关系。 |
| 8 | 检查循环程序，是否可能出现死循环的情况。 |
| 任务1.4 | 1 | 是否可以简化一下计算公式。 |
| 2 | 单步观察计算过程，结果是否正确？ |
| 3 | 用TD直接修改数据区的数值，使得程序对应的每个分支都能得到验证。 |
| 4 | 选取特殊的值，观察计算结果溢出的情况。 |
|  |  |

* 实验报告撰写的提示：

**实验一的实验报告形成过程提示：**

（1）第一个4学时上机前，需要熟悉书上各个题目的意思，了解各个软件工具的情况。看一下《80X86汇编语言程序设计上机指南》或教材第7章相关内容，形成一个大致的实验方法指导下一步的实验操作。上机实验后，将自己觉得最有收获的实验记录放到实验报告中并给出分析说明（任务1.1至1.3的每个任务只需给出一个关键点的记录和说明即可）。写出已经完成任务的小结。

（2）第二个4学时上机前，实验报告应完成任务1.4的步骤描述，程序设计思想、流程图、源程序初稿等。进入实验后，按照步骤完成程序调试、实验操作并记录相关结果（可以截图），对结果进行分析说明。在任务1.1至1.3的小结基础上，写出对任务1.4的小结。

（3）最后提交的实验报告应包含对实验目的和要求以及实验内容的描述，请复制上述页面中的相关内容，但需要把所有提示都删除。