实验报告三

一、实验目的：

通过实验了解DOS常用命令，汇编就是把用汇编语言编写的源程序翻译（汇编）成机器语言的目标程序。汇编程序可以使用小汇编程序（ASM）也可以用宏汇编程序（MASM），用于宏汇编程序不但可以代替ASM，而且可以汇编具有宏定义的汇编程序，因此我们在汇编程序时使用宏汇编程序（MASM）。开发汇编语言源程序的主要步骤有哪些？首先用EDIT等编辑程序产生汇编语言的源程序，源程序是用汇编语言的语句编写的且不能为机器所识别的程序，所以要经过汇编程序加以翻译，因此汇编程序的作用就是把源文件转换成用二进制代码表示的目标文件（称为OBJ文件）。在转换的过程中，如果源程序中有语法错误，则汇编结束后，汇编程序将指出源程序中的错误信息，如非法格式，未定义的助记符、标号，漏掉操作数等。用户还可以用编辑程序来修改源程序中的错误，最后得到无语法错误的目标文件。目标文件虽然已经是二进制文件，但它还不能直接上机运行，必须经过连接程序（LINK）把目标文件与库文件或其他目标文件连接在一起形成可执行文件（EXE文件），才可以在机器上运行。

二、实验任务：

1．dos命令建立目录拷贝文件（edit.com、masm.exe、link.exe、debug.exe）执行宏汇编程序。

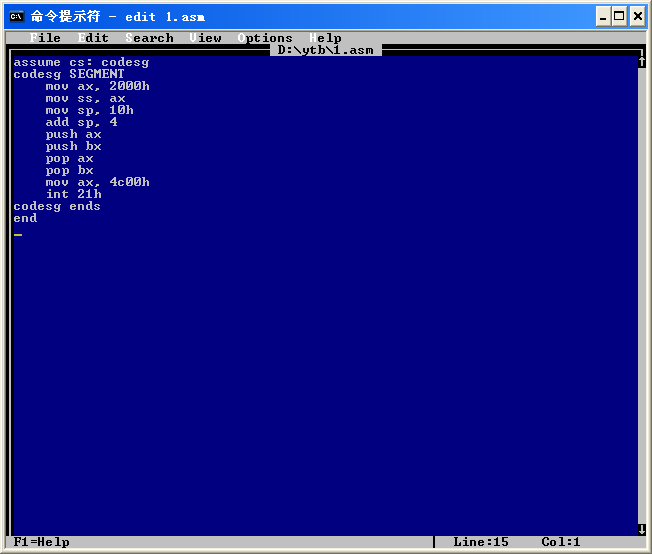
2．通过调用程序DEBUG的主要命令，熟悉各种命令的用法。

三、实验过程：

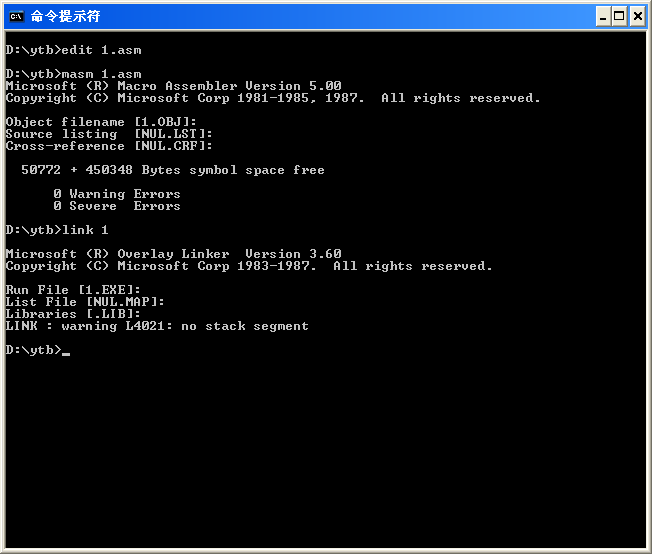
1．将下面的程序保存为1.asm，将其生成可执行文件1.exe。

|  |
| --- |
| assume cs: codesg  codesg SEGMENT  mov ax, 2000h  mov ss, ax  mov sp, 10h  add sp, 4  push ax  push bx  pop ax  pop bx  mov ax, 4c00h  int 21h  codesg ends  end |

（1）编辑1.asm：

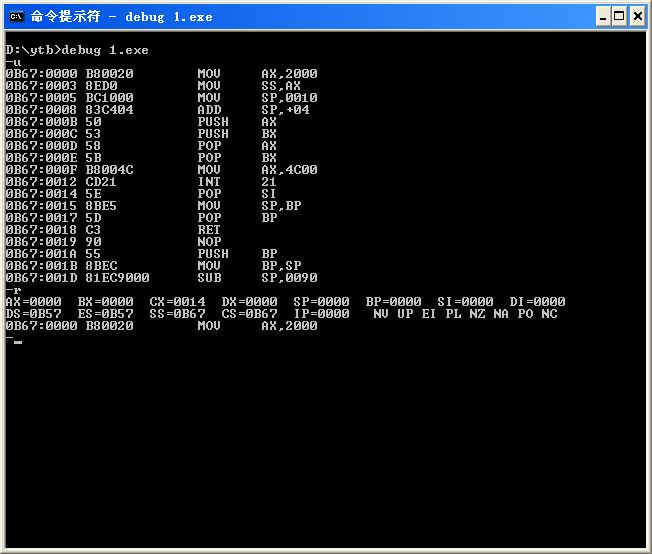


（2）使用MASM编译生成目标文件1.obj，使用LINK将目标程序连接定位，生成可执行文件1.exe：



2．使用DEBUG跟踪1.exe，写出每一步执行后，相关寄存器的内容。

（1）使用DEBUG跟踪1.exe：



（2）记录每一步执行后相关寄存器的内容

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 行号 | 机器码 | 字节数 | 汇编指令 | 汇编指令执行后寄存器的内容 | | | |
| ax | bx | ip | sp |
| 1  2  3  4  5  6  7  8  9  10 | B80020  8ED0  BC1000  83C404  50  53  58  5B  B8004C  CD21 | 3  2  3  3  1  1  1  1  3  2 | MOV AX, 2000  MOV SS, AX  MOV SP, 0010  ADD SP, +04  PUSH AX  PUSH BX  POP AX  POP BX  MOV AX, 4C00  INT 21 | 2000  2000  2000  2000  2000  0000  0000  4C00 | 0000  0000  0000  0000  0000  0000  2000  2000 | 0000  0008  000B  000C  000D  000E  000F  0012 | 0000  0010  0014  0012  0010  0012  0014  0014 |

在Debug中用T命令执行第二行语句mov ss, ax后，它的下一条指令mov sp, 10h并没有显示，这是因为Debug的T命令在执行修改寄存器SS的指令时，下一条指令也紧接着被执行。

下面以压栈图的形式展示栈操作的过程：

|  |  |
| --- | --- |
|  |  |
| add sp, 4后 | push ax后 |
|  |  |
| push bx后 | pop ax后 |
|  | |
| pop bx后 | |

上述过程中，push ax后，SP=SP-2，将ax的值送入SS:SP指向的内存单元；push bx后，SP=SP-2，将bx的值送入SS:SP指向的内存单元；pop ax后，先取出SS:SP指向内存单元处的一个字放入ax，然后SP=SP+2；pop bx后，先取出SS:SP指向内存单元处的一个字放入bx，然后SP=SP+2。

经过以上程序，交换了寄存器ax和bx中的值，IP每次增加的值是执行汇编指令对应的机器码的字节数。