

Computer Input/output System

2014

Instructors: Yang Quansheng

**School of Computer Science and Engineering
College of Software Engineering
Southeast University**



汇编语言上机过程（自学）



- 16 位调试工具 **DEBUG** 的使用
- 16 位汇编语言上机过程
- 16 位汇编语言的调试
- 用 **VC6.0** 实现 **C++** 中嵌入汇编

0. 实验包的安装

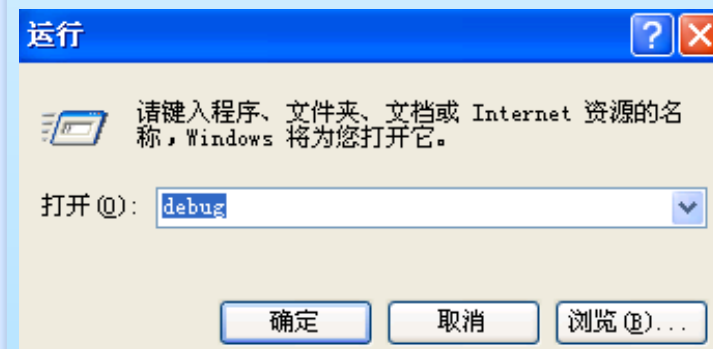
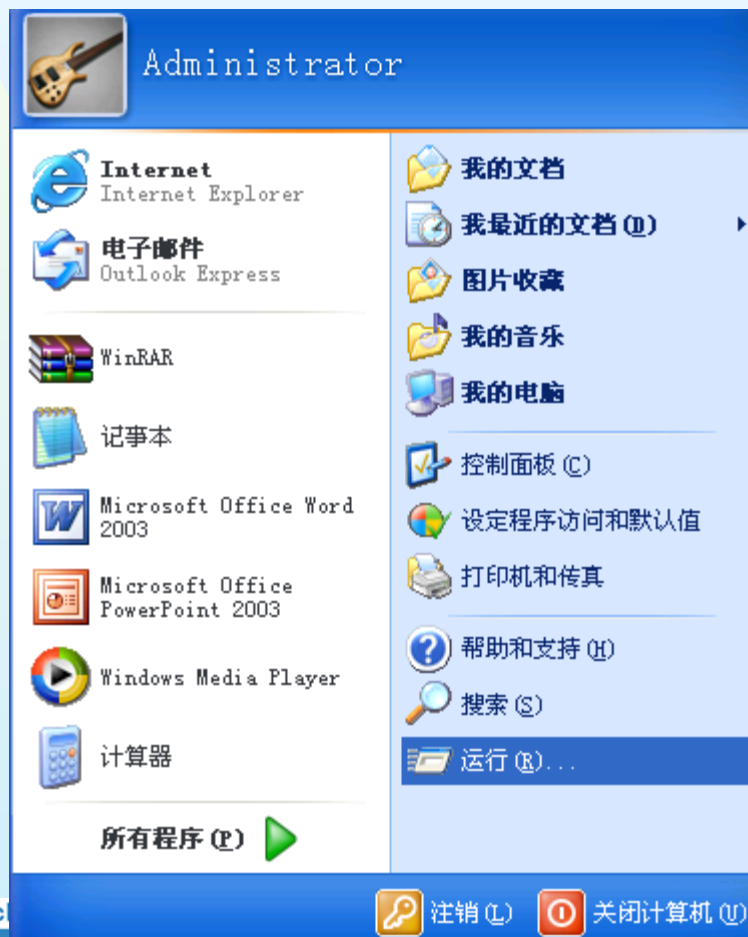
- 请参看《实验包安装手册》一文，尤其要注意安装的缺省路径，本 PPT 均按照缺省路径，其中
 - ◆ 32 位汇编编辑器路径
 - ✦ d:\masmisis
 - ◆ Prtoteus 7.6 路径
 - ✦ d:\Program Files\Labcenter Electronics\Proteus 7 Professional
 - ◆ 作业工作目录
 - ✦ d:\masmisis\exercise
 - 该目录做接口实验用，汇编实验在 d:\masmisis 目录做



1.16 位调试工具 DEBUG 的使用

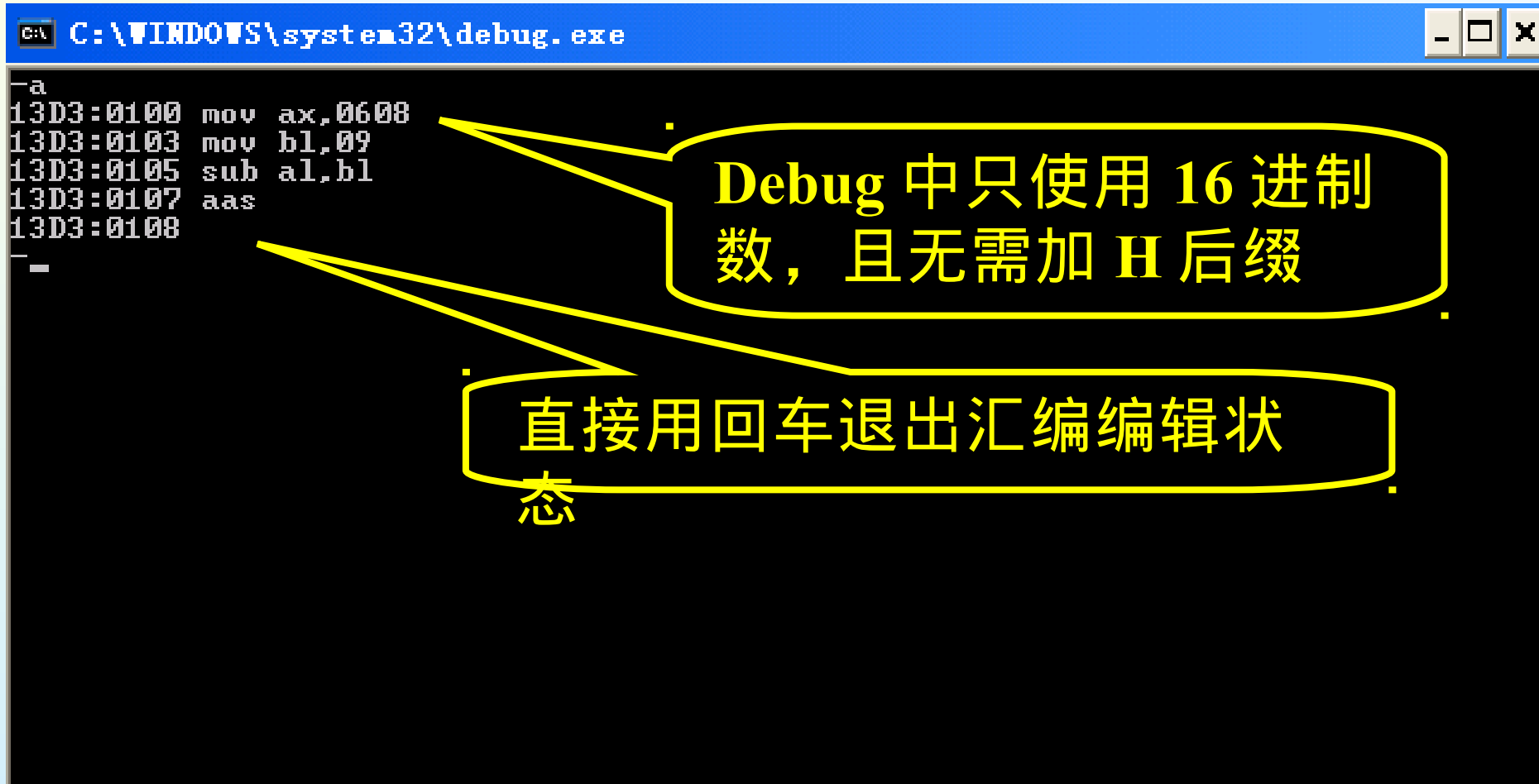
■ 题目：非压缩 BCD 码的减法运算，做 68-9

```
mov ax, 0608h
mov bl, 09h
sub al, bl
aas
```



1.16 位调试工具 DEBUG 的使用

首先用 A 命令输入程序



```
C:\WINDOWS\system32\debug.exe

-a
13D3:0100 mov ax,0608
13D3:0103 mov bl,09
13D3:0105 sub al,bl
13D3:0107 aas
13D3:0108
-
```

Debug 中只使用 16 进制数, 且无需加 H 后缀

直接用回车退出汇编编辑状态

使用 T 命令跟踪执行

```
C:\WINDOWS\system32\debug.exe

13D3:0103 mov bl,09
13D3:0105 sub al,bl
13D3:0107 aas
13D3:0108
-t=13d3:0100

AX=0608 BX=0000 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=13D3 ES=13D3 SS=13D3 CS=13D3 IP=0103  NU UP EI PL NZ NA PO NC
13D3:0103 B309      MOV     BL,09
-t

AX=0608 BX=0009 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=13D3 ES=13D3 SS=13D3 CS=13D3 IP=0105  NU UP EI PL NZ NA PO NC
13D3:0105 28D8      SUB     AL,BL
-t

AX=06FF BX=0009 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=13D3 ES=13D3 SS=13D3 CS=13D3 IP=0107  NU UP EI NG NZ AC PE CY
13D3:0107 3F        AAS
-t

AX=0509 BX=0009 CX=0000 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=13D3 ES=13D3 SS=13D3 CS=13D3 IP=0108  NU UP EI PL NZ AC PE CY
13D3:0108 0000      ADD     [BX+SI],AL      DS:0009=F0
```

第一个 T 命令要带上程序首地址

后面的 T 命令无需地址

标志位

这是还未执行的
下一条指令的地
址和指令码

这是还未执行的
下一条指令
的反汇编

当前指令执行后的
各寄存器的结
果

调试完后用 **Q** 命令退出 **DEBUG**。

DEBUG 命令参见《16 位汇编语言程序调试方法 -**DEBUG.doc**》一文。下面给出 **DEBUG** 中标志位状态符号的含义。

标志	为 1 时	为 0 时
溢出 OF	OV	NV
方向 DF	DN	UP
中断 IF	EI	DI
符号 SF	NG	PL
零位 ZF	ZR	NZ
辅助 AF	AC	NA
奇偶 PF	PE	PO
进位 CF	CY	NC

再举一个有访存操作的例子

MOV SI, 0050H ; (DS)=2000H

MOV DI, 0100H ; (ES)=3000H

MOV CX, 5

CLD

REP MOVSB

1) 先用 A 命令输入程序

```
C:\WINDOWS\system32\debug.exe
-a
13D3:0100 mov si,50
13D3:0103 mov di,100
13D3:0106 mov cx,5
13D3:0109 cld
13D3:010A rep movsb
13D3:010C
-
```

2) 用 R 命令修改 DS 和 ES 寄存器到约定值

```
-r ds
DS 13D3
:2000
-r es
ES 13D3
:3000
_
```

DS 的原始值

输入的修改值

3) 用 D 命令查看源数据区和目标数据区

```
-d ds:50
2000:0050  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:0060  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:0070  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:0080  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:0090  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:00A0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:00B0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
2000:00C0  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
-d es:100
3000:0100  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0110  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0120  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0130  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0140  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0150  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0160  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
3000:0170  00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  .....
_
```

4) 用 E 命令初始化源数据区后再用 D 命令检查源数据区和目的数据区

```
-e ds:50 'ABCDEF'f3 8d 12
-d ds:50
2000:0050  41 42 43 44 45 46 F3 8D-12 00 00 00 00 00 00 00 00  ABCDEF.....
2000:0060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:0080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:0090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:00A0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:00B0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:00C0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
-d es:100
3000:0100  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0110  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0130  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0140  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0150  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0160  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0170  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
```

5) 单步跟踪执行程序

-t=13d3:100

AX=0000	BX=0000	CX=0000	DX=0000	SP=FFEE	BP=0000	SI=0050	DI=0000
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=0103	NU UP EI PL NZ NA PO NC		
13D3:0103 BF0001		MOV		DI,0100			

-t

AX=0000	BX=0000	CX=0000	DX=0000	SP=FFEE	BP=0000	SI=0050	DI=0100
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=0106	NU UP EI PL NZ NA PO NC		
13D3:0106 B90500		MOV		CX,0005			

-t

AX=0000	BX=0000	CX=0005	DX=0000	SP=FFEE	BP=0000	SI=0050	DI=0100
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=0109	NU UP EI PL NZ NA PO NC		
13D3:0109 FC		CLD					

-t

AX=0000	BX=0000	CX=0005	DX=0000	SP=FFEE	BP=0000	SI=0050	DI=0100
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=010A	NU UP EI PL NZ NA PO NC		
13D3:010A F3		REPZ					
13D3:010B A4		MOUSB					

-t

AX=0000	BX=0000	CX=0004	DX=0000	SP=FFEE	BP=0000	SI=0051	DI=0101
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=010A	NU UP EI PL NZ NA PO NC		
13D3:010A F3		REPZ					
13D3:010B A4		MOUSB					

-t

AX=0000	BX=0000	CX=0003	DX=0000	SP=FFEE	BP=0000	SI=0052	DI=0102
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=010A	NU UP EI PL NZ NA PO NC		
13D3:010A F3		REPZ					
13D3:010B A4		MOUSB					

-t

AX=0000	BX=0000	CX=0002	DX=0000	SP=FFEE	BP=0000	SI=0053	DI=0103
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=010A	NU UP EI PL NZ NA PO NC		
13D3:010A F3		REPZ					
13D3:010B A4		MOUSB					

-t

AX=0000	BX=0000	CX=0001	DX=0000	SP=FFEE	BP=0000	SI=0054	DI=0104
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=010A	NU UP EI PL NZ NA PO NC		
13D3:010A F3		REPZ					
13D3:010B A4		MOUSB					

-t

AX=0000	BX=0000	CX=0000	DX=0000	SP=FFEE	BP=0000	SI=0055	DI=0105
DS=2000	ES=3000	SS=13D3	CS=13D3	IP=010C	NU UP EI PL NZ NA PO NC		
13D3:010C 0000		ADD		[BX+SI],AL		DS:0055=46	

6) 执行后检查源数据区和目标数据区

```
-d ds:50
2000:0050  41 42 43 44 45 46 F3 8D-12 00 00 00 00 00 00 00 00  ABCDEF.....
2000:0060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:0080  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:0090  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:00A0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:00B0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
2000:00C0  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
-d es:100
3000:0100  41 42 43 44 45 00 00 00-00 00 00 00 00 00 00 00 00  ABCDE.....
3000:0110  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0120  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0130  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0140  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0150  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0160  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
3000:0170  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  .....
-
```

注意，用 A 命令输入指令时，如果输入错误 debug 会立即指出错误和位置。地址不会变化，以便用户修正指令。

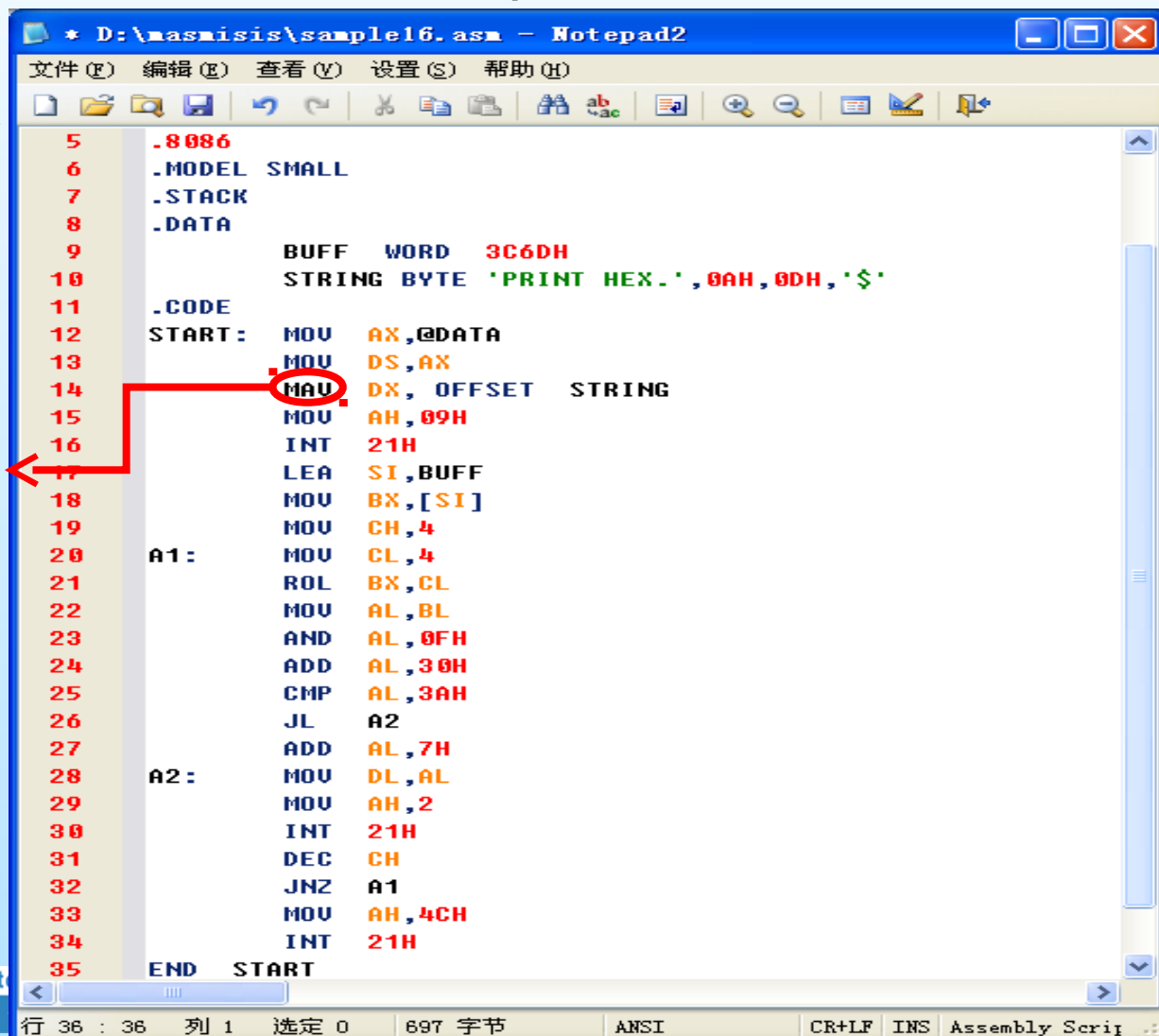
```
-a
13D3:0100 mov ax,b1
                        ^ Error
13D3:0100 mov ax,bx
13D3:0102 ads ax,0
                        ^ Error
13D3:0102 cmp 0,ax
                        ^ Error
13D3:0102 _
```

2. 16 位汇编语言上机过程

■ 第一步：编辑

- ◆ 转到 d:\masmisis 目录并运行 Notepad2.exe 编辑源程序，编辑好后一定要记住存盘，本题存盘为：
sample16.asm

14 行一个错



```
* D:\masmisis\sample16.asm - Notepad2
文件(F) 编辑(E) 查看(V) 设置(S) 帮助(H)

5      .8086
6      .MODEL SMALL
7      .STACK
8      .DATA
9          BUFF WORD 3C6DH
10         STRING BYTE 'PRINT HEX.',0AH,0DH,'$'
11      .CODE
12      START: MOV AX,@DATA
13             MOV DS,AX
14             MOV DX, OFFSET STRING
15             MOV AH,09H
16             INT 21H
17             LEA SI,BUFF
18             MOV BX,[SI]
19             MOV CH,4
20      A1:     MOV CL,4
21             ROL BX,CL
22             MOV AL,BL
23             AND AL,0FH
24             ADD AL,30H
25             CMP AL,3AH
26             JL  A2
27             ADD AL,7H
28      A2:     MOV DL,AL
29             MOV AH,2
30             INT 21H
31             DEC CH
32             JNZ A1
33             MOV AH,4CH
34             INT 21H
35      END START
```

行 36 : 36 列 1 选定 0 697 字节 ANSI CR+LF INS Assembly Scrip



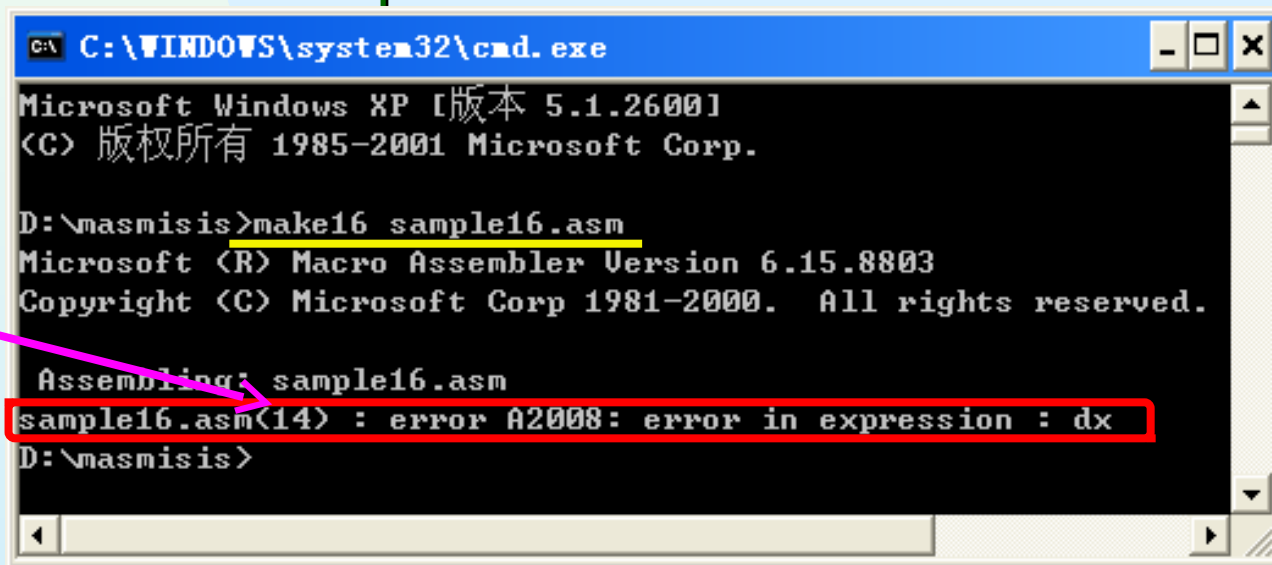
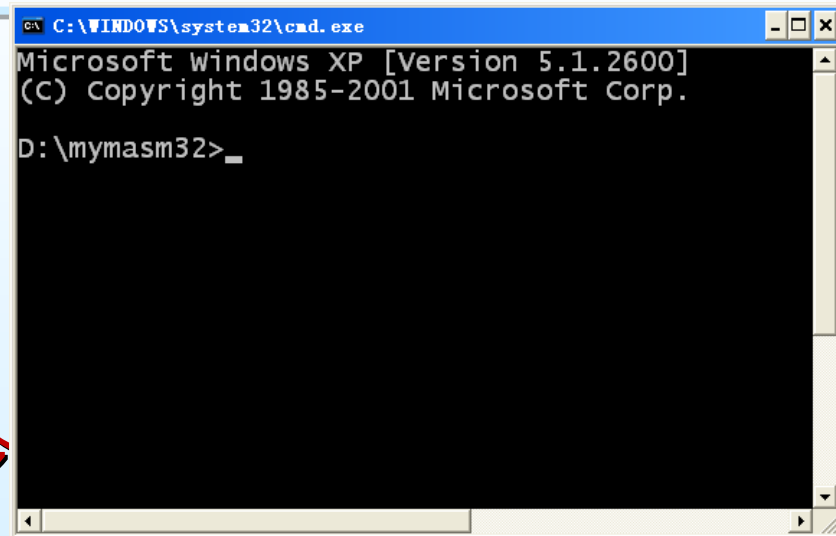
2. 16 位汇编语言上机过程

■ 第二步：编译连接

◆ 执行 DOS16.bat

◆ 在 CMD 窗口中敲入下面的命令

◆ make16 sample16



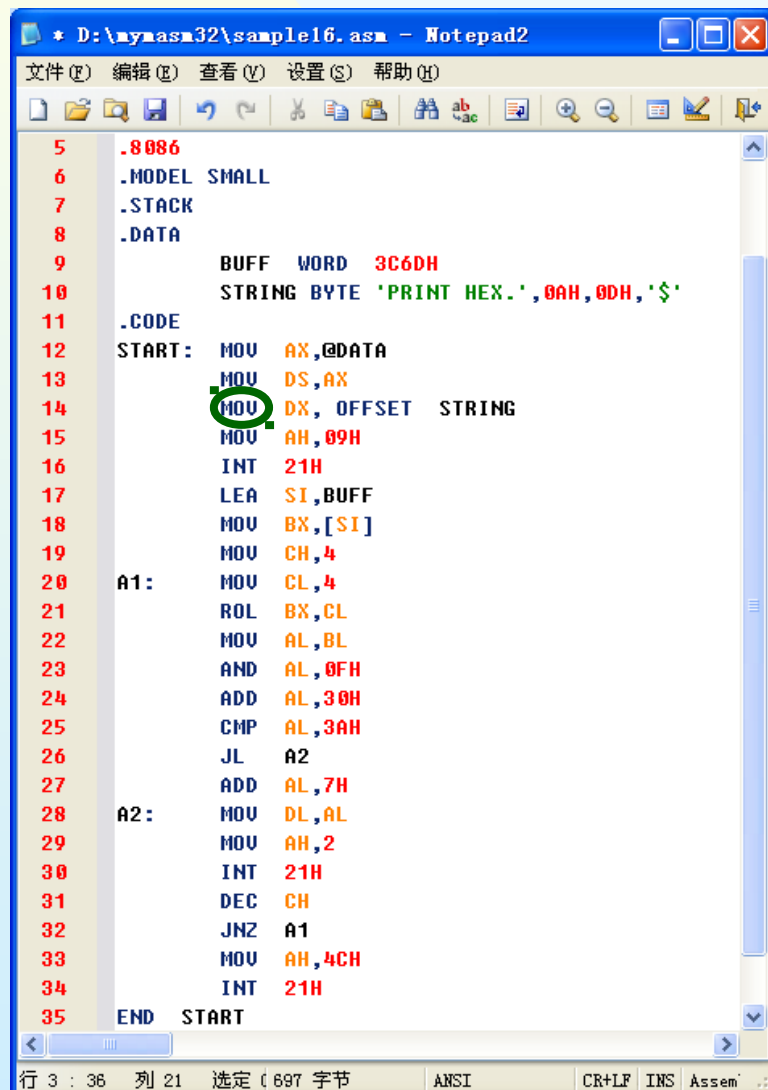
14 行出错

◆ 回编辑状态修改错误后再编译连接和执行



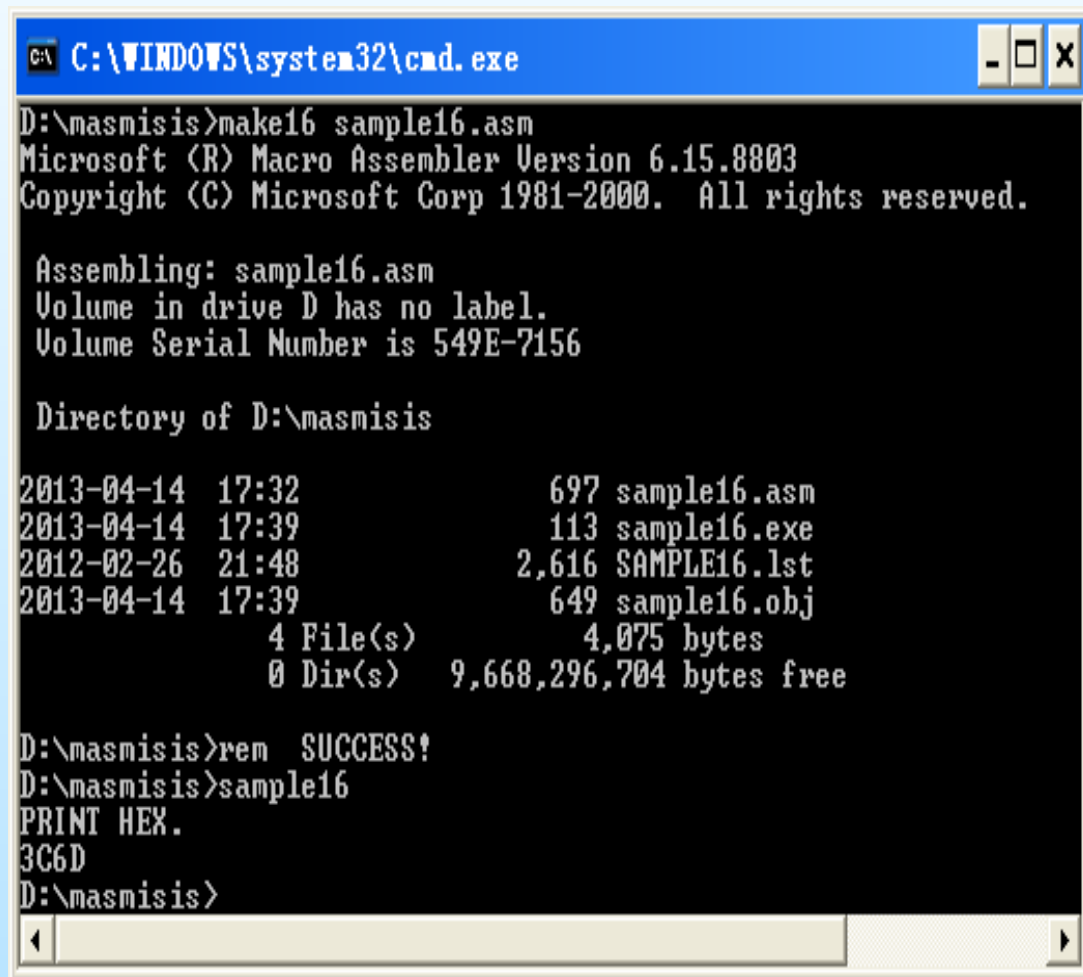
2. 16 位汇编语言上机过程

- 第三步：回编辑状态修改错误后存盘，然后再编译连接和执行



```

5 .8086
6 .MODEL SMALL
7 .STACK
8 .DATA
9     BUFF WORD 3C6DH
10    STRING BYTE 'PRINT HEX.',0AH,0DH,'$'
11 .CODE
12 START: MOV AX,@DATA
13        MOV DS,AX
14        MOV DX, OFFSET STRING
15        MOV AH,09H
16        INT 21H
17        LEA SI,BUFF
18        MOV BX,[SI]
19        MOV CH,4
20 A1:    MOV CL,4
21        ROL BX,CL
22        MOV AL,BL
23        AND AL,0FH
24        ADD AL,30H
25        CMP AL,3AH
26        JL A2
27        ADD AL,7H
28 A2:    MOV DL,AL
29        MOV AH,2
30        INT 21H
31        DEC CH
32        JNZ A1
33        MOV AH,4CH
34        INT 21H
35 END START
  
```



```

C:\WINDOWS\system32\cmd.exe

D:\masmisis>make16 sample16.asm
Microsoft (R) Macro Assembler Version 6.15.8803
Copyright (C) Microsoft Corp 1981-2000. All rights reserved.

Assembling: sample16.asm
Volume in drive D has no label.
Volume Serial Number is 549E-7156

Directory of D:\masmisis

2013-04-14 17:32                697 sample16.asm
2013-04-14 17:39                113 sample16.exe
2012-02-26 21:48             2,616 SAMPLE16.lst
2013-04-14 17:39                649 sample16.obj
                     4 File(s)          4,075 bytes
                     0 Dir(s)  9,668,296,704 bytes free

D:\masmisis>rem SUCCESS!
D:\masmisis>sample16
PRINT HEX.
3C6D
D:\masmisis>
  
```

3. 16 位汇编语言的调试

- 接上例，在 CMD 窗口中键入：
 - ◆ Debug sample16.exe
- 用 U 命令查看程序和目标码及指令地址

```

C:\WINDOWS\system32\cmd.exe - de...
D:\masmisis>debug sample16.exe
-u
0BA2:0000 B8A50B      MOV     AX,0BA5
0BA2:0003 8ED8          MOV     DS,AX
0BA2:0005 BA0400      MOV     DX,0004
0BA2:0008 B409          MOV     AH,09
0BA2:000A CD21          INT     21
0BA2:000C 8D360200     LEA     SI,[0002]
0BA2:0010 8B1C          MOV     BX,[SI]
0BA2:0012 B504          MOV     CH,04
0BA2:0014 B104          MOV     CL,04
0BA2:0016 D3C3          ROL     BX,CL
0BA2:0018 8AC3          MOV     AL,BL
0BA2:001A 240F          AND     AL,0F
0BA2:001C 0430          ADD     AL,30
0BA2:001E 3C3A          CMP     AL,3A
  
```

段值 偏移 指令码 反汇编的源码

3. 16 位汇编语言的调试

- 用 T 命令单步跟踪，逐条执行看中间结果，DEBUG 将显示每个寄存器以及各标志位的当前值

```

C:\WINDOWS\system32\cmd.exe - debug sample16.exe

0BA2:001E 3C3A          CMP     AL,3A
-t

AX=0BA5  BX=FFFF  CX=FE71  DX=0000  SP=0400  BP=0000  SI=0000  DI=0000
DS=0B92  ES=0B92  SS=0BA7  CS=0BA2  IP=0003  NU UP EI PL NZ NA PO NC
0BA2:0003 8ED8          MOV     DS,AX
-t

AX=0BA5  BX=FFFF  CX=FE71  DX=0000  SP=0400  BP=0000  SI=0000  DI=0000
DS=0BA5  ES=0B92  SS=0BA7  CS=0BA2  IP=0005  NU UP EI PL NZ NA PO NC
0BA2:0005 BA0400       MOV     DX,0004
-t

AX=0BA5  BX=FFFF  CX=FE71  DX=0004  SP=0400  BP=0000  SI=0000  DI=0000
DS=0BA5  ES=0B92  SS=0BA7  CS=0BA2  IP=0008  NU UP EI PL NZ NA PO NC
0BA2:0008 B409          MOV     AH,09
-t

AX=09A5  BX=FFFF  CX=FE71  DX=0004  SP=0400  BP=0000  SI=0000  DI=0000
DS=0BA5  ES=0B92  SS=0BA7  CS=0BA2  IP=000A  NU UP EI PL NZ NA PO NC
0BA2:000A CD21          INT     21

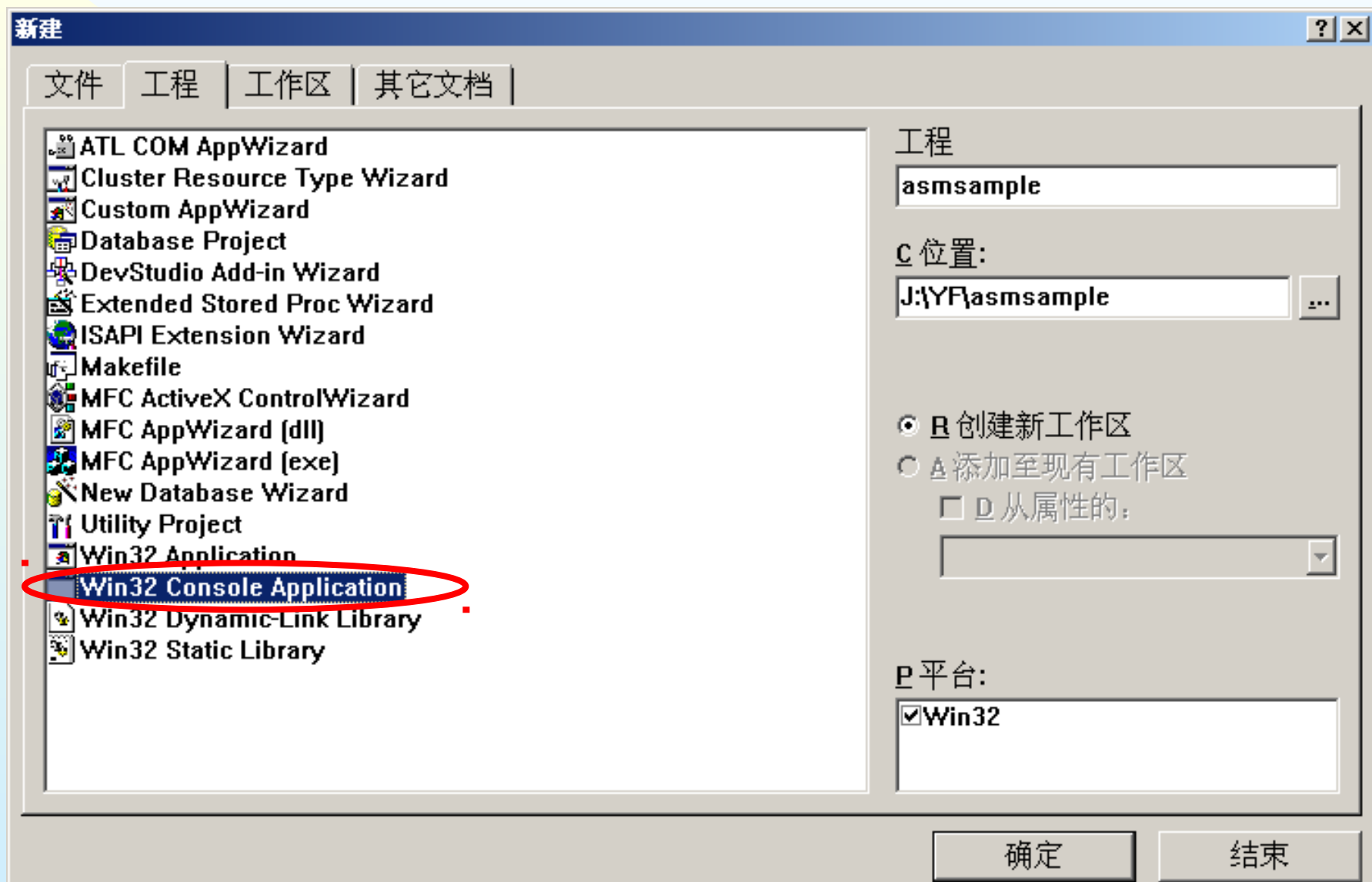
```

标志位

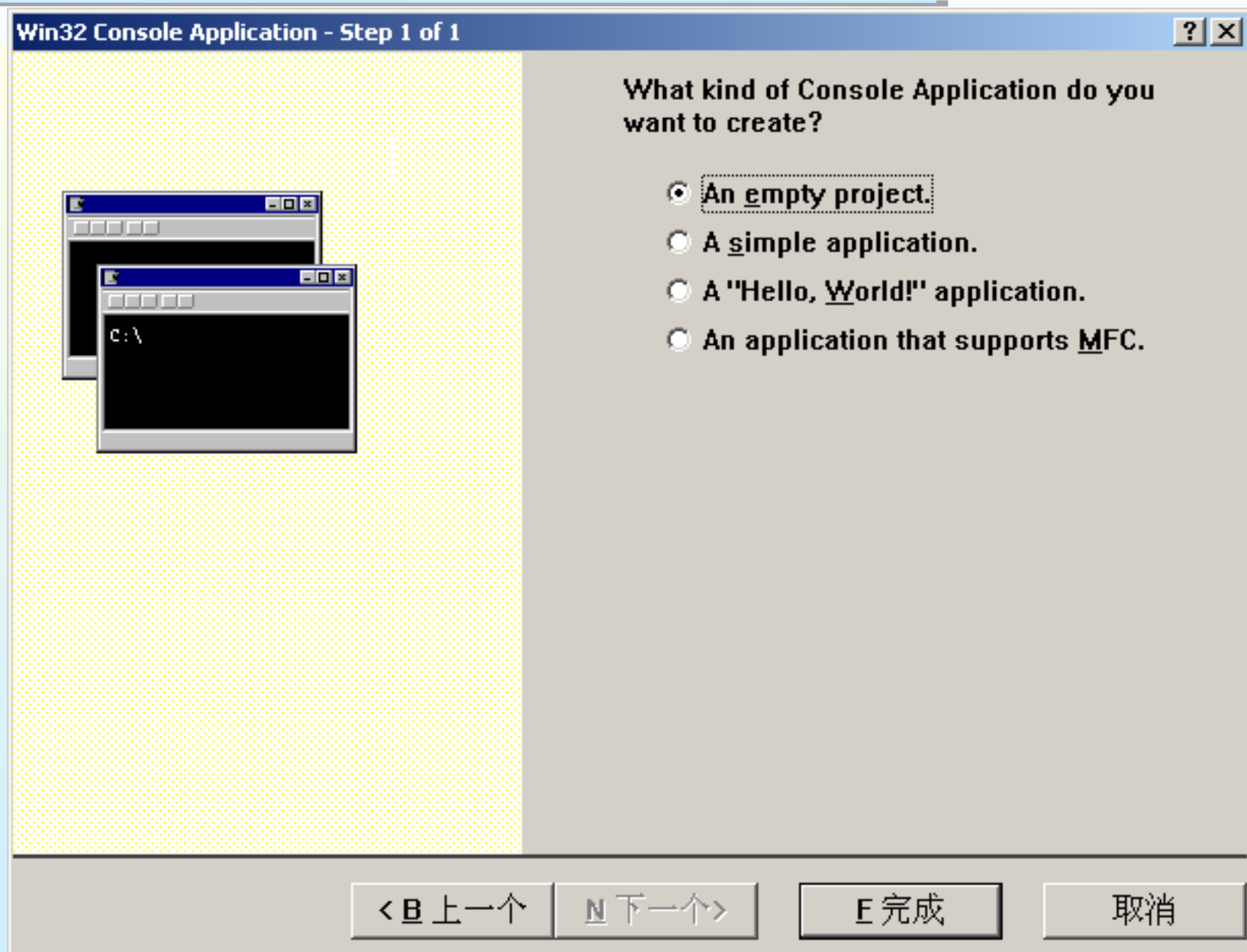
这是 MOV AH, 09 的执行结

这是还未执行的下一条指令

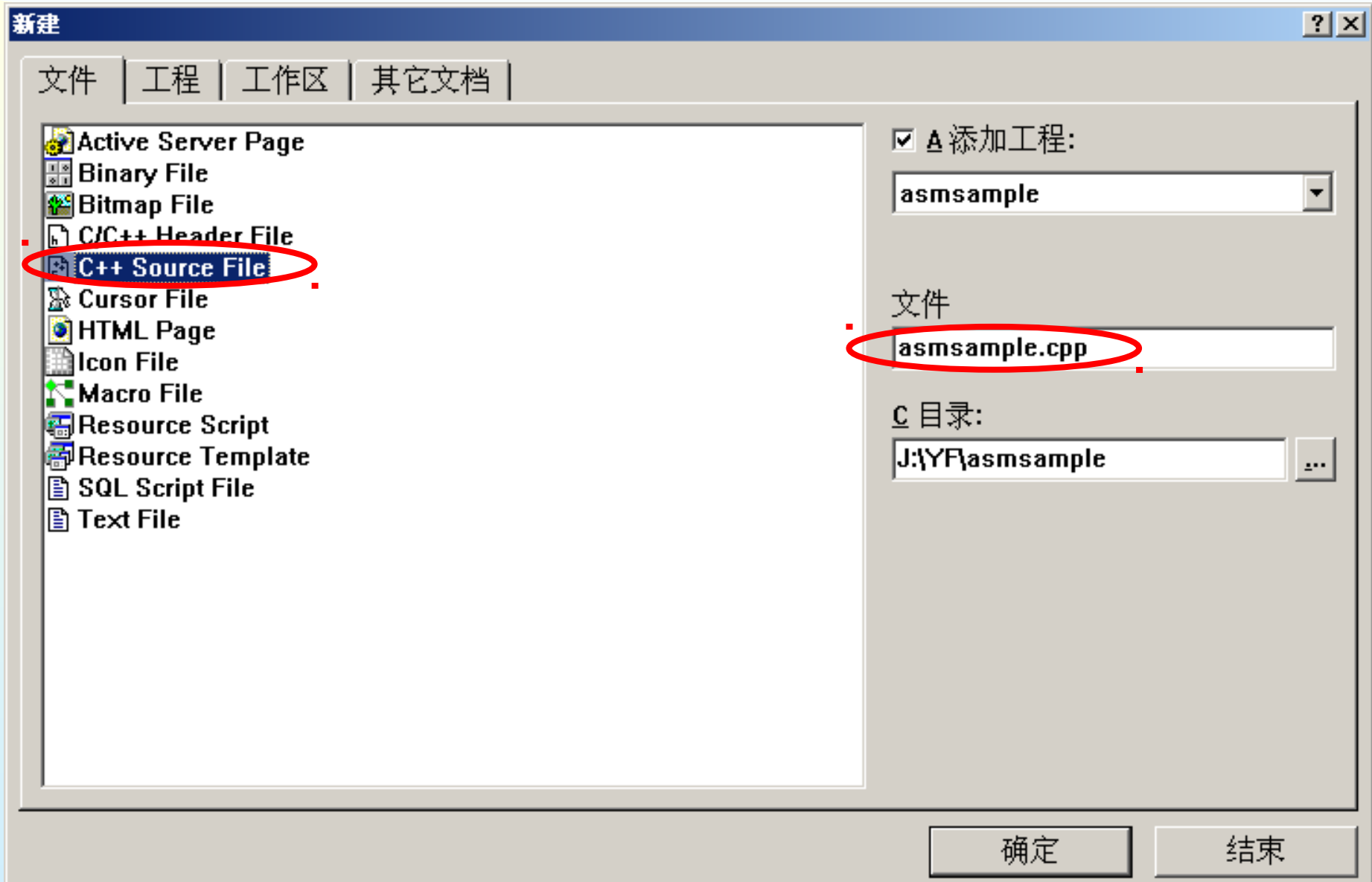
4. 用 VC6.0 实现 C++ 中嵌入汇编



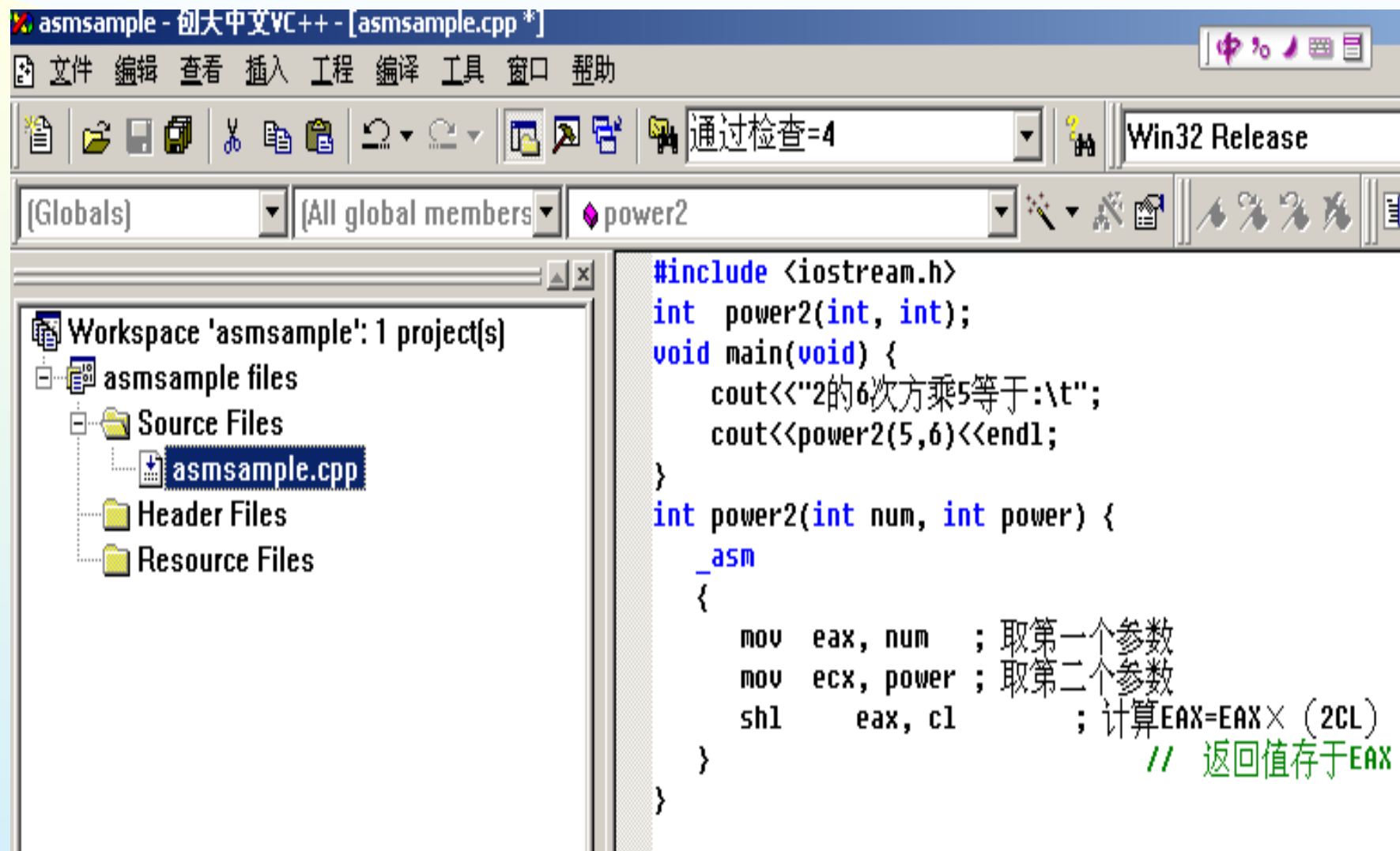
4. 用 VC6.0 实现 C++ 中嵌入汇编



4. 用 VC6.0 实现 C++ 中嵌入汇编



4. 用 VC6.0 实现 C++ 中嵌入汇编



4. 用 VC6.0 实现 C++ 中嵌入汇编

C:\ "J:\YF\asmsample\Release\asmsample.exe"

2的6次方乘5等于: 320
Press any key to continue

