

南京林业大学



汇编语言上机实验 任务书

实验二 编程、编译、连接、跟踪

实验目的

编程、编译、链接、跟踪

实验内容

1.通过 edit 输入实验内容



The screenshot shows a DOSBox window titled "DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: EDIT". The menu bar includes "File", "Edit", "Search", "View", "Options", and "Help". The file name "C:\NT1.ASM" is displayed. The editor contains the following assembly code:

```
assume cs:codesg
codesg segment
    mov ax,2000
    mov ss,ax
    mov sp,0
    add sp,10
    pop ax
    pop bx
    push ax
    push bx
    pop ax
    pop bx
    mov ax,4c00
    int 21H
end
```

The status bar at the bottom shows "F1=Help" on the left and "Line:1 Col:1" on the right.

2.查看文件系统

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

Run File [T1.EXE]:
List File [INUL.MAP]:
Libraries [.LIB]:
LINK : warning L4021: no stack segment

C:\>dir
Directory of C:\.
.                <DIR>                05-11-2025 10:25
..               <DIR>                31-10-2025 10:11
EX               <DIR>                03-02-2017  8:31
DEBUG           EXE                  20,634 10-01-2000 20:00
DESKTOP         INI                   317 19-10-2008 14:34
EDIT            COM                  69,886 10-01-2000 20:00
EDIT            EXE                  30,776 04-04-1996 13:30
EDLIN           COM                   4,608 08-03-1983 12:00
LINK            EXE                  64,992 21-05-1992 10:22
MASM            EXE                 103,184 21-05-1992 10:21
T1              ASM                   267 05-11-2025 10:24
T1              EXE                   534 05-11-2025 10:25
T1              OBJ                    74 05-11-2025 10:24
10 File(s)      295,272 Bytes.
 3 Dir(s)       262,111,744 Bytes free.

C:\>
```

3.执行 t1.exe

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX

LINK : warning L4021: no stack segment

C:\>dir
Directory of C:\.
.                <DIR>                05-11-2025 10:25
..               <DIR>                31-10-2025 10:11
EX               <DIR>                03-02-2017  8:31
DEBUG           EXE                  20,634 10-01-2000 20:00
DESKTOP         INI                   317 19-10-2008 14:34
EDIT            COM                  69,886 10-01-2000 20:00
EDIT            EXE                  30,776 04-04-1996 13:30
EDLIN           COM                   4,608 08-03-1983 12:00
LINK            EXE                  64,992 21-05-1992 10:22
MASM            EXE                 103,184 21-05-1992 10:21
T1              ASM                   267 05-11-2025 10:24
T1              EXE                   534 05-11-2025 10:25
T1              OBJ                    74 05-11-2025 10:24
10 File(s)      295,272 Bytes.
 3 Dir(s)       262,111,744 Bytes free.

C:\>t1
C:\>t1.exe
C:\>
```

4.通过 debug 执行 t1.exe

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
-r
AX=FFFF BX=0000 CX=0016 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0000  NU UP EI PL NZ NA PO NC
076A:0000 B80020      MOV     AX,2000
-t

AX=2000 BX=0000 CX=0016 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0003  NU UP EI PL NZ NA PO NC
076A:0003 8ED0      MOV     SS,AX
-t

AX=2000 BX=0000 CX=0016 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=0008  NU UP EI PL NZ NA PO NC
076A:0008 83C40A     ADD     SP,+0A
-t

AX=2000 BX=0000 CX=0016 DX=0000 SP=000A BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000B  NU UP EI PL NZ NA PE NC
076A:000B 5B      POP     AX
-t

AX=01A2 BX=0000 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000C  NU UP EI PL NZ NA PE NC
076A:000C 5B      POP     BX
_

D
AX=01A2 BX=0000 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000C  NU UP EI PL NZ NA PE NC
076A:000C 5B      POP     BX
-t

AX=01A2 BX=7206 CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000D  NU UP EI PL NZ NA PE NC
076A:000D 50      PUSH    AX
-t

AX=01A2 BX=7206 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000E  NU UP EI PL NZ NA PE NC
076A:000E 53      PUSH    BX
-t

AX=01A2 BX=7206 CX=0016 DX=0000 SP=000A BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000F  NU UP EI PL NZ NA PE NC
076A:000F 5B      POP     AX
-t

AX=7206 BX=7206 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=0010  NU UP EI PL NZ NA PE NC
076A:0010 5B      POP     BX
_
```

```

DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

AX=7206 BX=7206 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=0010  NU UP EI PL NZ NA PE NC
076A:0010 5B          POP      BX
-t

AX=7206 BX=01A2 CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=0011  NU UP EI PL NZ NA PE NC
076A:0011 B8004C     MOV      AX,4C00
-t

AX=4C00 BX=01A2 CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=0014  NU UP EI PL NZ NA PE NC
076A:0014 CD21     INT      21
-t

AX=4C00 BX=01A2 CX=0016 DX=0000 SP=0008 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=F000 IP=14A0  NU UP DI PL NZ NA PE NC
F000:14A0 FB          STI
-t

AX=4C00 BX=01A2 CX=0016 DX=0000 SP=0008 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=F000 IP=14A1  NU UP EI PL NZ NA PE NC
F000:14A1 FE3B     ???      [BX+SI]          DS:01A2=7A

```

5.t1.exe 执行完成，退出

```

AX=4C00 BX=01A2 CX=0016 DX=0000 SP=0008 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=F000 IP=14A1  NU UP EI PL NZ NA PE NC
F000:14A1 FE3B     ???      [BX+SI]          DS:01A2=7A
-q
C:\>_
01A2=7A

```

6.PSP 的头两个字节是 CD 20，用 debug 加载 t1.exe，查看 psp 的内容

```

C:\>debug t1.exe
-d 0
075A:0000  CD 20 FF 9F 00 EA FF FF-AD DE 4F 03 A3 01 8A 03  . . . . .0. . . .
075A:0010  A3 01 17 03 A3 01 92 01-01 01 01 00 02 FF FF FF  . . . . .
075A:0020  FF FF FF FF FF FF FF FF-FF FF FF FF 50 07 4C 01  . . . . .P.L.
075A:0030  63 06 14 00 18 00 5A 07-FF FF FF FF 00 00 00 00  c. . . .Z. . . .
075A:0040  05 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . .
075A:0050  CD 21 CB 00 00 00 00 00-00 00 00 00 00 00 00 00  .! . . . .
075A:0060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . .
075A:0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00  . . . . .

```