

## 汇编语言程序设计课程作业（四）

姓名：袁昊男 学号：2018091618008

### 实验3 编程、编译、连接、跟踪

(1) 将下面的程序保存为 t1.asm 文件，将其生成可执行文件 t1.exe。

```
assume cs:codesg
```

```
codesg segment
```

```
    mov ax,2000H
```

```
    mov ss,ax
```

```
    mov sp,0
```

```
    add sp,10
```

```
    pop ax
```

```
    pop bx
```

```
    push ax
```

```
    push bx
```

```
    pop ax
```

```
    pop bx
```

```
    mov ax,4c00H
```

```
    int 21H
```

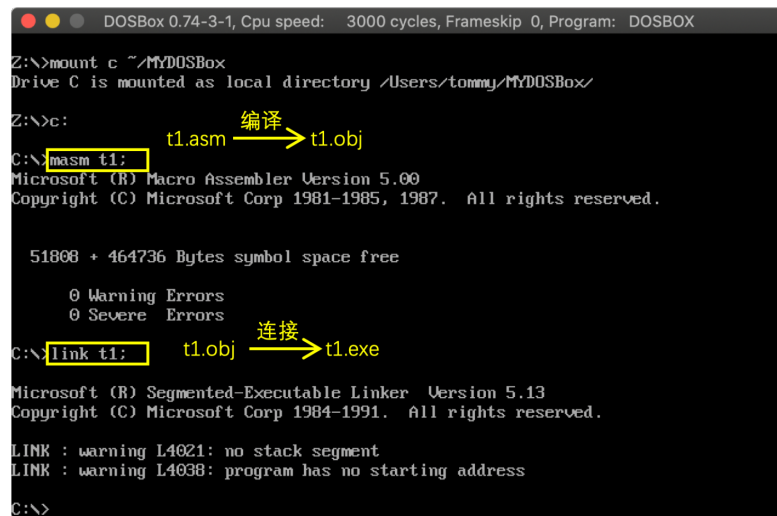
```
codesg ends
```

```
end
```

① 保存为 t1.asm 文件



② 生成可执行文件 t1.exe



```
DOSBox 0.74-3-1, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Z:\>mount c ~/MYDOSBox
Drive C is mounted as local directory /Users/tommy/MYDOSBox/

Z:\>c:
C:\>masm t1:
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

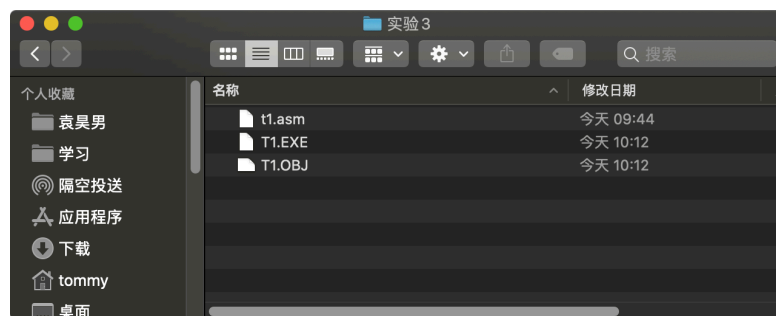
51808 + 464736 Bytes symbol space free

0 Warning Errors
0 Severe Errors
C:\>link t1:
Microsoft (R) Segmented-Executable Linker Version 5.13
Copyright (C) Microsoft Corp 1984-1991. All rights reserved.

LINK : warning L4021: no stack segment
LINK : warning L4038: program has no starting address
C:\>
```

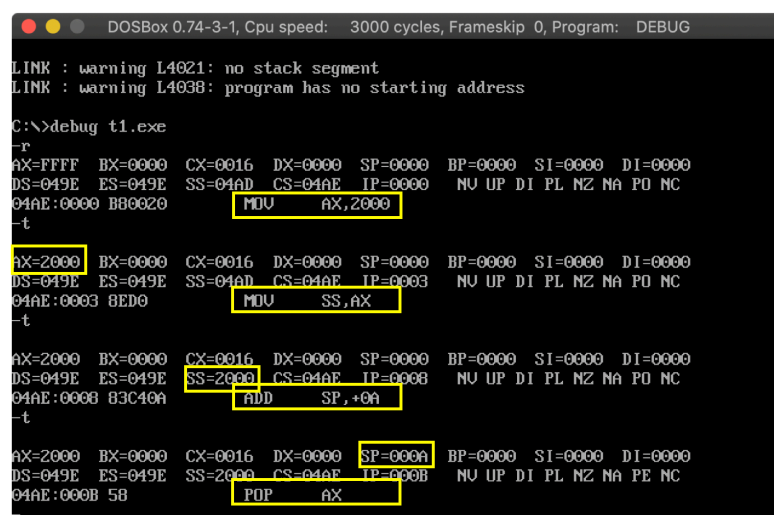
Diagram showing the process: t1.asm is compiled (编译) into t1.obj, which is then linked (连接) into t1.exe.

③ asm 文件通过编译、连接得到 obj 和 exe 文件



(2) 用 Debug 跟踪 t1.exe 的执行过程，写出每一步执行后相关寄存器中的内容和栈顶的内容。

① 使用 T 命令单步执行



```
DOSBox 0.74-3-1, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG

LINK : warning L4021: no stack segment
LINK : warning L4038: program has no starting address

C:\>debug t1.exe
-r
AX=FFFF BX=0000 CX=0016 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=04AD CS=04AE IP=0000  NU UP DI PL NZ NA PO NC
04AE:0000 B80020  MOV     AX,2000
-t
AX=2000 BX=0000 CX=0016 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=04AD CS=04AE IP=0003  NU UP DI PL NZ NA PO NC
04AE:0003 8ED0  MOV     SS,AX
-t
AX=2000 BX=0000 CX=0016 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=0008  NU UP DI PL NZ NA PO NC
04AE:0008 B3C40A  ADD     SP,+0A
-t
AX=2000 BX=0000 CX=0016 DX=0000 SP=000A BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000B  NU UP DI PL NZ NA PE NC
04AE:000B 5B  POP     AX
-t
```

```

DOSBox 0.74-3-1, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=2000 BX=0000 CX=0016 DX=0000 SP=000A BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000B  NU UP DI PL NZ NA PE NC
04AE:000B 5B          POP     AX
-t
AX=706F BX=0000 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000C  NU UP DI PL NZ NA PE NC
04AE:000C 5B          POP     BX
-t
AX=706F BX=6E65 CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000D  NU UP DI PL NZ NA PE NC
04AE:000D 50          PUSH    AX
-t
AX=706F BX=6E65 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000E  NU UP DI PL NZ NA PE NC
04AE:000E 53          PUSH    BX
-t
AX=706F BX=6E65 CX=0016 DX=0000 SP=000A BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000F  NU UP DI PL NZ NA PE NC
04AE:000F 5B          POP     AX
-t
04AE:000E 53          PUSH    BX
-t
AX=706F BX=6E65 CX=0016 DX=0000 SP=000A BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=000F  NU UP DI PL NZ NA PE NC
04AE:000F 5B          POP     AX
-t
AX=6E65 BX=6E65 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=0010  NU UP DI PL NZ NA PE NC
04AE:0010 5B          POP     BX
-t
AX=6E65 BX=706F CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=0011  NU UP DI PL NZ NA PE NC
04AE:0011 B8004C      MOV     AX,4C00
-t
AX=4C00 BX=706F CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=0014  NU UP DI PL NZ NA PE NC
04AE:0014 CD21      INT     21
-t
Program terminated normally

```

② 每一步执行后相关寄存器内容

mov ax,2000H	ax = 2000H
mov ss,ax	ss = 2000H
mov sp,0	sp = 0
add sp,10	sp = 0010H
pop ax	ax = 706FH
pop bx	bx = 6E65H
push ax	ax = 706FH
push bx	bx = 6E65H
pop ax	ax = 6E65H
pop bx	bx = 706FH

(3) PSP 的头两个字节是 CD 20，用 Debug 加载 t1.exe，查看 PSP 的内容。

① PSP 地址：DS 值为 049E，则 PSP 地址为 049E:0。

程序地址：(049E+10):0，即 04AE:0。

② 查看 PSP 内容

```

DOSBox 0.74-3-1, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=4C00 BX=706F CX=0016 DX=0000 SP=000E BP=0000 SI=0000 DI=0000
DS=049E ES=049E SS=2000 CS=04AE IP=0014 NU UP DI PL NZ NA PE NC
04AE:0014 CD21 INT 21
-g
Program terminated normally
-d 049e:0
049E:0000 CD 20 FF 9F 00 EA FF FF-AD DE 42 02 92 01 70 02 M ...j...^B...p.
049E:0010 92 01 10 01 18 01 92 01-FF FF FF FF FF FF FF FF .....B...
049E:0020 FF FF FF FF FF FF FF FF-FF FF FF FF 94 04 F6 FF .....U.
049E:0030 00 20 14 00 18 00 9E 04-FF FF FF FF 00 00 00 00 .....
049E:0040 05 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:0050 CD 21 CB 00 00 00 00 00-00 00 00 00 00 00 00 00 M!K.....
049E:0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
-d
049E:0080 00 0D 74 31 2E 65 78 65-0D 00 00 00 00 00 00 00 00 ..t1.exe.....
049E:0090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:00A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:00B0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:00C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:00D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:00E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....
049E:00F0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....

```