

暨南大学本科实验报告专用纸

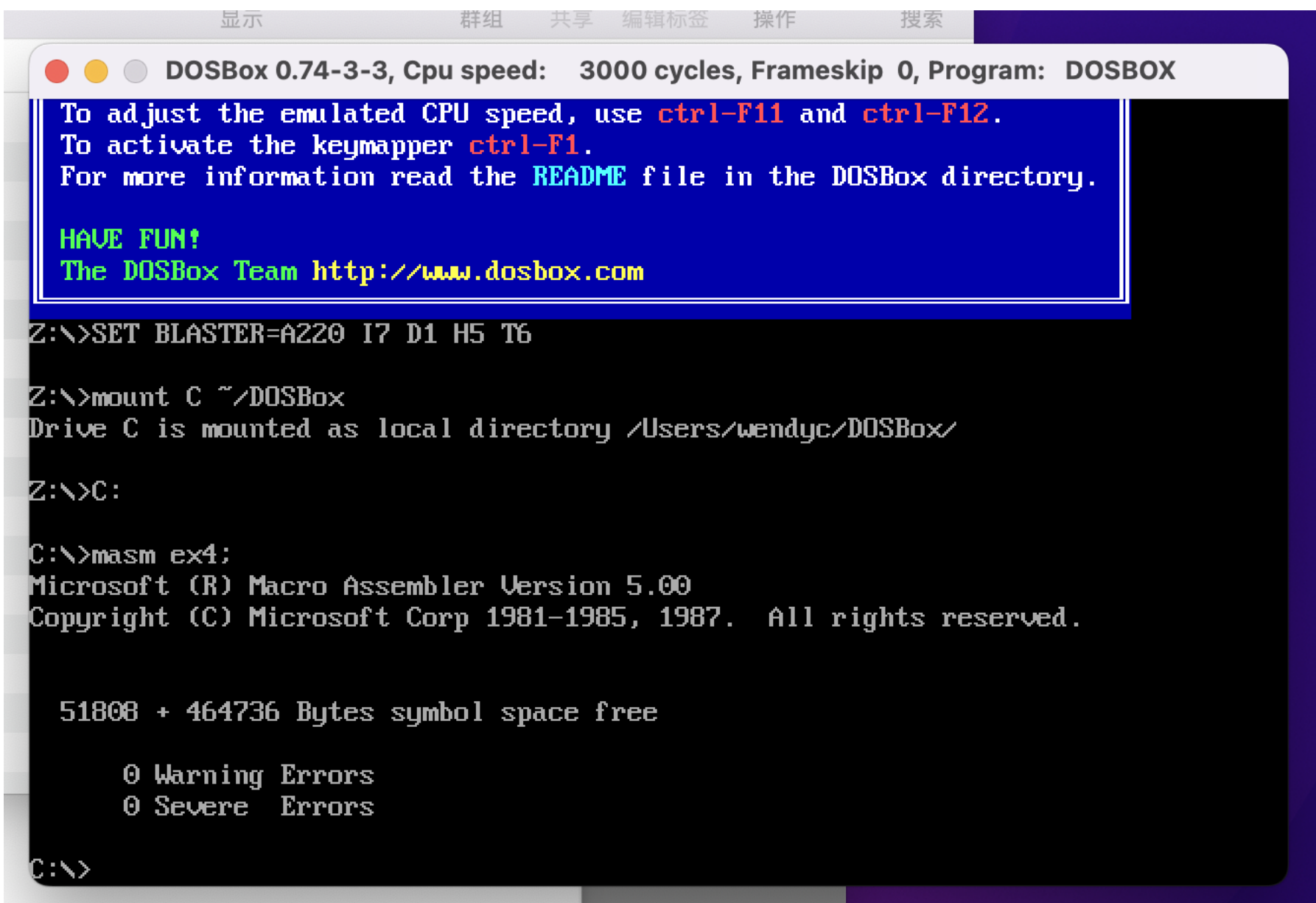
课程名称 汇编语言实验 实验项目名称 汇编语言编程、编译、连接及跟踪 实验项目编号 4 实验项目类型 上机 实验地点 517 成绩评定 _____
学生姓名 陈文笛 学号 2021103285 学院 网络空间安全 系 网络空间安全 专业 网络空间安全 实验时间 2023 年 3 月 13 日 下 午 ~ 月 日 午
温度 °C 湿度 指导教师 张银炎

任务 1

实验简介

将下面的程序保存为 ex4.asm, 并生成对应的可执行文件 ex4.exe

实验结果截图



```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
To adjust the emulated CPU speed, use ctrl-F11 and ctrl-F12.
To activate the keymapper ctrl-F1.
For more information read the README file in the DOSBox directory.
HAVE FUN!
The DOSBox Team http://www.dosbox.com

Z:\>SET BLASTER=A220 I7 D1 H5 T6

Z:\>mount C ~/DOSBox
Drive C is mounted as local directory /Users/wendyc/DOSBox/

Z:\>C:

C:\>masm ex4;
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

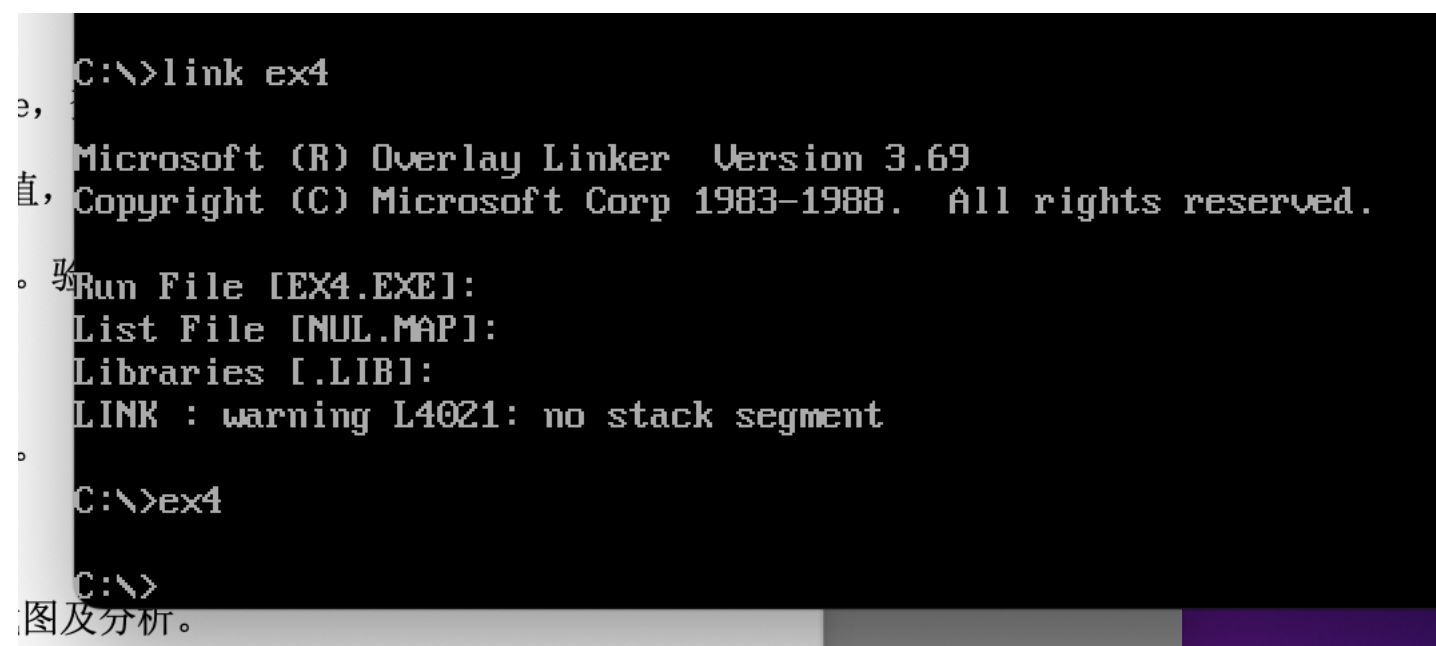
51808 + 464736 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>
```

学生签名 陈文笛

编译



链接与执行

实验结果分析

按回车后，重新出现了 c:\> 说明执行成功

任务 2

实验简介

用 debug 单步执行跟踪 ex4.exe 的执行过程。

实验结果截图

```

DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
01A3:0350 803E8B4A00 CMP BYTE PTR [4A8B],00 CS:4A8B=00
-quit
C:\>debug ex4.exe
-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 NV 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 NV 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 NV UP EI PL NZ NA PE NC
076A:000B 58 POP AX
-t
AX=076A BX=0000 CX=0016 DX=0000 SP=000C BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=2000 CS=076A IP=000C NV UP EI PL NZ NA PE NC
076A:000C 5B POP BX

```

进入 debug, 使用 t 命令开始单步执行

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=076A 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=076A 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=076A 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 58 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
-t
AX=7206 BX=076A 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
```

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
DS=075A ES=075A SS=2000 CS=076A IP=000F NU UP EI PL NZ NA PE NC
076A:000F 58 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
-t
AX=7206 BX=076A 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=076A 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
-p
Program terminated normally
-r
AX=4C00 BX=076A 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
```

到 int21, 使用 P 命令执行

实验结果分析

```
076A:0014 CD21          INT     21
-p
Program terminated normally
-r
AX=4C00  BX=076A  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
```

Int21 执行后，显示 program terminated normally, 说明程序执行正常

任务 3

实验简介

PSP 的头两个字节是 CD 20, 用 debug 加载 ex4.exe，查看 PSP 的内容。

实验结果截图

```
C:\>debug ex4.exe
-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
-d 075A:0000
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  . . . . .
```

DS=075A，则 PSP 的地址为 129E: 0。使用 D 命令查看内存。

实验结果分析

```
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  . . . . .
```

PSP 的内容如上。头两个字节是 CD 20 ，实验正确。

任务 4

实验简介

编写完整的汇编语言程序，计算 $1+2+3+\dots+20$ 的值，并将计算结果保存到 dl

实验结果截图

```

C:\>masm add:
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 add:
Microsoft (R) Overlay Linker Version 3.69
Copyright (C) Microsoft Corp 1983-1988.  All rights reserved.

LINK : warning L4021: no stack segment

C:\>add
C:\>_
```

编译、链接、运行

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

Z:\>C:

C:\>debug add.exe
-t

AX=FFFF BX=0000 CX=0012 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0002  NU UP EI PL NZ NA PO NC
076A:0002 B001          MOV     AL,01
-t

AX=FF01 BX=0000 CX=0012 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0004  NU UP EI PL NZ NA PO NC
076A:0004 B91400      MOV     CX,0014
-t

AX=FF01 BX=0000 CX=0014 DX=0000 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0007  NU UP EI PL NZ NA PO NC
076A:0007 02D0          ADD     DL,AL
-t

AX=FF01 BX=0000 CX=0014 DX=0001 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0009  NU UP EI PL NZ NA PO NC
076A:0009 0401          ADD     AL,01
-t_
```

用 debug 进行跟踪

中间 t 命令就不一一放出了

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
DS=075A ES=075A SS=0769 CS=076A IP=0009  NU UP EI NG NZ AC PE NC
076A:0009 0401      ADD     AL,01
-t
AX=FF15 BX=0000 CX=0001 DX=00D2 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=000B  NU UP EI PL NZ NA PO NC
076A:000B E2FA      LOOP    0007
-t
AX=FF15 BX=0000 CX=0000 DX=00D2 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=000D  NU UP EI PL NZ NA PO NC
076A:000D BB004C     MOV     AX,4C00
-t
AX=4C00 BX=0000 CX=0000 DX=00D2 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0010  NU UP EI PL NZ NA PO NC
076A:0010 CD21      INT     21
-p
Program terminated normally
-r
AX=4C00 BX=0000 CX=0000 DX=00D2 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0010  NU UP EI PL NZ NA PO NC
076A:0010 CD21      INT     21
-
```

跟踪结束

遇到的问题及解决方法


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

add.ASM(3): error A2105: Expected: instruction or directive
add.ASM(4): error A2105: Expected: instruction or directive
add.ASM(5): error A2105: Expected: instruction or directive
add.ASM(10): error A2105: Expected: instruction or directive

51808 + 464736 Bytes symbol space free

0 Warning Errors
4 Severe Errors
```

显示有错误，检查后发现是把 mov 打错为 move

实验结果分析

```
Program terminated normally
-r
AX=4C00 BX=0000 CX=0000 DX=00D2 SP=0000 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=0769 CS=076A IP=0010 NV UP EI PL NZ NA PO NC
076A:0010 CD21 INT 21
```

显示 program terminated normally, 说明程序执行正常

DL=D2, D2 转化为 10 进制为 210。1+2+3+...+20 =210。结果正确。

代码

```
assume cs:code
```

code segment

mov dl,0

mov al,1

mov cx,20

s: add dl,al

add al,1

loop s

mov ax,4c00h

int 21h

code ends

end

暨南大学本科实验报告专用纸(附页)
