

# 廈門大學



## 《汇编语言》实验报告

(一)

姓 名 苏一涵

学 号 36720232204041

学 院 信息学院

专 业 软件工程

2024 年 9 月

## 1 实验目的

- (1) 了解汇编语言程序(源程序)的基本组成部分;
- (2) 掌握汇编语言程序编写、编译、链接、运行的基本环境和步骤;
- (3) 自学并掌握运用 DEBUG 命令进行程序调试的基本命令。

## 2 实验环境

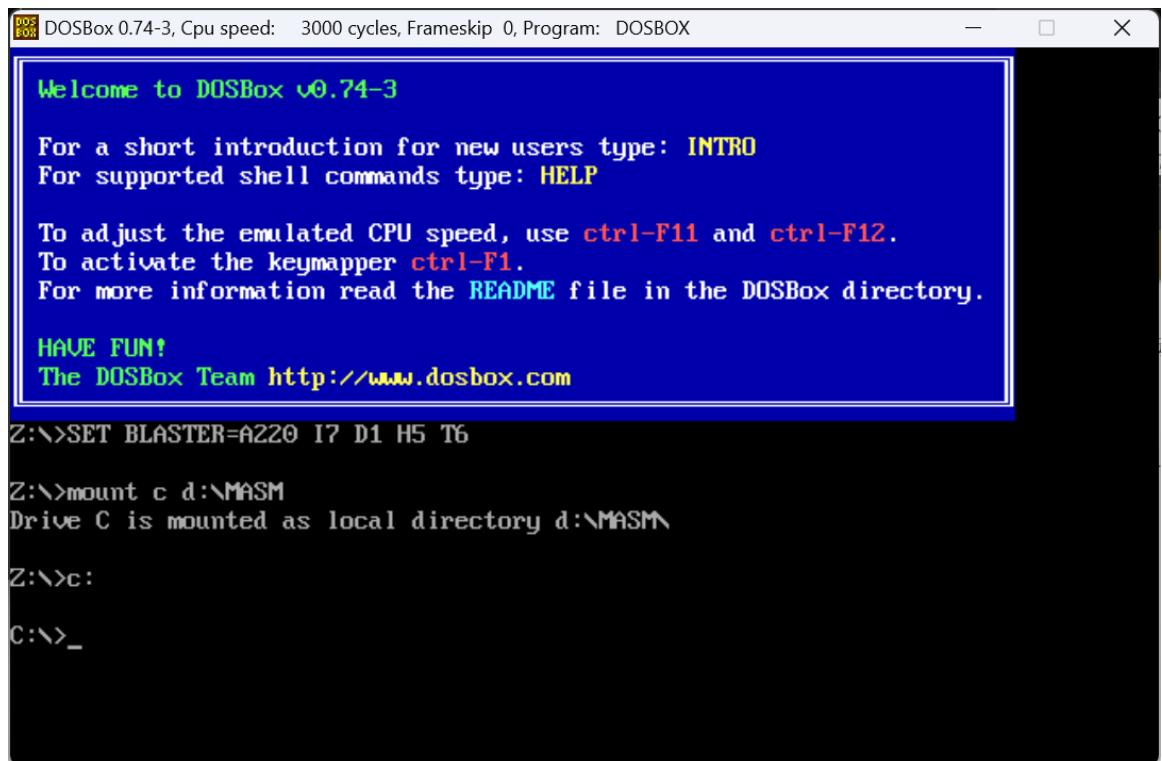
利用 DOSBox 在 64 位操作系统上模拟 DOS 环境来进行汇编编程

## 3 实验内容

- (1) 用给出的两个例程 a 和 b，分别采用模拟 DOS 环境以及集成环境完成程序的编辑、汇编、连接以及调试过程。
- (2) 提前了解汇编语言的一些助记词的意义以及使用，熟悉汇编操作以及 Debug 调试程序的操作

## 4 实验具体实现

- (1) 进行环境配置，如下图：



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

Welcome to DOSBox v0.74-3

For a short introduction for new users type: INTRO
For supported shell commands type: HELP

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 d:\MASM
Drive C is mounted as local directory d:\MASM\

Z:\>c:

C:\>_
```

## (2) 编写程序:

先创建后缀为 `asm` 的文件，将给出的俩个例程分别在上面复刻出来，具体如下图：

a.asm

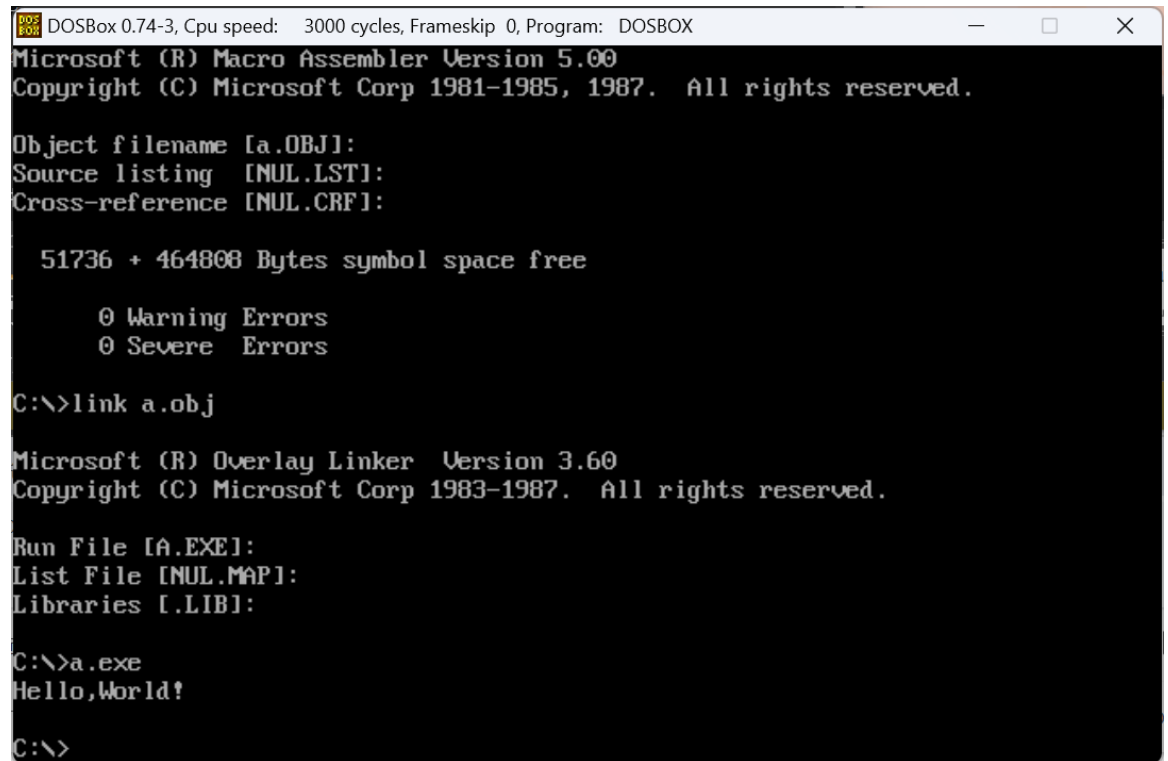
```
1  DSEG  SEGMENT
2  MESS  DB   'Hello, World!' , 0DH, 0AH, 24H
3  DSEG  ENDS
4
5  SSEG          SEGMENT PARA STACK
6                DW  256 DUP(?)
7  SSEG          ENDS
8
9  CSEG  SEGMENT
10         ASSUME  CS:CSEG, DS:DSEG
11  BEGIN: MOV  AX, DSEG
12         MOV  DS, AX
13         MOV  DX, OFFSET MESS
14         MOV  AH, 9
15
16         INT  21H
17         MOV  AH, 4CH
18         INT  21H
19  CSEG  ENDS
20  END    BEGIN
```

b.asm

```
1      DATAS SEGMENT
2          X DB 4
3          Y DB 5
4          Z DB ?
5          Z1 DB ?
6      DATAS ENDS
7
8      STACKS SEGMENT
9
10     STACKS ENDS
11
12     CODES SEGMENT
13         ASSUME CS:CODES, DS:DATAS
14
15     START:
16         MOV AX, DATAS
17         MOV DS, AX
18         MOV AL, X
19         ADD AL, Y
20         MOV BL, 8
21         IMUL BL
22         MOV BL, X
23         MOV BH, 0
24         SUB AX, BX
25         MOV BL, 2
26         IDIV BL
27         MOV Z, AL
28         MOV Z1, AH
29         MOV AL, Z
30         MOV AH, 0
31         MOV BL, 10
32         DIV BL;
33         MOV DX, AX
34         ADD DX, 3030H;
35         MOV AH, 2
36         INT 21H
37         MOV AH, 4CH
38         INT 21H
39
40     CODES ENDS
41     END START
```

(3) 对这两个例程进行分析测试：

i: 对于 a 程序，这是一个打印 hello world 的程序，首先在数据段定义了一个 MESS 变量，并赋予字符串 hello world，然后定义了一个堆栈段给他分配了 256 字节的空间不知道干啥用，再在代码段做了一个显示字符串的功能，通过调用 DOS 功能来输出字符串 "Hello,World!"，退出程序。运行结果如下：



```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [a.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51736 + 464808 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>link a.obj

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [A.EXE]:
List File [NUL.MAP]:
Libraries [LIB]:

C:\>a.exe
Hello,World!

C:\>
```

成功打印出 hello world，接下来将字符串该为 “I study in Informatic School of Xiamen University!”结果如下图：

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [a.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51736 + 464808 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>link a.obj

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [A.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:

C:\>a.exe
I study in Informatic School of Xiamen University!

C:\>
```

也是成功打印出来了

ii: 对于 b 程序，程序大体上是在数据段给 X 和 Y 分别赋值 4 和 5，Z 和 Z1 没赋值，然后大体操作就是将 X 和 Y 相加结果存到 AL 寄存器，再 AL\*8 把结果保存到 AX 寄存器，X 减去 BX 寄存器然后保存到 AX，AX 再除以 2 把存到 AL 寄存器，把 AL 存到 Z，Z 除以 10 并将余数保存到 DX 寄存器，最后打印出 DX+3030H 后的数据。运算公式应该就是  $((X+Y)*8-4)/2 \% 10 + 3030H$  都是 16 进制，结果如下：

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [b.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51774 + 464770 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>link b.obj

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

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

C:\>b.exe
3
C:\>
```

将 X 改为 6, Y 改为 8 得

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [b.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51774 + 464770 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>link b.obj

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

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

C:\>b.exe
5
C:\>
```

(4) 熟悉 debug 操作并利用 debug 调试程序

- i: 启用 debug 并将 a 程序的 H 和 W 分别改为小写



```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
5
C:\>MASM a.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [a.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:

51736 + 464808 Bytes symbol space free

0 Warning Errors
0 Severe Errors

C:\>link a.obj

Microsoft (R) Overlay Linker Version 3.60
Copyright (C) Microsoft Corp 1983-1987. All rights reserved.

Run File [A.EXE]:
List File [NUL.MAP]:
Libraries [.LIB]:

C:\>debug a.exe
- ▲
```

打开 debug，用 D 指令开始寻找 helloworld 所在的位置

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
-R
AX=FFFF BX=0000 CX=0220 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=075A ES=075A SS=076B CS=078B IP=0000 NU UP EI PL NZ NA PO NC
078B:0000 B86A07 MOV AX,076A
-D 075A
075A:0750 56 A1 58 27 39 46 U.X'9F
075A:0760 06 77 03 E9 8A 00 A1 36-22 2B 06 58 27 89 46 FE .w....6"+.X'.F.
075A:0770 2B C0 89 46 F8 89 46 FA-89 46 FC EB 22 90 8A 46 +..F..F..F..".F
075A:0780 08 2A E4 50 8B 5E FA FF-46 FA D1 E3 D1 E3 8B 76 .*P.^..F.....v
075A:0790 04 FF 70 02 FF 30 E8 CB-FE 83 C4 06 FF 46 FC 8B ..p..0.....F..
075A:07A0 46 06 39 46 FC 73 77 A1-58 27 39 46 FA 73 2A 8B F.9F.sw.X'9F.s*.
075A:07B0 46 FE 39 46 F8 73 C7 8B-46 F8 D1 E0 D1 E0 03 06 F.9F.s..F.....
075A:07C0 04 06 50 8B 46 FA D1 E0-D1 E0 03 46 04 50 FF 16 ..P.F.....F.P..
075A:07D0 C6 17 83 C4 04 0B C0 7E-A5 8A .....~..
-D 0109
075A:0100 6C 64 21 0D 0A 24 00 ld!..$.
075A:0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0180 00 00 00 00 00 00 00 00-00 .....
- ▲
```

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
075A:07A0 46 06 39 46 FC 73 77 A1-58 27 39 46 FA 73 2A 8B F.9F.sw.X'9F.s*.
075A:07B0 46 FE 39 46 F8 73 C7 8B-46 F8 D1 E0 D1 E0 03 06 F.9F.s..F.....
075A:07C0 04 06 50 8B 46 FA D1 E0-D1 E0 03 46 04 50 FF 16 ..P.F.....F.P..
075A:07D0 C6 17 83 C4 04 0B C0 7E-A5 8A .....~..
-D 0109
075A:0100                                6C 64 21 0D 0A 24 00 ld!..$.
075A:0110 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0120 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0130 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0140 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0150 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0160 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0170 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0180 00 00 00 00 00 00 00 00 00-00 .....
-D 00E0
075A:00E0 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:00F0 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0100 48 65 6C 6C 6F 2C 57 6F-72 6C 64 21 0D 0A 24 00 Hello,World!..$.
075A:0110 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0120 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0130 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0140 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0150 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
-E 0100
075A:0100 48.68 65. 6C. 6C. 6F. 2C. 57.77_
```

找到位置后使用 E 指令修改对应位置的数据使得 H 和 W 改为小写形式

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
075A:0160 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0170 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0180 00 00 00 00 00 00 00 00 00-00 .....
-D 00E0
075A:00E0 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:00F0 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0100 48 65 6C 6C 6F 2C 57 6F-72 6C 64 21 0D 0A 24 00 Hello,World!..$.
075A:0110 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0120 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0130 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0140 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0150 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
-E 0100
075A:0100 48.68 65. 6C. 6C. 6F. 2C. 57.77

-D 00E0
075A:00E0 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:00F0 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0100 68 65 6C 6C 6F 2C 77 6F-72 6C 64 21 0D 0A 24 00 hello,world!..$.
075A:0110 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0120 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0130 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0140 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
075A:0150 00 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
- ▲
```

改写成功

ii:利用 T 命令单步调试，以及熟悉其他指令

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=076A BX=0000 CX=0220 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=076B CS=078B IP=000B  NU UP EI PL NZ NA PO NC
078B:000B B409          MOV     AH,09
-T
AX=096A BX=0000 CX=0220 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=076B CS=078B IP=000A  NU UP EI PL NZ NA PO NC
078B:000A CD21          INT     21
-T
AX=096A BX=0000 CX=0220 DX=0000 SP=01FA BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=076B CS=F000 IP=14A0  NU UP DI PL NZ NA PO NC
F000:14A0 FB          STI
-T
AX=096A BX=0000 CX=0220 DX=0000 SP=01FA BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=076B CS=F000 IP=14A1  NU UP EI PL NZ NA PO NC
F000:14A1 FE38        ???     [BX+SI]          DS:0000=68
-T
hello,world!
AX=096A BX=0000 CX=0220 DX=0000 SP=01FA BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=076B CS=F000 IP=14A5  NU UP EI PL NZ NA PO NC
F000:14A5 CF          IRET
- ▲
```

其他指令的使用:

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
-R
AX=096A BX=0000 CX=0220 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000
DS=076A ES=075A SS=076B CS=078B IP=000C  NU UP EI PL NZ NA PO NC
078B:000C B44C          MOV     AH,4C
-F 1AF5:100 L20 1 2 3 4 5
-D 1AF5:100
1AF5:0100 01 02 03 04 05 01 02 03-04 05 01 02 03 04 05 01 .....
1AF5:0110 02 03 04 05 01 02 03 04-05 01 02 03 04 05 01 02 .....
1AF5:0120 63 74 20 66 69 6C 65 0A-00 10 01 57 72 69 74 65 ct file....Write
1AF5:0130 20 65 72 72 6F 72 20 6F-6E 20 6C 69 73 74 69 6E error on listin
1AF5:0140 67 20 66 69 6C 65 0A 00-11 01 57 72 69 74 65 20 g file....Write
1AF5:0150 65 72 72 6F 72 20 6F 6E-20 63 72 6F 73 73 2D 72 error on cross-r
1AF5:0160 65 66 65 72 65 6E 63 65-20 66 69 6C 65 0A 00 12 eference file...
1AF5:0170 01 55 6E 61 62 6C 65 20-74 6F 20 6F 70 65 6E 20 .Unable to open
-M 1AF5:100 13F 1AF5:140
-D 1AF5:100
1AF5:0100 01 02 03 04 05 01 02 03-04 05 01 02 03 04 05 01 .....
1AF5:0110 02 03 04 05 01 02 03 04-05 01 02 03 04 05 01 02 .....
1AF5:0120 63 74 20 66 69 6C 65 0A-00 10 01 57 72 69 74 65 ct file....Write
1AF5:0130 20 65 72 72 6F 72 20 6F-6E 20 6C 69 73 74 69 6E error on listin
1AF5:0140 01 02 03 04 05 01 02 03-04 05 01 02 03 04 05 01 .....
1AF5:0150 02 03 04 05 01 02 03 04-05 01 02 03 04 05 01 02 .....
1AF5:0160 63 74 20 66 69 6C 65 0A-00 10 01 57 72 69 74 65 ct file....Write
1AF5:0170 20 65 72 72 6F 72 20 6F-6E 20 6C 69 73 74 69 6E error on listin
- ▲
```

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
1AF5:0160 65 66 65 72 65 6E 63 65-20 66 69 6C 65 0A 00 12 eference file...
1AF5:0170 01 55 6E 61 62 6C 65 20-74 6F 20 6F 70 65 6E 20 .Unable to open
-M 1AF5:100 13F 1AF5:140
-D 1AF5:100
1AF5:0100 01 02 03 04 05 01 02 03-04 05 01 02 03 04 05 01 .....
1AF5:0110 02 03 04 05 01 02 03 04-05 01 02 03 04 05 01 02 .....
1AF5:0120 63 74 20 66 69 6C 65 0A-00 10 01 57 72 69 74 65 ct file....Write
1AF5:0130 20 65 72 72 6F 72 20 6F-6E 20 6C 69 73 74 69 6E error on listin
1AF5:0140 01 02 03 04 05 01 02 03-04 05 01 02 03 04 05 01 .....
1AF5:0150 02 03 04 05 01 02 03 04-05 01 02 03 04 05 01 02 .....
1AF5:0160 63 74 20 66 69 6C 65 0A-00 10 01 57 72 69 74 65 ct file....Write
1AF5:0170 20 65 72 72 6F 72 20 6F-6E 20 6C 69 73 74 69 6E error on listin
-H 10 1
0011 000F
-C 1AF5:100 13F 1AF5:140
-D
1AF5:0180 69 6E 70 75 74 20 66 69-6C 65 3A 20 25 73 0A 00 input file: %s..
1AF5:0190 13 01 55 6E 61 62 6C 65-20 74 6F 20 61 63 63 65 ..Unable to acce
1AF5:01A0 73 73 20 69 6E 70 75 74-20 66 69 6C 65 3A 20 25 ss input file: %
1AF5:01B0 73 0A 00 14 01 55 6E 61-62 6C 65 20 74 6F 20 6F s....Unable to o
1AF5:01C0 70 65 6E 20 6C 69 73 74-69 6E 67 20 66 69 6C 65 pen listing file
1AF5:01D0 3A 20 25 73 0A 00 15 01-55 6E 61 62 6C 65 20 74 : %s....Unable t
1AF5:01E0 6F 20 6F 70 65 6E 20 6F-62 6A 65 63 74 20 66 69 o open object fi
1AF5:01F0 6C 65 3A 20 25 73 0A 00-16 01 20 57 61 72 6E 69 le: %s.... Warni
```

## 5 实验分析与总结

在实验过程中，对 b 程序，改变 XY 的值可使得运算的结果也发生改变，但是当赋值过大时就会报错

```
DOSBox 0.74-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DOSBOX
HAVE FUN!
The DOSBox Team http://www.dosbox.com

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

Z:\>mount c d:\MASM
Drive C is mounted as local directory d:\MASM\

Z:\>c:

C:\>MASM b.asm
Microsoft (R) Macro Assembler Version 5.00
Copyright (C) Microsoft Corp 1981-1985, 1987. All rights reserved.

Object filename [b.OBJ]:
Source listing [NUL.LST]:
Cross-reference [NUL.CRF]:
b.asm(2): error A2029: Division by 0 or overflow

51774 + 464770 Bytes symbol space free

0 Warning Errors
1 Severe Errors

C:\>_
```

说明赋值不能超过寄存器的大小。

同时，通过这次实验，我初步了解了 dosbox 的使用和 debug 的使用，更深刻的理解了数据在寄存器中的存放，但对于例程 b 的输出结果仍然有疑问，输出的结果与我手动计算的不同，也许是表达式的推理有误，还需要加强理解。