

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 查看 CPU 和内存 实验项目编号 2 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 2 日 下午 ~ 3 月 2 日 下午 温度 °C 湿度 指导教师 张银炎

学生签名 陈文笛

实验【1】简介

1. 打开 DOSBox, 输入 debug 按回车进入 Debug 程序。
2. 实验任务<1>仅利用寄存器 BL, 用 A 命令将采用 mov 和 add 指令编写计算 $2+13+108+39+11$ 的值的汇编程序写入物理地址 20010H 开始的内存单元中, 要求完成计算后 CS:IP 为 2000:10, 并用 T 命令运行程序, 然后用 R 命令查看计算结果。用 U 命令查看写入的汇编程序。

实验【1】结果截图

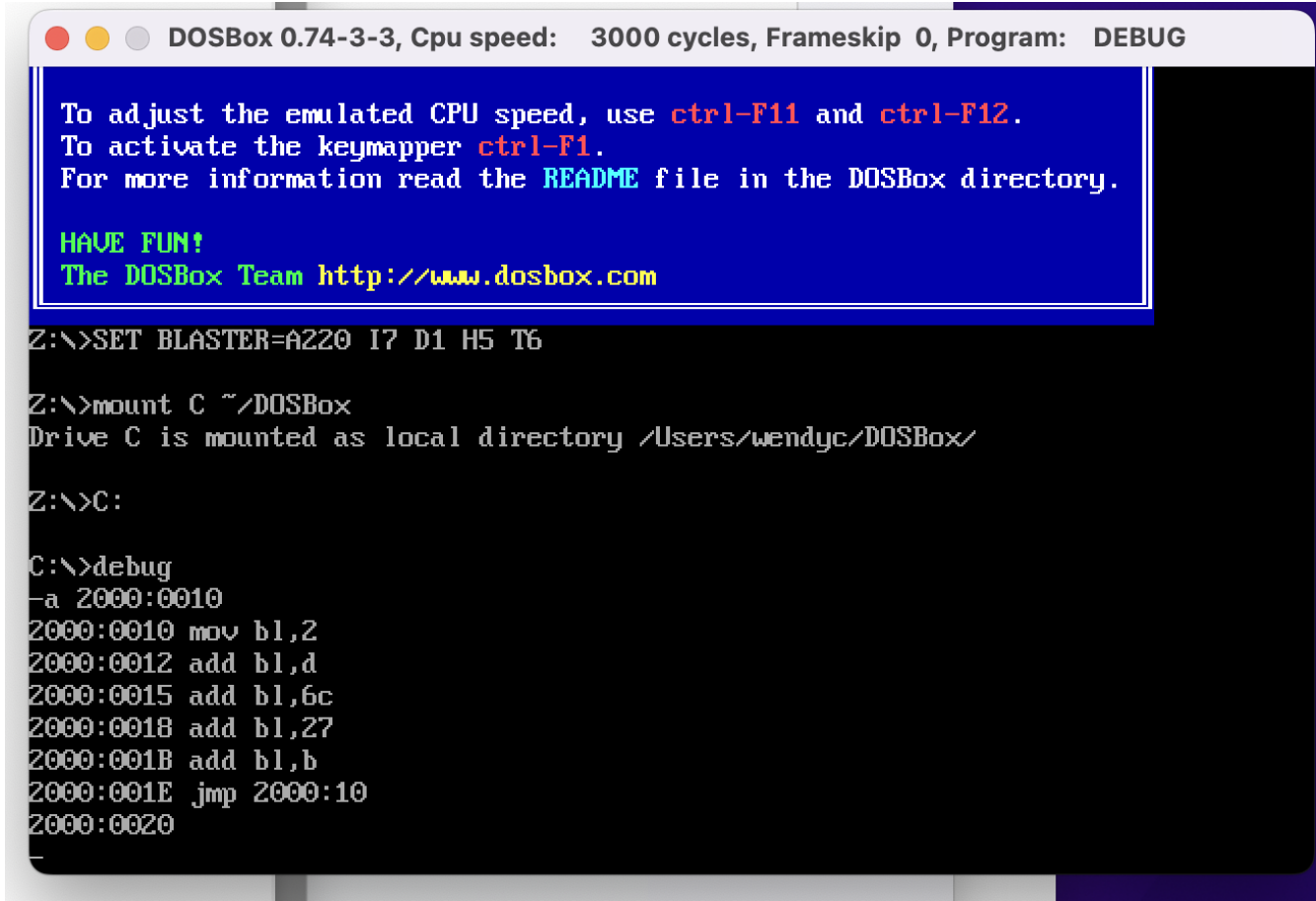
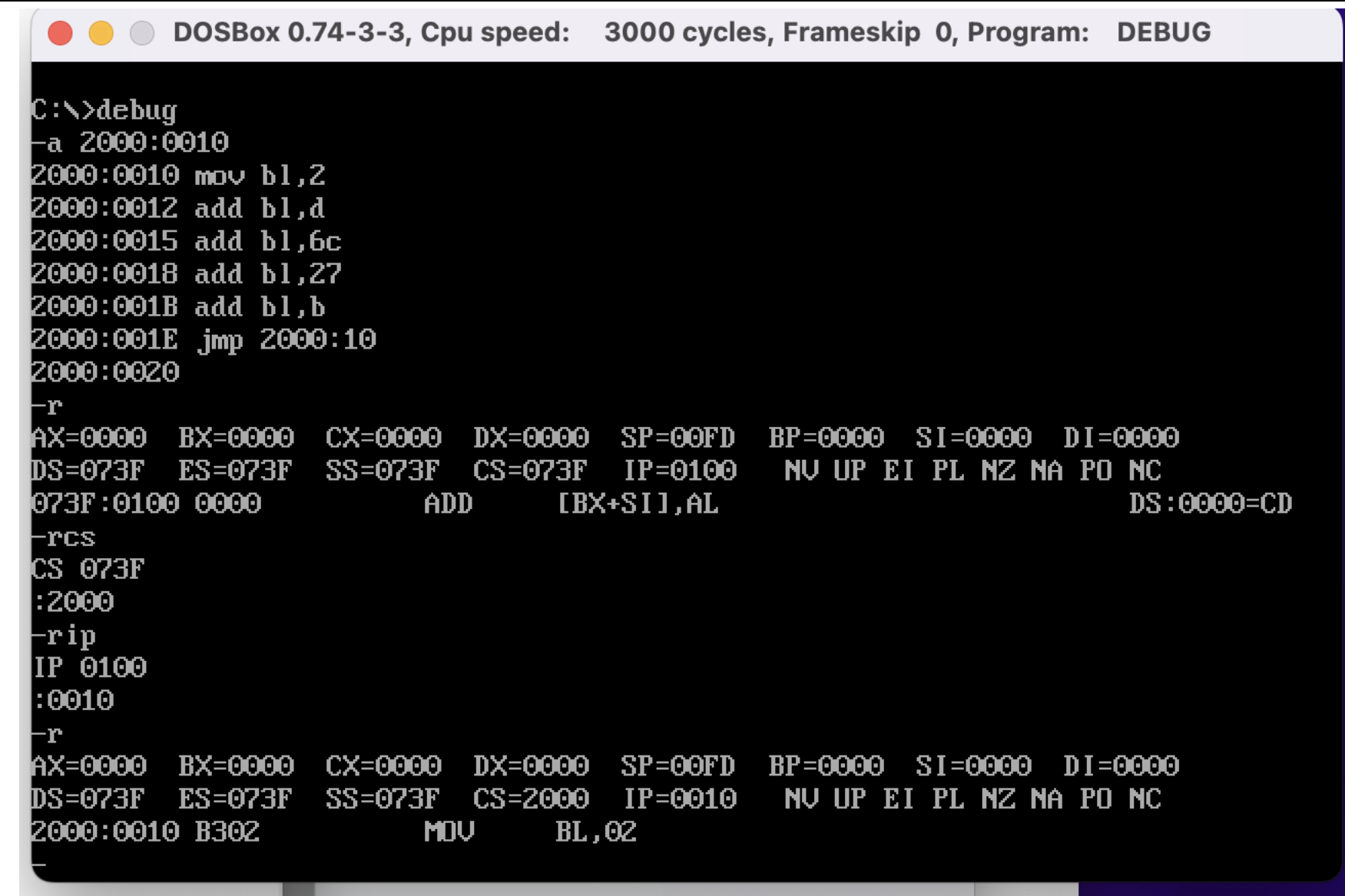


图 1: 进入 Debug 程序。用 A 命令将采用 mov 和 add 指令编写计算 $2+13+108+39+11$ 的值的汇编程序写入物理地址 20010H 开始的内存单元中, 并设置最后的 CS:IP 为 2000:10。

暨南大学本科实验报告专用纸(附页)



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

C:\>debug
-a 2000:0010
2000:0010 mov bl,2
2000:0012 add bl,d
2000:0015 add bl,6c
2000:0018 add bl,27
2000:001B add bl,b
2000:001E jmp 2000:10
2000:0020
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=073F IP=0100  NU UP EI PL NZ NA PO NC
073F:0100 0000          ADD     [BX+SI],AL          DS:0000=CD
-r cs
CS 073F
:2000
-r ip
IP 0100
:0010
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2000 IP=0010  NU UP EI PL NZ NA PO NC
2000:0010 B302          MOV     BL,02
```

图 2:

r 命令查看 CPU 中寄存器的状态。

r 命令修改 CS: IP 中的内容。使 CS: IP 为 2000:0010。

再次用 r 命令查看 CPU 中寄存器的状态 CS=2000, IP=0010。

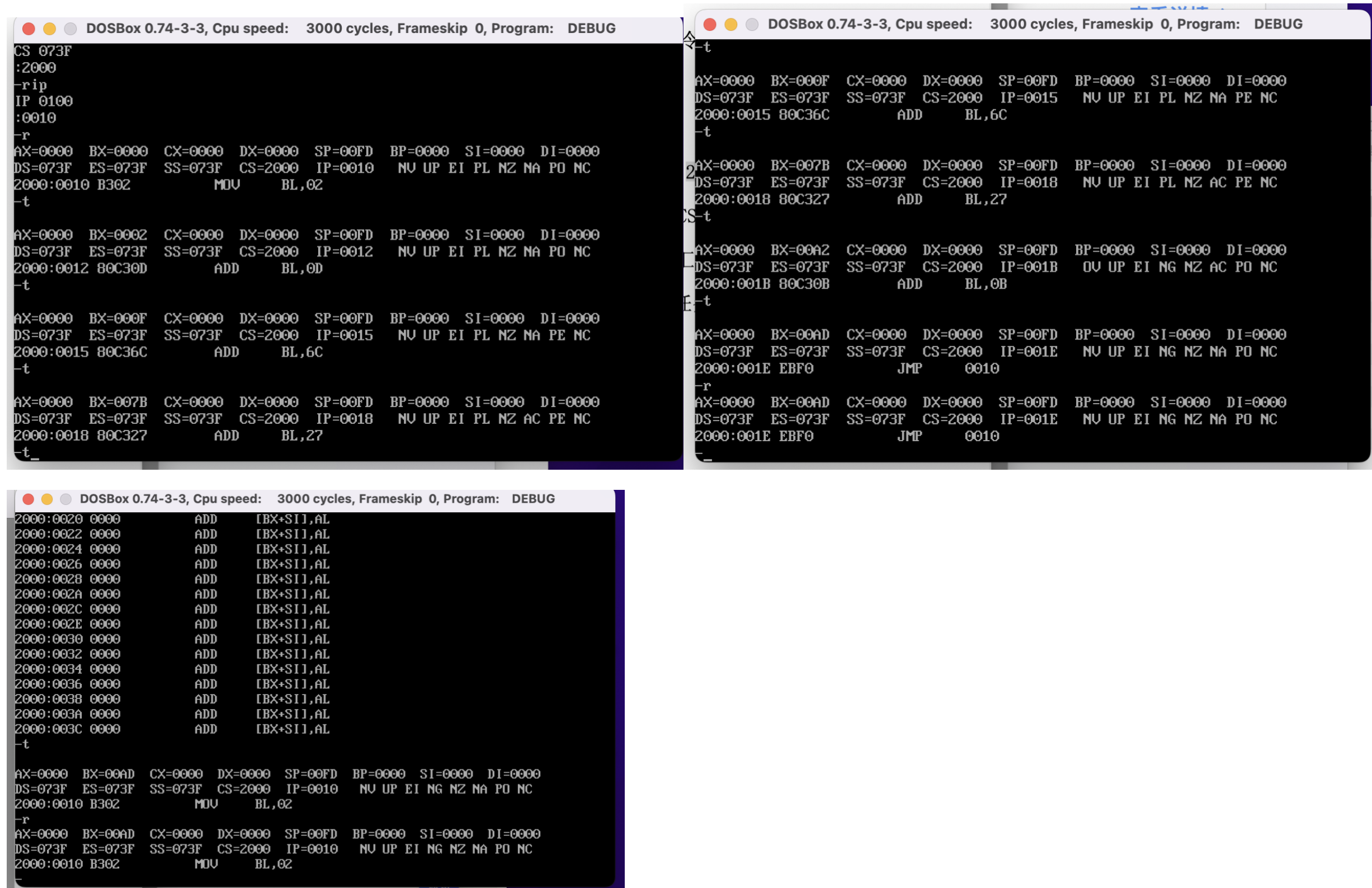


图 3, 4, 5:

使用 t 命令来执行之前写入的指令。

(一开始少执行了一次 t 命令, 可以看到图 4 中 IP=001E, 所以在图 5 又执行了一次 t 命令)

实验【2】简介

找到生产日期并试图修改

实验【2】结果截图

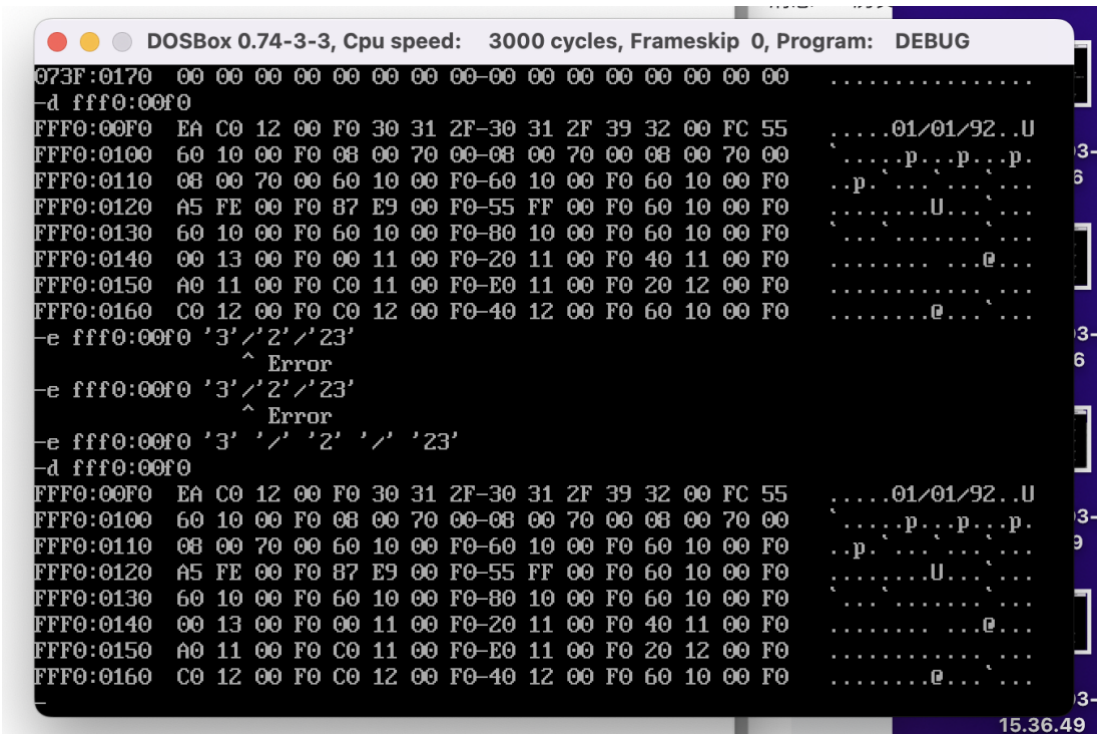


图 1:可见生产日期：01/01/92

试图修改为 3/2/23，再一次查看，修改失败。

实验【2】结果分析

不能改写。因为该生产日期在 ROM 上。ROM 为只读存储器--Read-Only Memory，只能读出信息无法写入信息。信息一旦写入后就固定下来，即使切断电源，信息也不会丢失，所以又称为固定存储器。

书本 P13，向地址 C0000-FFFFF 的内存单元写入数据的操作是无效的，因为这等于改写只读存储器中的内容。

实验【3】简介

向内存 B800H 的单元中写入数据。

实验【3】结果截图

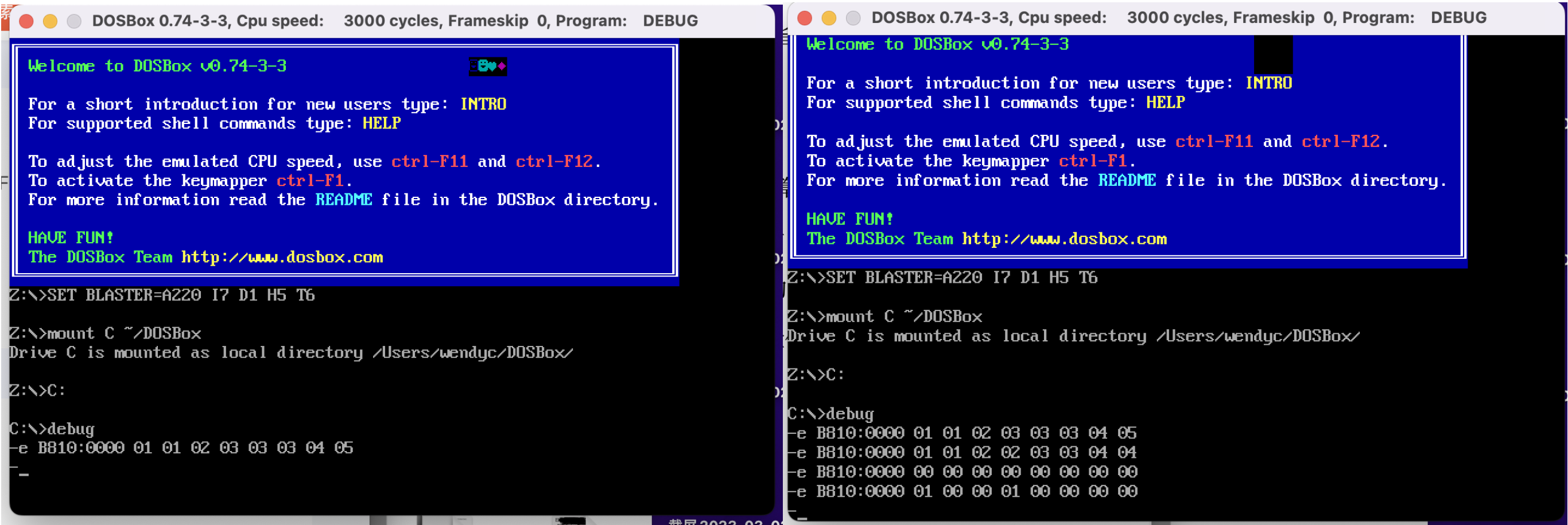


图 2、3:蓝色框内有图案出现。修改输入的数据，有不同的图案。

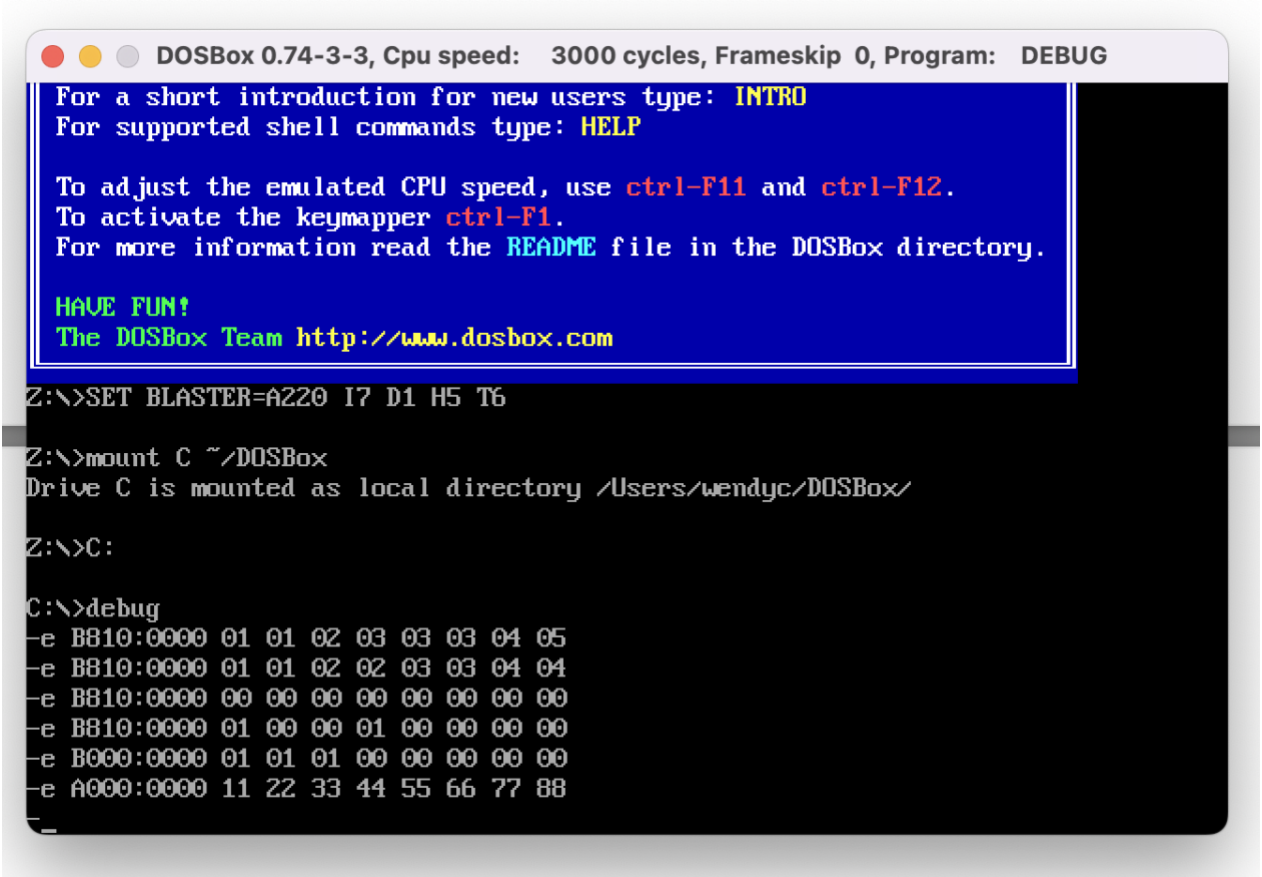


图 4: 换一个地址写入，图案消失。

实验【3】 结果分析

8086CPU 的显存地址空间是 A0000H-BFFFFH，其中 B8000H-BFFFFH 为 80*25 彩色字符模式显示缓存区，当向这个地址空间写入数据时，这些数据会立即出现在显示器上。

遇到的问题及解决方法

DEBUG 下的数据都是十六进制数。

错误：

忘记把 13 和 11 也转换成 16 进制


```
Drive C is mounted as local directo
Z:\>C:
C:\>debug
-a 2000:0010
2000:0010 mov BL,2
2000:0012 add BL,13
2000:0015 add BL,6c
2000:0018 add B1,27
2000:001B add BL,11
2000:001E jmp 2000:10
2000:0020
```

最后出结果的时候发现不对

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
-T
AX=0000 BX=0015 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2000 IP=0015 NU UP EI PL NZ NA PO NC
2000:0015 80C36C      ADD     BL,6C
-T
AX=0000 BX=00B1 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2000 IP=0018 OU UP EI NG NZ AC PE NC
2000:0018 80C327      ADD     BL,27
-T
AX=0000 BX=00A8 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2000 IP=001B NU UP EI NG NZ NA PO NC
2000:001B 80C311      ADD     BL,11
-T
AX=0000 BX=00B9 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2000 IP=001E NU UP EI NG NZ NA PO NC
2000:001E EBF0      JMP     0010
-R
AX=0000 BX=00B9 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2000 IP=001E NU UP EI NG NZ NA PO NC
2000:001E EBF0      JMP     0010
```

可以看到显示的结果是 B9，而 $2+13+108+39+11=173$ ，换成 16 进制是 AD 。说明不对。

错误：

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
073F:0170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
-a fff0:00f0
FFF0:00f0 EA C0 12 00 F0 30 31 2F-30 31 2F 39 32 00 FC 55 .....01/01/92..U
FFF0:0100 60 10 00 F0 08 00 70 00-08 00 70 00 08 00 70 00 .....p..p..p..
FFF0:0110 08 00 70 00 60 10 00 F0-60 10 00 F0 60 10 00 F0 .....p.....
FFF0:0120 A5 FE 00 F0 87 E9 00 F0-55 FF 00 F0 60 10 00 F0 .....U.....
FFF0:0130 60 10 00 F0 60 10 00 F0-80 10 00 F0 60 10 00 F0 .....
FFF0:0140 00 13 00 F0 00 11 00 F0-20 11 00 F0 40 11 00 F0 .....e...
FFF0:0150 A0 11 00 F0 C0 11 00 F0-E0 11 00 F0 20 12 00 F0 .....
FFF0:0160 C0 12 00 F0 C0 12 00 F0-40 12 00 F0 60 10 00 F0 .....e...
-e fff0:00f0 '3'/'2'/'23'
^
Error
-e fff0:00f0 '3'/'2'/'23'
^
Error
-e fff0:00f0 '3' '/' '2' '/' '23'
-a fff0:00f0
FFF0:00f0 EA C0 12 00 F0 30 31 2F-30 31 2F 39 32 00 FC 55 .....01/01/92..U
FFF0:0100 60 10 00 F0 08 00 70 00-08 00 70 00 08 00 70 00 .....p..p..p..
FFF0:0110 08 00 70 00 60 10 00 F0-60 10 00 F0 60 10 00 F0 .....p.....
FFF0:0120 A5 FE 00 F0 87 E9 00 F0-55 FF 00 F0 60 10 00 F0 .....U.....
FFF0:0130 60 10 00 F0 60 10 00 F0-80 10 00 F0 60 10 00 F0 .....
FFF0:0140 00 13 00 F0 00 11 00 F0-20 11 00 F0 40 11 00 F0 .....e...
FFF0:0150 A0 11 00 F0 C0 11 00 F0-E0 11 00 F0 20 12 00 F0 .....
FFF0:0160 C0 12 00 F0 C0 12 00 F0-40 12 00 F0 60 10 00 F0 .....e...
15.36.49
```

输入/的时候也要打引号