

暨南大学本科实验报告专用纸

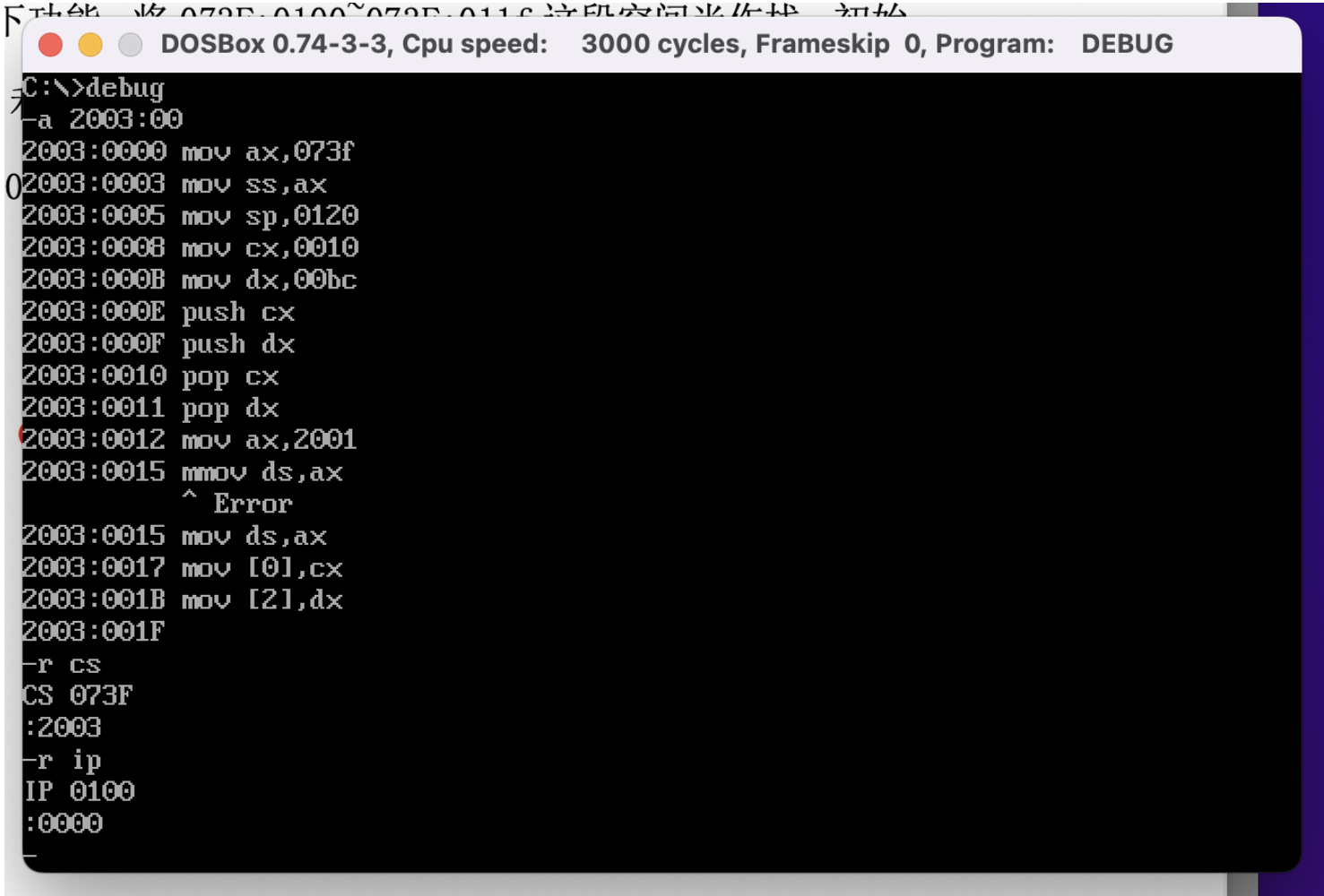
课程名称 汇编语言实验 实验项目名称 栈及内存访问 实验项目编号 3 实验项目类型 上机 实验地点 517 成绩评定 _____
学生姓名 陈文笛 学号 2021103285 学院 网络空间安全 系 网络空间安全 专业 网络空间安全 实验时间 2023 年 3 月 6 日 午 ~ 3 月 6 日 午 温
度 °C 湿度 指导教师 张银炎

学生签名 陈文笛

实验简介

编写汇编语言程序，实现以下功能：将 073F:0100~073F:011f 这段空间当作栈，初始 状态栈为空，设置 CX=10H，DX=BCH，利用栈交换 CX 和 DX 中的数据，完成交换后将 CX、DX 中 的内容依次写入内存单元 20010H~20013H 中。

实验结果截图



```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=073F BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=0003 NU UP EI PL NZ NA PO NC
2003:0003 8ED0          MOV     SS,AX
-t
AX=073F BX=0000 CX=0000 DX=0000 SP=0120 BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=0008 NU UP EI PL NZ NA PO NC
2003:0008 B91000      MOV     CX,0010
-t
AX=073F BX=0000 CX=0010 DX=0000 SP=0120 BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=000B NU UP EI PL NZ NA PO NC
2003:000B BAB000      MOV     DX,00BC
-t
AX=073F BX=0000 CX=0010 DX=00BC SP=0120 BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=000E NU UP EI PL NZ NA PO NC
2003:000E 51          PUSH    CX
-t
AX=073F BX=0000 CX=0010 DX=00BC SP=011E BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=000F NU UP EI PL NZ NA PO NC
2003:000F 52          PUSH    DX
-t
```

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=073F BX=0000 CX=0010 DX=00BC SP=0120 BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=000E NU UP EI PL NZ NA PO NC
2003:000E 51          PUSH    CX
-t
AX=073F BX=0000 CX=0010 DX=00BC SP=011E BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=000F NU UP EI PL NZ NA PO NC
2003:000F 52          PUSH    DX
-t
AX=073F BX=0000 CX=0010 DX=00BC SP=011C BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=2003 IP=0010 NU UP EI PL NZ NA PO NC
2003:0010 59          POP     CX
-t
-d 073f:0110
073F:0110 00 00 3F 07 00 00 10 00-03 20 A3 01 BC 00 10 00 ..?.....
073F:0120 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
073F:0130 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
073F:0140 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
073F:0150 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
073F:0160 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
073F:0170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
073F:0180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
```

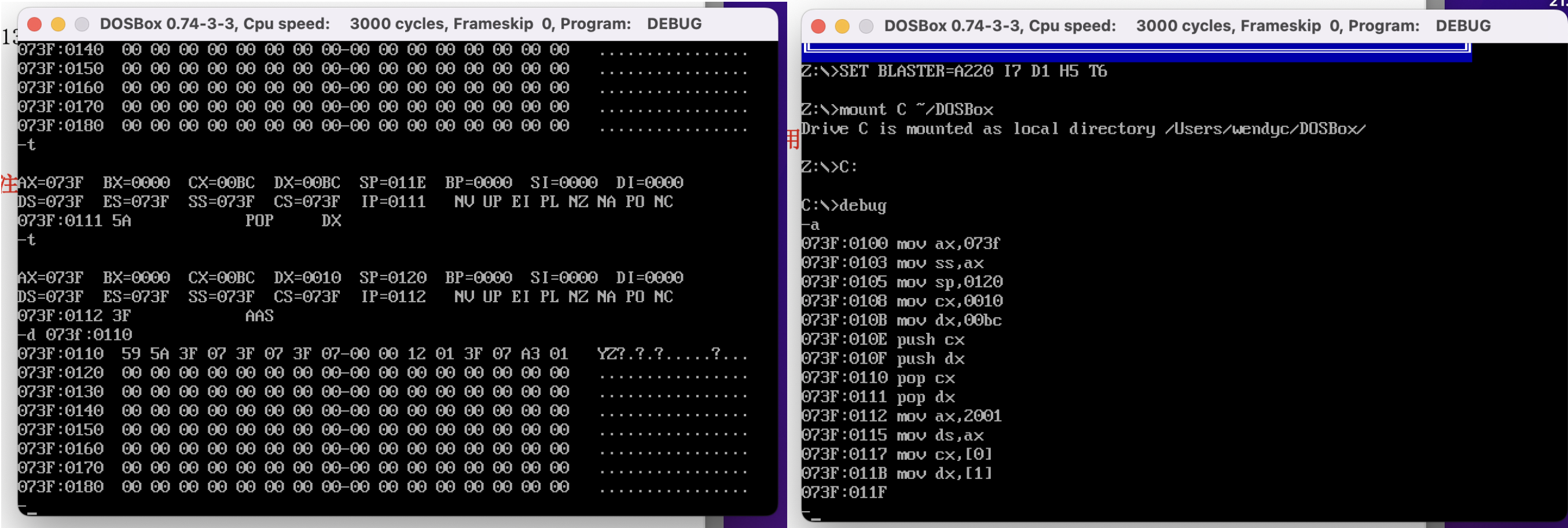
右图：cx、dx 入栈成功

```
DOSBox 0.74-3-3, Cpu speed: 3000 cycles, Frameskip 0, Program: DEBUG
AX=2001 BX=0000 CX=00BC DX=0010 SP=0120 BP=0000 SI=0000 DI=0000
DS=2001 ES=073F SS=073F CS=2003 IP=0017 NU UP EI PL NZ NA PO NC
2003:0017 890E0000      MOV     [0000],CX          DS:0000=0000
-t
AX=2001 BX=0000 CX=00BC DX=0010 SP=0120 BP=0000 SI=0000 DI=0000
DS=2001 ES=073F SS=073F CS=2003 IP=001B NU UP EI PL NZ NA PO NC
2003:001B 89160200      MOV     [0002],DX          DS:0002=0000
-t
AX=2001 BX=0000 CX=00BC DX=0010 SP=0120 BP=0000 SI=0000 DI=0000
DS=2001 ES=073F SS=073F CS=2003 IP=001F NU UP EI PL NZ NA PO NC
2003:001F 0000          ADD     [BX+SI],AL          DS:0000=BC
-t
-d 2001:0000
2001:0000 BC 00 10 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0010 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0020 B8 3F 07 8E D0 BC 20 01-B9 10 00 BA BC 00 51 52 .?....QR
2001:0030 59 5A B8 01 20 8E D8 89-0E 00 00 89 16 02 00 00 YZ..
2001:0040 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0050 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0060 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0070 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
```

cd、dx 成功取出并存入 20010H~20013H

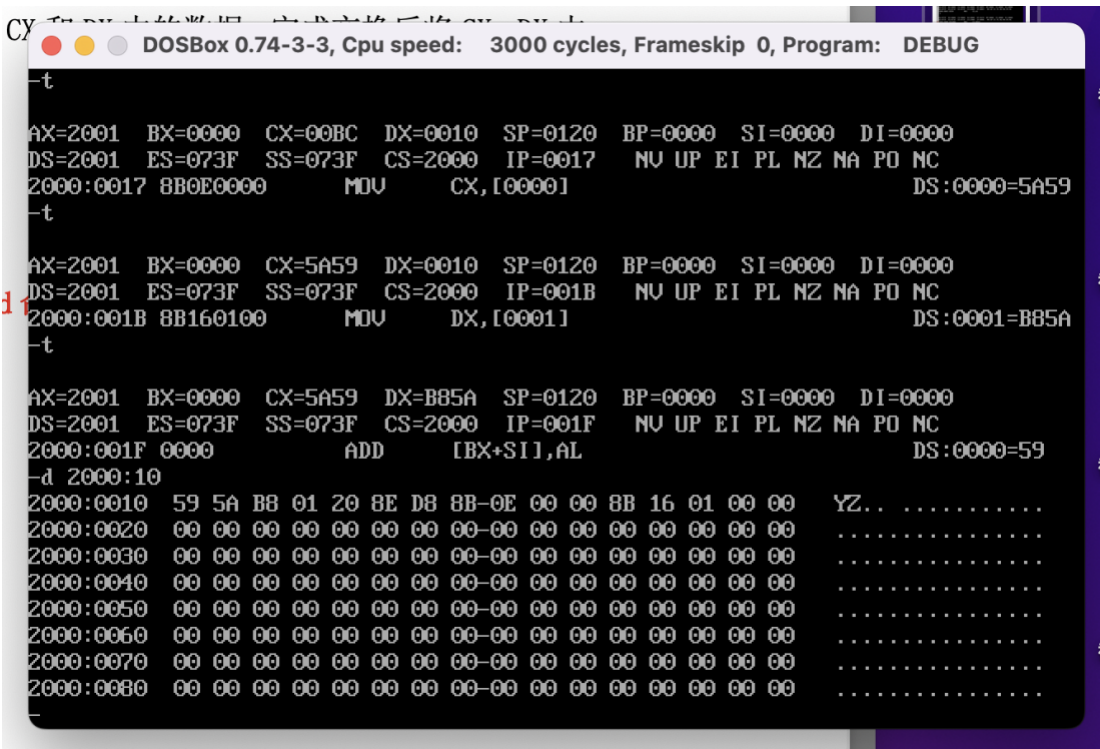
遇到的问题及解决方法

- 1.出现了没有写过的命令 AAS。发现命令所用的内存空间在栈内，估计是栈的操作影响了存储的命令。
- 2.栈进行了 pop 操作后，栈的内存空间中出现了不一样的字符。



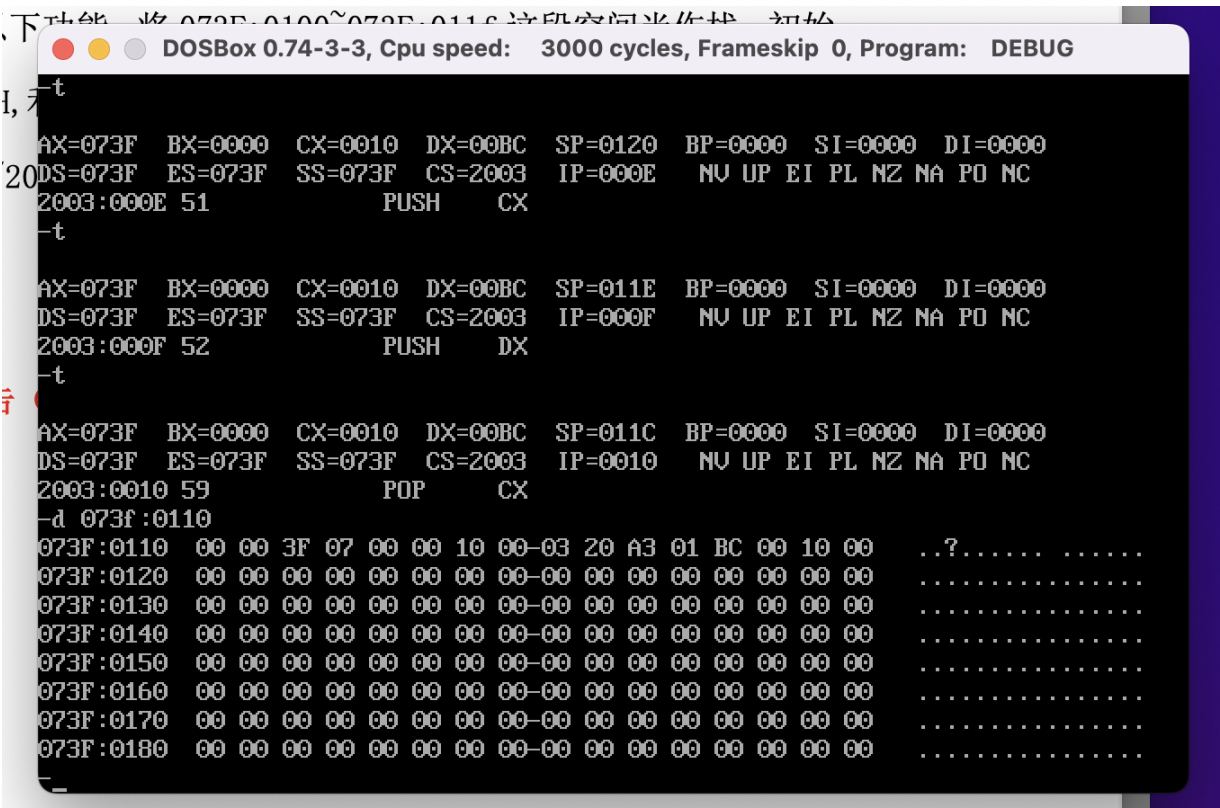
解决方法：将命令写在与栈不同的空间中。

3. 可以看到 2000:10 的存储值不是我们想要的



解决方法：mov cx,[0] mov dx,[1] 应该改为 mov [0],cx mov [2],dx

实验结果分析



cx、dx 入栈成功

以下功能：将 070F:0100~070F:0110 这段空间当作堆 初始
H, 不
~20
告

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

```
-t
AX=2001 BX=0000 CX=00BC DX=0010 SP=0120 BP=0000 SI=0000 DI=0000
DS=2001 ES=073F SS=073F CS=2003 IP=0017  NU UP EI PL NZ NA PO NC
2003:0017 890E0000      MOV     [0000],CX      DS:0000=0000
-t
AX=2001 BX=0000 CX=00BC DX=0010 SP=0120 BP=0000 SI=0000 DI=0000
DS=2001 ES=073F SS=073F CS=2003 IP=001B  NU UP EI PL NZ NA PO NC
2003:001B 89160200      MOV     [0002],DX      DS:0002=0000
-t
AX=2001 BX=0000 CX=00BC DX=0010 SP=0120 BP=0000 SI=0000 DI=0000
DS=2001 ES=073F SS=073F CS=2003 IP=001F  NU UP EI PL NZ NA PO NC
2003:001F 0000      ADD     [BX+SI],AL      DS:0000=BC
-d 2001:0000
2001:0000  BC 00 10 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0010  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0020  B8 3F 07 8E D0 BC 20 01-B9 10 00 BA BC 00 51 52  .?....  ....QR
2001:0030  59 5A B8 01 20 8E D8 89-0E 00 00 89 16 02 00 00  YZ..  ....
2001:0040  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0050  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0060  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
2001:0070  00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....

```

cd、dx 成功取出并存入 20010H~20013H