

南京林业大学



汇编语言上机实验 任务书

实验二 用机器指令和汇编指令编程

一. 实验目的

二. 实验内容

程序输入过程

```
-a 200:0000
0200:0000 mov ax,ffff
0200:0003 mov ds,ax
0200:0005 mov ax,2200
0200:0008 mov ss,ax
0200:000A mov sp,0100
0200:000D mov ax,[0]
0200:0010 add ax,[2]
0200:0014 mov bx,[4]
0200:0018 add bx,[6]
0200:001C push ax
0200:001D push bx
0200:001E pop ax
0200:001F pop bx
0200:0020 push [4]
0200:0024 push [6]
0200:0028
-r
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F SS=073F CS=0200 IP=0000 NU UP EI PL NZ NA PO NC
0200:0000 B8FFFF MOV AX,FFFF
-
```

程序执行到第 5 行, ax=C0EA

```
AX=C0EA BX=0000 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=0010 NU UP EI PL NZ NA PO NC
0200:0010 03060200 ADD AX,[0002] DS:0002=0012
-
```

程序执行到第 6 行, ax=C0FC

```
-t
AX=C0FC BX=0000 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=0014 NU UP EI NG NZ NA PE NC
0200:0014 8B1E0400 MOV BX,[0004] DS:0004=30F0
-
```

程序执行到第 7 行, bx=30F0

```

-t
AX=C0FC BX=30F0 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=001B  NU UP EI NG NZ NA PE NC
0200:001B 031E0600      ADD     BX,[0006]          DS:0006=2F31

```

程序执行到第 8 行, bx=6021

```

-t
AX=C0FC BX=6021 CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=001C  NU UP EI PL NZ NA PE NC
0200:001C 50          PUSH    AX

```

程序执行到第 9 行, sp=00FE; 修改的内存单元的地址是 2200:0100
内容为 C0FC

```

-t
AX=C0FC BX=6021 CX=0000 DX=0000 SP=00FE BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=001D  NU UP EI PL NZ NA PE NC
0200:001D 53          PUSH    BX

```

程序执行到第 10 行, sp=00FC; 修改的内存单元的地址是 2200:00FE
内容为 6021

```

-t
AX=C0FC BX=6021 CX=0000 DX=0000 SP=00FC BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=001E  NU UP EI PL NZ NA PE NC
0200:001E 58          POP     AX

```

程序执行到第 11 行, sp=00FE, ax=6021

```

-t
AX=6021 BX=6021 CX=0000 DX=0000 SP=00FE BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=001F  NU UP EI PL NZ NA PE NC
0200:001F 5B          POP     BX

```

程序执行到第 12 行, sp=0100, bx=C0FC

```

-t
AX=6021 BX=C0FC CX=0000 DX=0000 SP=0100 BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=0020  NU UP EI PL NZ NA PE NC
0200:0020 FF360400      PUSH      [0004]                      DS:0004=30F0

```

程序执行到第 13 行, sp=00FE;修改的内存单元的地址是 2200:0100
内容为 30F0

```

-t
AX=6021 BX=C0FC CX=0000 DX=0000 SP=00FE BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=0024  NU UP EI PL NZ NA PE NC
0200:0024 FF360600      PUSH      [0006]                      DS:0006=2F31

```

程序执行到第 14 行, sp=00FC;修改内存单元的地址是 2200:00FE
内容为 2F31

```

-t
AX=6021 BX=C0FC CX=0000 DX=0000 SP=00FC BP=0000 SI=0000 DI=0000
DS=FFFF ES=073F SS=2200 CS=0200 IP=0028  NU UP EI PL NZ NA PE NC
0200:0028 36          SS:
0200:0029 A0324A      MOV      AL,[4A32]                      SS:4A32=00

```

第 2 题：因为 Debug 过程中会发生中断，而发生中断时 CPU 会自动把一些关键信息存储到栈里，所以栈的内容会变化。