

Hello 另类方式

——手工 Debug 输入机器码实验报告

2351273 邓语乐

一、实验目的

掌握用 debug 工具手工输入汇编代码并运行的方法,理解机器码与汇编指令的对应关系。
并学习学院服务器下的 hello 剖析.pdf 文件中对 hello 的另类执行方式,学会应用、学习、转化或复现。

二、实验步骤

1. 启动 debug 并输入代码

```
debug
-a 100
MOV AH,9
MOV DX,010D
INT 21
MOV AH,4C
INT 21
```

(空行结束)

2. 输入字符串数据

```
-e 010D 'Hello$'
```

3. 查看反汇编代码

```
-u 100
```

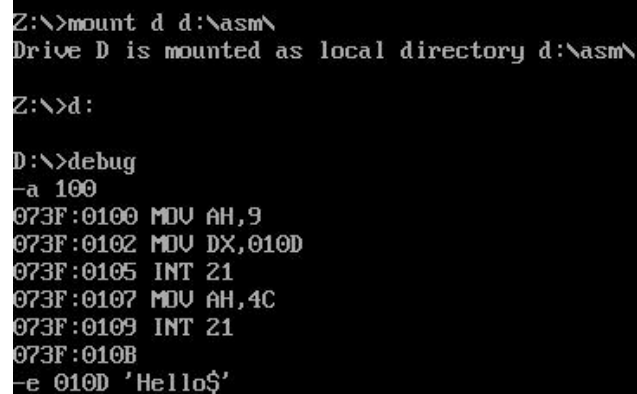
4. 查看数据段

```
-d 010D
```

5. 运行程序

```
-g =100
```

三、实验结果截图



```
Z:\>mount d d:\asm\
Drive D is mounted as local directory d:\asm\

Z:\>d:

D:\>debug
-a 100
073F:0100 MOV AH,9
073F:0102 MOV DX,010D
073F:0105 INT 21
073F:0107 MOV AH,4C
073F:0109 INT 21
073F:010B
-e 010D 'Hello$'
```

```
073F:0107 MOV AH,4C
073F:0109 INT 21
073F:010B
-e 010D 'Hello$'
-u 100
073F:0100 B409      MOV     AH,09
073F:0102 BA0D01    MOV     DX,010D
073F:0105 CD21      INT      21
073F:0107 B44C      MOV     AH,4C
073F:0109 CD21      INT      21
073F:010B 0000      ADD     [BX+SI],AL
073F:010D 48        DEC     AX
073F:010E 65        DB      65
073F:010F 6C        DB      6C
073F:0110 6C        DB      6C
073F:0111 6F        DB      6F
073F:0112 2400      AND     AL,00
073F:0114 0000      ADD     [BX+SI],AL
073F:0116 0000      ADD     [BX+SI],AL
073F:0118 0000      ADD     [BX+SI],AL
073F:011A 0000      ADD     [BX+SI],AL
073F:011C 3400      XOR     AL,00
073F:011E 2E        CS:
073F:011F 07        POP     ES

073F:011E 2E        CS:
073F:011F 07        POP     ES
-d 010D
073F:0100          48 65 6C          He1
073F:0110 6C 6F 24 00 00 00 00 00-00 00 00 00 34 00 2E 07  lo$......4...
073F:0120 00 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 00  .....
073F:0140 00 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 00  .....
073F:0160 00 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 00  .....
073F:0180 00 00 00 00 00 00 00 00-00 00 00 00 00          .....
-g =100
Hello
D:\>
```

四、机器码分析

汇编指令	机器码	说明
MOV AH,09	B409	调用 DOS 显示字符串功能
MOV DX,010D	BA0D01	设置字符串地址
INT 21	CD21	调用 DOS 中断
MOV AH,4C	B44C	程序终止功能号
INT 21	CD21	返回 DOS

字符串数据位于 010D 地址： 48 65 6C 6C 6F 24 = "Hello\$"

五、实验结论

成功使用 debug 工具手工输入汇编代码，程序正确输出"Hello"，验证了机器码与汇编指令的对应关系。