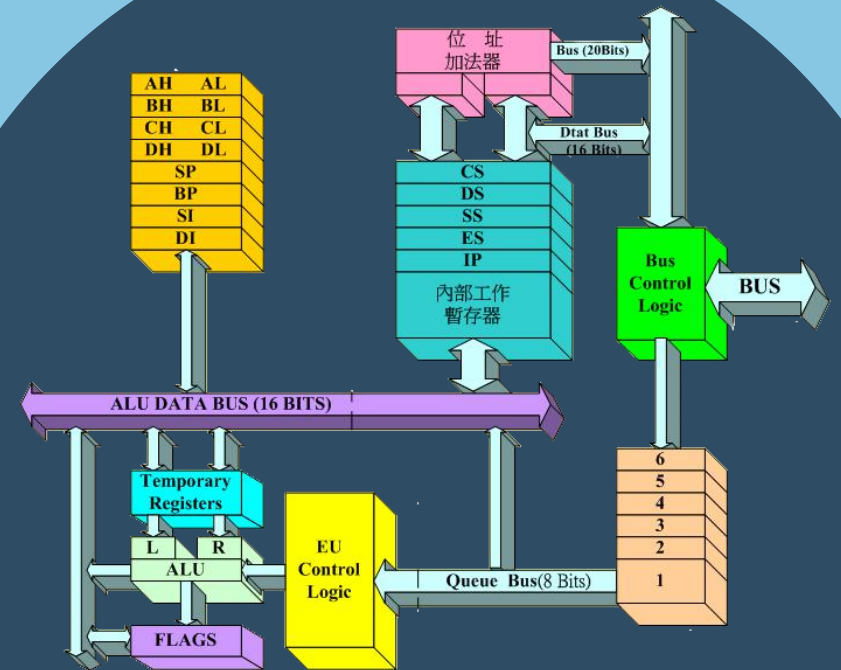


Debug的使用

贺利坚 主讲



汇编语言程序设计
Assembly Language

Debug是什么？

- Debug是DOS系统中的著名的调试程序，也可以运行在windows系统实模式下。
- 使用Debug程序，可以查看CPU各种寄存器中的内容、内存的情况，并且在机器指令级跟踪程序的运行！
- Debug就是传奇！



```
DOSBox 0.74, Cpu speed: 3000 cycles, Frameskip 0, Program: DEB... - [X]
073F:0112 01D8      ADD     AX,BX
-t
AX=8642 BX=4321  CX=0000 DX=0000  SP=00FD BP=0000 SI=0000 DI=0000
DS=073F ES=073F  SS=073F CS=073F  IP=0114  OV UP EI NG NZ NA PE NC
073F:0114 0000      ADD     [BX+SI],AL      DS:4321=00
-
^ Error
-q
C:\>debug
-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  NV UP EI PL NZ NA PO NC
073F:0100 B82301      MOV     AX,0123
-d
073F:0100  B8 23 01 BB 03 00 89 D8-01 D8 B8 21 43 BB FF FF  .#.....!C...
073F:0110  89 C3 01 D8 00 00 00 00-00 00 00 00 34 00 2E 07  .....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  .....
```

Debug能做什么？

- 🖥️ 用R命令查看、改变CPU寄存器的内容
- 🖥️ 用D命令查看内存中的内容
- 🖥️ 用E命令改变内存中的内容
- 🖥️ 用U命令将内存中的机器指令翻译成汇编指令
- 🖥️ 用A命令以汇编指令的格式在内存中写入机器指令
- 🖥️ 用T命令执行机器指令
- 🖥️



厉害了, Debug!


启动Debug



在DOS提示符下输入命令：debug

用R命令查看、改变CPU寄存器的内容

 R - 查看寄存器内容

 R 寄存器名 - 改变指定寄存器内容

用D命令查看内存中的内容



D - 列出预设地址内存处的
128个字节的内容




D 段地址:偏移地址 - 列出内
存中指定地址处的内容




D 段地址:偏移地址 结尾偏移
地址 - 列出内存中指定地址范
围内的内容

用E命令改变内存中的内容

 E 段地址:偏移地址 数据1 数据2 ...

 E 段地址:偏移地址

 逐个询问式修改

 空格 - 接受，继续

 回车 - 结束

用U命令将内存中的机器指令翻译成汇编指令

 有汇编指令

mov ax, 0123H

mov bx, 0003H

mov ax, bx

add ax, bx

 对应的机器码为

B8 23 01


BB 03 00

89 D8

01 D8

 e 地址 数据 - 写入

 d 地址 - 查看

 u 地址 - 查看代码

用A命令以汇编指令的格式在内存中写入机器指令

 有汇编指令

```
mov ax, 0123H
```

```
mov bx, 0003H
```

```
mov ax, bx
```

```
add ax, bx
```

 对应的机器码为


```
B8 23 01
```


```
BB 03 00
```

```
89 D8
```

```
01 D8
```

 a 地址 - 写入汇编指令

 d 地址 - 查看数据

 u 地址 - 查看代码

用T命令执行机器指令



t - 执行CS:IP处的指令

```
mov ax, 0123H
```

```
mov bx, 0003H
```

```
mov ax, bx
```

```
add ax, bx
```

用Q命令退出Debug

 q - 退出Debug

Debug是敲门砖，
尽快习练！

