DEBUG 各命令详细说明

启动 DEBUG

1.打开 Windows 命令窗口

在 Windows 95/98 的环境中 ,打开命令窗口的步骤为 :点击“开始”→“运行”，输入“command”命令； 在 WindowsXP 及 WIN7 的环境中，打开命令窗口的步骤为：点击“开始”→“运行” ，输入“cmd”命令；

2.启动 DEBUG

在命令窗口中启动 DEBUG，启动命令一般为：DEBUG [文件名] [参数表]。其中：文件名指定被调试的文件，其包括名和后缀，参数表是被调试文件运行时所需要的参数。被调试的文件可以是系统中的任何文件 ,但通常它们的 后缀为.EXE 或.COM。当 DEBUG 启动成功后 ,将显示连接符“-”,这时 ,可输入各种 DEBUG 命令。DEBUG 中所有命令及其含义如 DEBUG 各命令功能说明表 所示。 关于使用命令的几点说明：在提示符“-”下才能输入命令，在按“回车”键后，该命令才开始执行命令是单个字母 ,命令和参数的大小写可混合输入可用 F1、F2、F3、Ins、Del、左移键、右移键等编辑键来编辑本行命令当命令出现语法错误时，将在出错位置显示“^ Error”可用 Ctrl+C 或 Ctrl+Break 来终止当前命令的执行，还可用 Ctrl+S 或 Ctrl+Num Lock 来暂停屏幕显示(当连续不断地显示信息时)

以下通过实现十九个示例来熟悉 DEBUG 的命令集和基本的汇编指令。

R 命令的使用

R 命令作用：观看和修改寄存器的值。

在提示符“-”下输入以下命令：R。DEBUG 将会显示出当前所有寄存器和标志位的状态。

接下来再输入命令 RCX。在提示符“：”后输入 100。该命令的作用是将寄存器 CX 的值设置为 100（注意：DEBUG 使用的是十六进制，这里的 100 相当于十进制的 256。）

最后再执行 R 命令，观看修改后的寄存器值。

H 命令的使用

H 命令作用：计算两个十六进制数的和与差。

在提示符“–”下输入以下命令：H 10 1。观看命令执行结果。

运行结果的前一个数是计算出来的和，后一个数是计算出来的差。计算结果均用十六进制形式表示。

D 命令的使用

D 命令作用：显示内存区域的内容。

在提示符“–”下连续执行命令 R、D、D。观看命令执行结果。

前面已经介绍过了，命令 R 的作用是显示当前寄存器的值。而命令 D 的作用是显示内存区域的内容，最左边是内存的起始地址，中间以十六进制的形式显示内存值，最右边是以 ASCII 码的形式显示内存值。每行最多显示 16 个字节的内容。

命令 D 可以带参数也可省略参数。设 DEBUG 启动时 DS 的值为 X，当省略参数时，命令 D 显示内容以 X：100 为起始，每次显示 128 个字节的内容。以后再执行不带参数的命令 D 时，DEBUG 将按上次的位置接着显示下去。

带参数时 DEBUG 能够显示指定地址范围的内容。带参数的方式有三种：

方式一：d [起始位置]。DEBUG 从起始位置开始显示 128 个字节的内容。在提示符“-”下执行命令 D 1AF5:100。观看命令执行结果。

方式二：d [起始位置] [结束位置]。DEBUG 从起始位置开始一直显示到结束位置。在提示符“-”下执行命令 D DS:100 1FF。观看命令执行结果。

方式三：d [起始位置] [L 长度]，长度以 L 参数为标识。DEBUG 从起始位置开始显示指定长度的内容。在提示符“-”下执行命令 D DS:100 L10。观看命令执行结果。

E 命令的使用

E 命令作用：改变内存单位的内容。

E 命令的使用方式为：E [起始位置]。

在提示符“-”下输入以下命令：E 1AF5:100。

DEBUG 首先显示[1AF5:0000]的内容 00.，这时可以修改该字节的值。如果还要修改后续的内容，可以按空格键继续。当要跳过某个字节时，可以按连续的两个空格跳到后一个字节去。

F 命令的使用

F 命令作用：使用指定的值填充指定内存区域中的地址。

F 命令的使用方式为：F [范围] [填充列表]。

在提示符“-”下输入以下命令：F 1AF5:100 L20 1 2 3 4 5。执行命令

D 1AF5:100 观看命令执行结果。

说明：该命令是用字节序列 01、02、03、04、05 轮流填充从 1AF5:100 开始长度为 20H 的内存区域。

在提示符“-”下输入以下命令：F 1AF5:100 13F 41 42 43 44。

说明：该命令是用字节序列 41、42、43、44 轮流填充从 1AF5:100 开始一直到 1AF5:13F 的内存区域。

M 命令的使用

M 命令作用：将指定内存区域的数据复制到指定的地址去。

M 命令的使用方式为：M [范围] [指定地址]。

在提示符“-”下输入以下命令：M 1AF5:100 13F 1AF5:140。执行命令

D 1AF5:100 观看命令执行结果。

C 命令的使用

C 命令作用：将两块内存的内容进行比较。

C 命令的使用方式为：C [范围] [指定地址]，意思就是将指定范围的内存区域与从指定地址开始的相同长度的内存区域逐个字节进行比较，列出不同的内容。

在提示符“-”下输入以下命令：C 1AF5:100 13F 1AF5:140。由于两块内容完全相同，所以命令执行后没有任何显示。

在提示符“-”下输入以下命令：C 1AF5:100 107 1AF5:180，比较的区域长度为 8 个字节。命令执行后列出比较结果不同的各个字节。

S 命令的使用

S 命令作用：在指定的内存区域中搜索指定的串。

S 命令的使用方式为：S [范围] [指定串]。

在提示符“-”下输入以下命令：D 1AF5:100 11F。显示该区域的内存值。

在提示符“-”下输入以下命令：S 1AF5:100 11F 41 42 43 44。搜索该区域是否存在字节串 41 42 43 44，并将搜索结果一一列出。

从执行结果可以看出，总共搜索到八处。

A 命令的使用

A 命令作用：输入汇编指令。

以下的程序要在屏幕上显示“ABCD”四个字符。

首先用 E 命令将“ABCD$”四个字符预先放在内存 CS:200 处，然后执行 A100 命令输入汇编程序代码：

```
MOV AX,CS

MOV DS,AX

MOV DX,200

MOV AH,9
```

INT 21

INT 20

（说明：前两行汇编指令用于将段寄存器 CS 的值赋给段寄存器 DS。第三到第五行汇编代码的作用是显示以“$”为结尾的字符串。最后一行用于结束程序。

G 命令的使用

G 命令作用：执行汇编指令。

G 命令的使用方法是：G [=起始地址] [断点地址]，意思是从起始地址开始执行到断点地址。如果不设置断点，则程序一直运行到中止指令才停止。
在设置完示例九的的内存数据并且输入完示例九的程序后运行这些汇编代码。在 DEBUG 中执行命令 G=100，观看运行结果。

汇编程序运行后在屏幕上显示出“ABCD”四个字符。

接下来在 DEBUG 中执行 G=100 10B，意思是从地址 CS：100 开始，一直运行到 CS：10B 停止。观看运行结果。

命令执行后，不但显示出字符串“ABCD”，而且列出当前寄存器和标志位的值。

U 命令的使用

U 命令作用：对机器代码反汇编显示。

U 命令的使用方法是：U [范围]。如果范围参数只输入了起始地址，则只对 20H 个字节的机器代码反汇编。执行命令 U100，观看反汇编结果。

执行命令 U100 10B，观看反汇编结果。该命令的作用是对从 100 到 10B 的机器代码进行反汇编。

N 命令的使用

N 命令作用：设置文件名，为将刚才编写的汇编程序存盘做准备。

以下的 DEBUG 命令序列作用将刚才的汇编程序存为磁盘的 COM 可执行程序。

D200 20F

U100 10C

N E:\FIRST.COM

RCX

:110

W

第一和第二条命令的作用是检查一下刚才编写的汇编指令。第三条命令的作用是设置存盘文件名为 E:\FIRST.COM，第四条命令的作用是设置存盘文件大小为 110H 个字节。最后一条命令是将文件存盘。

文件存盘后执行 E:\FIRST.COM，观看存盘的可执行文件的运行效果。

W 命令的使用

W 命令作用：将文件或者特定扇区写入磁盘。

在示例“N 命令的使用”中已经实验了如何使用 W 命令将文件存盘。

在没有很好地掌握汇编语言和磁盘文件系统前，暂时不要使用 W 命令写磁盘扇区，否则很容易损坏磁盘文件，甚至破坏整个磁盘的文件系统。

L 命令的使用

L 命令作用：从磁盘中将文件或扇区内容读入内存。

将文件调入内存必须先用 DEBUG 的 N 命令设定文件名。以下例子是将 E:\FIRST.COM 读入内容。

N FIRST.COM

L

观看调入程序的汇编代码可以使用 DEBUG 的 U 命令，用 U100 观看调入的 COM 文件。

读取磁盘扇区的方式是：L [内存地址] [磁盘驱动器号] [起始扇区] [扇区数]。“内存地址”指定要在其中加载文件或扇区内容的内存位置，如果不指定“内存地址”的话，DEBUG 将使用 CS 寄存器中的当前地址。“磁盘驱动器号”指定包含读取指定扇区的磁盘的驱动器，该值是数值型：0=A，1=B，2=C 等。“起始扇区”指定要加载其内容的第一个扇区的十六进制数。“扇区数”指定要加载其内容的连续扇区的十六进制数。

只有要加载特定扇区的内容而不是加载文件时，才能使用[磁盘驱动器号] [起始扇区] [扇区数]参数。

例如：要将 C 盘第一扇区读取到内存 DS:300 的位置，相应的 DEBUG 命令为 L DS:300 2 1 1。但是由于 Windows 操作系统对文件系统的保护，这条命令可能会被操作系统禁止运行。

T 命令的使用

T 命令作用：执行汇编程序，单步跟踪。

T 命令的使用方式是 T [=地址] [指令数]。如果忽略“地址”的话，T 命令从 CS:IP 处开始运行。“指令数”是要单步执行的指令的数量。

以下示例对 E:\FIRST.COM 进行单步跟踪。

N E:\FIRST.COM

L

U100 10B

R

T=100

T

第一、二条命令是装入文件，第三条命令是列出程序反汇编代码，第四条命令是显示当前寄存器值，第五条命令是从 CS:100 处开始单步跟踪，第六条命令是继续跟踪后续的指令。

P 命令的使用

P 命令作用：执行汇编程序，单步跟踪。与 T 命令不同的是：P 命令不会跟踪进入子程序或软中断。

P 命令的使用方式与 T 命令的使用方式完全相同。

I 命令的使用

I 命令作用：从计算机输入端口读取数据并显示。

I 命令的用法是 I [端口地址]。例如从 3F8 号端口读取数据并显示的命令为 I 3F8。这里不对该命令做解释。

O 命令的使用

O 命令作用：向计算机输出端口送出数据。

O 命令的用法是 O [端口地址] [字节值]。例如向 278 号端口发出数据 20H 的命令为：I 278 20。这里不对该命令做解释。

Q 命令的使用

Q 命令的作用是退出 DEBUG，回到 DOS 状态。