《 DEBUG 使用方法 》

DEBUG 是专门为汇编语言设计的一种调试工具软件，可用来检查、修改寄存器和内存单元的内容，装入运行程序，汇编及反汇编机器语言程序，可用单步、断点及连续的方式执行程序。

DEBUG 启动方式:

>DEBUG 文件名.EXE(Enter) ; 回车进入DEBUG状态

- ; "-" 是 DEBUG 提示符

以下是 DEBUG 的基本操作命令

一. A (汇编) 命令

用途: 把计算机的宏汇编语句直接汇编到内存中。

格试: A [address]

说明: A 是一条逐行汇编命令，当使用 A 命令时，并不直接将 16 进制字节，机器码

而键入是助记符，但键入的汇编语言被汇编在指定地址的连续单元中。

在A命令后没指出地址，分两种情况。

没指定地址同时前面没有使用汇编命令，则语句被汇编到 CS:100 开始的区域中

没指定地点，但前面已有汇编命令，则语句被汇编到紧接着前一条汇编语句的后一个地址单元里。

例:-A

1298:0200 PUSH DS

1298:0201 MOV AX,0000

1298:0204 PUSH AX

1298:0205 MOV AX,128F

1298:0208 MOV DS,AX

1298:020A MOV AX,F000

1298:020D MOV ES,AX

1298:020F MOV SI,FFFE

1298:0212 ES:

1298:0213 MOV AL,[SI]

1298:0215 CMP AL,FC

1298:0217 JNZ 0223

1298:0219 LEA DX,[006B]

1298:021D CALL 024B

二. C(比较)命令

用途: 比较两个内存的内容。

格式: C range address

说明: 比较两个内存的内容，比较长度由 range 决定，若发现不等的字节，按下列格式显示它们的内容。

例:-D 100

33E2:0100 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

33E2:0110 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

-D 200

33E2:0200 74 68 65 20 6B 69 6E 64-20 6F 66 20 6D 69 63 72

33E2:0210 6F 20 63 6F 6D 70 6E 74-65 72 20 69 73 20 41 54

-C 0100 L08 0200 ;比较100H和200H开始的八个字符。

33E2:0100 00 74 33E2:0200 ;显示不同的字符。

33E2:0101 00 68 33E2:0201

33E2:0102 00 65 33E2:0202

33E2:0103 00 20 33E2:0203

33E2:0104 00 6B 33E2:0204

33E2:0105 00 69 33E2:0205

33E2:0106 00 6E 33E2:0206

33E2:0107 00 64 33E2:0207

三. D(显示)命令

用途: 显示部分存储区的内容。

格式: D [range]或 D [address]

说明: 显示指定内存单元的内容。

⑴ 在输入的起始地址中，只键入一个相对偏移量，段地址为 DS 中。

例:-D

1298:0200 1E B8 00 00 50 B8 8F 12-8E D8 B8 00 F0 8E C0 BE

1298:0210 FE FF 26 8A 04 3C FC 75-0A 8D 16 6B 00 E8 2B 00

1298:0220 EB 28 90 3C FD 75 0A 8D-16 46 00 E8 1D 00 EB 1A

⑵ 若要显示指定范围的内容，则要输入显示的圃橡始和结束地址。

例:-D 0200 027F

125F:0200 00 42 34 00 00 00 00 00-00 00 00 00 00 00 00 00

125F:0210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

125F:0270 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

⑶ 如果没有指定地址，则从上一次的 D 命令最后一个单元开始显示。

四. E(修改)命令

用途: 修改RAM区单元的内容。

格式: E address[List]

说明: 该命令可以在指定的地址里修改一个或多个字节的内容，同时也可连续的修改每个字节的内容。

⑴ 连续修改每个字节的内容。

例:-E 0200

125F:0200 00.12 00.13 00.14 00.15 00.16

⑵ 用给定的内容去代替指定范围的内存单元内容。

例:-E 0200 'the kind of micro compnter is AT'

-D 200

33E2:0200 74 68 65 20 6B 69 6E 64-20 6F 66 20 6D 69 63 72 the kind of micr

33E2:0210 6F 20 63 6F 6D 70 6E 74-65 72 20 69 73 20 41 54 o compnter is AT

⑶ 输入一个连接号"-"，则显示前一个地址单元的内容。

例:-E 0200

125F:0200 12.- ;200单元不修改，键入"-"。

125F:01FF 13.AC- ;AC代替13。

-D 01FE 0200

125F:01FF AC 12

五. F(填充)命令

用途: 把表中的值，填到内存单元中。

格式: F range List

说明: 如果 List 所含的字节数比 range 小，则 List 被重复使用，

如 List 所含的字节数比 range 大，则 List 多余被略去。

例:-D 0200 0210

33E2:0200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

33E2:0210 00

-F 0200 L0a'abcdefghij'

-D 0200 0210

33E2:0200 61 62 63 64 65 66 67 68-69 6A 00 00 00 00 00 00 abcdefghij

33E2:0210 00

六. G(执行)命令

用途: 执行需运行的程序，并对调试的程序进行断点测试跟踪。

格式: G[=address][address[address..]

说明: 程序从当前指令开始执行，执行的地址由 CS 和 IP 的内容决定。如用"=address"

参数取代，则程序从 CS:"=address" 开始执行。

-G ;从IP=0200开始执行，结果显示在屏幕上。

the kind of micro compnter is AT

Program terminated normally

-G 0252 ;程序从0200H单元开始执行,在0252H处设置一个断点。

AX=0000 BX=0000 CX=04E2 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000

DS= 125F ES=125F SS=126F CS=1298 IP=0200 NV UP EI PL NZ NA PO NC

1298:0252 CB RETF

-

* 注意:一旦程序运行结束(DEBUG 显示"program terminated normally"信息)，

⑴ 再次执行，必须重新启动程序。

⑵ 地址参数指向的位置必须含有合法的 8086/8088 指令码。

⑶ 堆栈指标器必须是合法的。

⑷ 对断点只键入一个偏移量，G 命令设该断在CS寄存器中。

七. H(16进制运算)命令

用途: 对两个十六进制数进行加、减，然后显示出和与差。

格式: H Value Value

例:- H A B

0015 FFFF ;和为15H ， 差为 FFFFH

-H 12 30

0042 FFE2 ;和为42H ， 差为 FFE2H

八. M(传送)命令

用途: 把由 range 规定的内存单元区域的内容传送到 address 开始的单元。

格式: M range address

说明: 传送期间总是执行复盖传送，源区域的数据保持不变。

-Dcs:0000 000f

1298:0000 1E B8 00 00 50 B8 8F 12-8E D8 B8 00 F0 8E C0 BE

-Dds:0000 0010

125F:0000 CD 20 00 A0 00 9A F0 FE-1D F0 F4 02 94 0E 2F 03

-Mcs:0000 l10 ds:0000

-Dds:0000 000f

125F:0000 1E B8 00 00 50 B8 8F 12-8E D8 B8 00 F0 8E C0 BE

-q

九. N(命名)命令

用途: 给文件定名，用于文件存盘或装入内存区。

格式: N filespec[filespec...]

-N A.COM ;给文件命名为A，扩展名为COM。

-L ;把A.COM文件装入内存。

-U ;用反汇编检查装入内存的程序正确否。

1298:0200 1E PUSH DS

1298:0201 B80000 MOV AX,0000

1298:0204 50 PUSH AX

1298:0205 B88F12 MOV AX,128F

1298:0208 8ED8 MOV DS,AX

1298:020A B800F0 MOV AX,F000

1298:020D 8EC0 MOV ES,AX

1298:020F BEFEFF MOV SI,FFFE

1298:0212 26 ES:

1298:0213 8A04 MOV AL,[SI]

1298:0215 3CFC CMP AL,FC

1298:0217 750A JNZ 0223

1298:0219 8D166B00 LEA DX,[006B]

1298:021D E82B00 CALL 024B

十. Q(退出)命令

用途: 退出 DEBUG状态。

格式: Q

说明: Q命令不保留正在内存中运行的文件，若保留需用 "W" 命令， DEBUG返回

到命令处理程序，然后显示出正常的命令提示。

-Q

> ;回到DOS下

十一. R(寄存器)命令

用途:显示和修改各寄存器的内容。

格式:R[Register name]

说明:当 R 命令后面不带任何参数时，显示出 13 个 16 位寄存器的内容，同时又显示

出标志寄存器各位状态，最后显示出下一条要执行的指令内容。

当R命令后面带参数时，显示出该寄存器的内容，同时又可进行修改。

例:-R

AX=0000 BX=0000 CX=04E2 DX=0000 SP=0200 BP=0000 SI=0000 DI=0000

DS=125F ES=125F SS=126F CS=1298 IP=0200 NV UP EI PL NZ NA PO NC

1298:0200 1E PUSH DS

-R AX ;显示AX寄存器的内容。

AX 0000

:0200 ;用0200取代0000,AX的当前值。

-RAX

-AX 0200

:

-R F

NV UP EI PL NZ NA PO NC - OV EI ZR ;修改NVEI，NZ标志位。

标志寄存器共有九个标志位，其中追踪标志 T 不能改变，其它八个标志位可以显示和修改，并且以二个字母的带码来分别表示各位状态。

十二. S(检索)命令

用途: 在指定的 Range 范围内找到 List 规定的字符。

格式: S range List

说明: 显示出符合规定字符处的地址，如显示提示符 "-"，则表示没有发现规定字符。

-D 0200 0220

33E2:0200 61 62 63 64 65 66 67 68-69 6A 00 00 00 00 00 00

33E2:0210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

33E2:0220 00

-S 02 0220 60 ;在0200H单元，到0220H单元内,查询60H字符。

- ;没有检索到，出现"-"。

-D 0200 0220

125F:0200 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

125F:0210 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00

125F:0220 00

-S 0200 0205 00 ;查询为00H的字符。

125F:0200

125F:0201

125F:0202

125F:0203

125F:0204

125F:0205 ;显示出查询到为00H的字符。

十三. T(跟踪)命令

用途: 执行以 CS:IP 中指定开始的一个或几个指令，并显示出执行每条指令后所有寄存器的内容。

格式: T[=address][Value]

说明: T 命令可以单条跟踪执行每一条指令，也可以由命令中Value决定执行几条指令，每执行一条指令，IP 就自动指向下一条指令的地址。为了改变程序的起始地址，可以修改 IP 的内容，使程序不按正常顺序执行。

-T

AX=0000 BX=0000 CX=04E2 DX=0000 SP=01FE BP=0000 SI=0000 DI=0000

DS=125F ES=125F SS=126F CS=1298 IP=0201 NV UP EI PL NZ NA PO NC

1298:0201 B80000 MOV AX,0000

-T 2 ;连续执行两条指令。

AX=0000 BX=0000 CX=04E2 DX=0000 SP=01FE BP=0000 SI=0000 DI=0000

DS=125F ES=125F SS=126F CS=1298 IP=0201 NV UP EI PL NZ NA PO NC

1298:0201 B80000 MOV AX,0000

AX=0000 BX=0000 CX=04E2 DX=0000 SP=01FE BP=0000 SI=0000 DI=0000

DS=125F ES=125F SS=126F CS=1298 IP=0204 NV UP EI PL NZ NA PO NC

1298:0204 50 PUSH AX

十四. U(反汇编)命令

用途: 将内存某一区的计器码(目标码)，用此命令反汇编为源程序。

格式: U [address]、(U range)

说明: U [address]命令从反汇编规定地址的指令开始，如未规定地址，

则以上一个 U 命令的最后一条指令的地址为下一条反汇编的起始地址，这样就可以进行连续的反汇编。

例:-U

1298:0200 1E PUSH DS

1298:0201 B80000 MOV AX,0000

1298:0204 50 PUSH AX

1298:0205 B88F12 MOV AX,128F

1298:0208 8ED8 MOV DS,AX

1298:020A B800F0 MOV AX,F000

1298:020D 8EC0 MOV ES,AX

1298:020F BEFEFF MOV SI,FFFE

1298:0212 26 ES:

1298:0213 8A04 MOV AL,[SI]

1298:0215 3CFC CMP AL,FC

1298:0217 750A JNZ 0223

1298:0219 8D166B00 LEA DX,[006B]

1298:021D E82B00 CALL 024B

十五. W(写)命令

用途: 把正在调试的文件写入磁盘。

格式: W [address]

说明: 此命令把指令内存区域中的数据写入文件,一般用 N 命令来命名文件名, BX:CX 置入文件长度.

-A

1298:0100 PUSH DS

1298:0101 MOV AX,0000

1298:0104 PUSH AX

1298:0105 MOV AX,128F

1298:0108 MOV DS,AX

1298:010A MOV AX,F000

1298:010D MOV ES,AX

1298:010F MOV SI,FFFE

1298:0112

-RBX

BX 0000

:0000

-RCX

CX 0000

:0012 ;文件长度送 BX:CX

-N A.COM ;文件名为 A.COM

-W ;存入磁盘

Writing 0000F bytes

-q

十六. O(输入)命令

用途: 向指定的端口输出一个字节。

格式: O prot address byte

例: -O 300 23 ;从 300H 端口输出 23H

十七. L(装入)命令

用途: 把磁盘上的内容装入内存。

格式: L [address]

例: -N A.COM

-L ;把A.COM文件从磁盘装入内存。

-U

1298:0200 1E PUSH DS

1298:0201 B80000 MOV AX,0000

1298:0204 50 PUSH AX

1298:0205 B88F12 MOV AX,128F

十八. I(输入)命令

用途: 从指定的端口显示出输入数据。

格式: I port address

例: -I 300

FF ;从 300H 端口读入 FFH