第三章
檢查記憶體和執行程式

DEBUG 的各種命令

協助組合語言程式的偵錯

MSDOS提供的
- DEBUG

較好的環境
- CODEVIEW
- TurboDebugger

DEBUG 命令 (1)

A: Assemble, 組譯 (使用者用組合語言寫程式, 翻譯成機器碼存到記憶體中)

D: Display (Dump) Memory, 顯示記憶體內容

E: Edit, 編輯(修改)記憶體內容

G: Go, 跑程式

H: Hexadecimal arithmetic, 十六進制計算 (顯示兩數的和和差)

DEBUG 命令 (2)

N: Name, 指定檔案名稱 (以後將讀或寫)

P: Proceed, 前進 n 個指令

Q: Quit, 結束, 回到DOS

R: Register, 顯示和修改暫存器內容

T: Trace, 追蹤(單步執行) n 個指令

U: Unassemble, 反組譯 (把記憶體內容轉成組合語言, 顯示出來)

其它 DEBUG 命令(附錄C)

C: Compare, 比較兩塊記憶體的內容
F:, Fill, 填滿, 將一塊記憶體填滿指定資料
I: Input, 輸入
L: Load, 載入檔案
M: Move, 移動記憶體內容
O: Output, 輸出
W: Write, 寫出到檔案

下命令的規則

1. 英文字母不分大小寫
2. 數字是十六進制
3. 空格 (逗號) 用以分開參數 (不計個數)
4. 分號 (:) 用以分開分段號碼和位移

例子: D命令

D DS:200
DDS:200
dds:200
d200
d,200

檢查記憶體內容

BIOS資料區由絕對地址400H(40:0, 0:400, 400:0, ...)起

400-407存放四個COM port地址, 每個地址16位元 (兩個位元組)。通常有COM1(3F8H), COM2 (2F8H)

408-40F存放四個 printer port地址。通常有LPT1(378H)

檢查安裝的裝置

狀況存放在410H和411H兩位置 (16位元)
各位元代表意義:
位元15,14: 平行列表機個數
11-9: 串列埠個數
7,6: 軟碟機個數
5,4: 啟始影像模式
1: 有算術運算器
0: 有軟碟機

檢查記憶體容量

狀況存放在413H和414H兩位置 (16位元)
單位是K Bytes

檢查序號和版權申告

由FE00[0]起, 7位數序號; 接著是版權申告

檢查ROM BIOS 日期

由FFFF[5]起

檢查Model ID

FFFF[E]一個位元組, 指示機型

第一個程式例子

立即資料

機器碼	組合語言	
B82301	MOV	AX,0123
052500	ADD	AX,0025
8BD8	MOV	BX,AX
03D8	ADD	BX,AX
8BCB	MOV	CX,BX
2BCB	SUB	CX,AX
2BC0	SUB	AX,AX
90	NOP	

各種命令的使用

輸入機器碼: E命令, 兩種格式

顯示所有暫存器內容: R<enter>命令

修改暫存器內容: R<暫存器名稱><enter>命令

一步一步執行程式: T命令, P命令

顯示記憶體內容: D命令

修改記憶體內容: E命令

執行程式: G命令

格式

G<=start address> <break point 1> <bp2> …

由start address開始執行

若未指定start address, 則由當時IP所指位置(上次執行停止位置)開始

遇到斷點, 即停止執行, 斷點處那指令未執行(IP指到斷點位置, 下次G命令可繼續)

第二個程式例子

直接地址

機器碼	組合語言	
A10002	MOV	AX,[0200]
03060202	ADD	AX,[0202]
A30402	MOV	[204],AX
90	NOP	

資料區

位移	內容
200	2301
202	2500
204	0000
206	2A2A2A

組譯和反組譯

A 100
U 100
U 100,106

系統呼叫: INT 21H指令

取日期: Subfunction 2AH

```
MOV AH,2A
INT  21
NOP
```

AL: 星期
CX: 年
DH: 月
DL: 日

取時間: Subfunction 2CH

```
MOV AH,2C
INT  21
NOP
```

CH: 小時

CL: 分鐘

DH: 秒

DL: 1/100秒

顯示一段文字: Subfunction 9

文字放在資料段 (DS所指分段), 以錢號($)結束

DX指到開頭位置

```
100   MOV     AH,9
102   MOV     DX,108
105   INT     21
107   NOP
108   DB      'YOUR NAME'.'$'
```

鍵盤輸入的BIOS呼叫:
INT 16H Subfunction 10H

```
100  MOV    AH,10
102  INT    16
104  JMP    100
106  NOP
```

貯存程式: W命令

以N命令指定檔案名稱(.com檔)
BX:CX放資料長度(多少位元組)
以W命令貯存程式到檔案

PTR 運算(Operator)

```
100     MOV   AX,[11A]
103     ADD   AX,[11C]
107     ADD   AX,25
10A     MOV   [11E],AX
10D     MOV   WORD PTR [120],25
113     MOV   BYTE PTR [122],30
118     NOP
119     NOP
11A     DB    14 23
11C     DB    05 00
11E     DB    00 00
120     DB    00 00 00
```