

CHÖÔNG TRÌNH GỒ ROÁI DEBUG

Muïc tiêu

- Dòch ñöôïc 1 chöông trình ngaén
- Xem caùc thanh ghi vaø côø cuûa CPU
- Xem söï thay ñoái noãi dung cuûa caùc bieán
- Døø tìm trò ôû daïng nhò phaân hoaëc ASCII trong boä nhòu

■ Hoã trôi luyeän taáp vieát chöông trình baèng Assembly

Daing leanh cuua Debug

■ <mao leanh > <thoang soa >

Trong noo mao leanh laø 1 trong cauc choo A,B,C,D,E, ... coøn thoang soa thi thay noai tuy theo leanh.

Cauc thoang soa cou thea laø :

Noo chæ : laø 1 boä noo chæ naay nuu segment : offset hay chæ caàn offset laø nuu. Segment cou thea duøng teän thanh ghi.

Ex : **F000:0100**

DS: 200

0AF5

Đãing leãnh cuũa Debug

Taäp tin : laø 1 tham khaũu teãn taäp tin ñaày ñuũ, ít nhaát phaũi coũ teãn taäp tin.

Danh saũch :

Laø 1 hay nhieàu trò byte hoaëc chuoải caũch nhau baèng daáu phaỹ.

Khoaũng : laø 1 tham khaũu ñeãn vuøng boã nhũu

Trò : laø 1 soá heä 16 coũ toái ña coũ 4 chũũ soá

Taäp leänh cuûa Debug

- A <Assemble> :
cho pheùp vieát töø baøn phím caùc
leänh maõ maùy döôùi daïng göi
nhôù.
- A [<ñòa chæ>]
Ex : - A 100 dòch ôu ñòa chæ
CS:100h
- A dòch ôu ñòa chæ
hieän taïi

Thí dụ minh họa lệnh A

- Phải nhập lệnh vào theo tổng dòng một và kết thúc bằng Enter.
- Kết thúc nhập nhấn Enter ô dòng trống.

User gõ vào

Ex : - A 100

5514:0100 MOV AH, 2

5514:0102 MOV DL, 41

INT 21H

SEGMENT

OFFSET

C (Compare)

- So sánh 2 vùng bộ nhớ và liệt kê các ô nhớ có nội dung khác nhau.

Cuộc chạy : C <khoảng> , <địa chỉ>

Ex : - C 100, 200, 3000 : 1000

So sánh ô nhớ DS:100h với ô nhớ 3000:1000h, ô nhớ DS:101h với ô nhớ 3000:1001h.... Cho đến ô nhớ DS :200h với ô nhớ 3000:1100h.

→ So sánh 101 bytes

D (Dump)

- Hiện nội dung boả nhòu theo dạng hệ 16 vàø ASCII.

Càùch gọi : **D** <khoàùng>

Ex : - D F000 : 0

- D ES : 100

- D 100

Leänh F (Fill)

- Cù phàup : F <khoaúng> <danh saùch>
- Coäng düng : laáp ñàày trò vaøo vuøng nhôu ngay tại ñòa chæ mong mu

Trò nhaáp vaøo töøng byte moät theo heä 16

Daáu tröø (-) duøng ñeå lui lai 1 ñòa chæ.

SPACE BAR duøng ñeå tôùi 1 ñòa chæ.

ENTER ñeå keát thuùc.

Minh hoĩa leãnh F

- Laép ñaày vuøng nhòu taïi ñòa chæ offset 100h chuoải “ Toi dua em sang song”.

F 100 “TOI DUA EM SANG SONG”

OFFSET 100H

KEÁT QUAÛ

-F 100 "TOI DUA EM SANG SONG"

-D 100

0ADD:0100	54 4F 49 20 44 55 41 20-45 4D 20 53 41 4E 47 20	TOI DUA EM SANG
0ADD:0110	53 4F 4E 47 54 4F 49 20-44 55 41 20 45 4D 20 53	SONGTOI DUA EM S
0ADD:0120	41 4E 47 20 53 4F 4E 47-54 4F 49 20 44 55 41 20	ANG SONGTOI DUA
0ADD:0130	45 4D 20 53 41 4E 47 20-53 4F 4E 47 54 4F 49 20	EM SANG SONGTOI
0ADD:0140	44 55 41 20 45 4D 20 53-41 4E 47 20 53 4F 4E 47	DUA EM SANG SONG
0ADD:0150	54 4F 49 20 44 55 41 20-45 4D 20 53 41 4E 47 20	TOI DUA EM SANG
0ADD:0160	53 4F 4E 47 54 4F 49 20-44 55 41 20 45 4D 20 53	SONGTOI DUA EM S
0ADD:0170	41 4E 47 20 53 4F 4E 47-54 4F 49 20 44 55 41 20	ANG SONGTOI DUA

D (DUMP)

Muïc ñích : in noäi dung boã nhôu trong MT ra maøn hình döôùi daïng soá hex.

Cuù phaùp : D [address]

D [range]

Ex : in noäi dung vuøng nhôu ñaõ laép ñaày ôu ví duï tröôùc ôu ñòa chæ 100h

Ex2 : xem noäi dung vuøng nhôu 16 bytes baét ñaàu ôu ñòa chæ F000:100

- D F000:100 L10

Thí dụ minh họa lệnh D

- Nhập vào lệnh D để xem nội dung vùng nhớ của 30h bytes bắt đầu từ địa chỉ 0000:0040 đến 0000:006F

- D 0000:0040 006F

Địa chỉ bắt đầu

- D 0000:0040 L 30

Số bytes

E (ENTER)

- Dùng để đưa dữ liệu byte vào bộ nhớ ngay tại địa chỉ mong muốn.
Cách gọi:

- E <địa chỉ> <danh sách>

Trò nhập vào theo dạng số 16 tổng byte một
Đấu - dùng để lùi lại 1 địa chỉ
Space Bar dùng để lùi 1 địa chỉ
Enter dùng để kết thúc

Minh hoĩa leãnh E

■ Mục đích : thay ñoãi noãi dung boã

nhôù.
Cuu pháp : - E [address] [list]

Ex : thay ñoãi 6 bytes baét ñààu ôu ñòà chæ 100 thaønh “ABCDE”

- E 100 “ABCDE”

Debug laáy ñoain chæ bôui
DS

Neáu ta khoâng qui ñòn
ñòà chæ ñoain

Leänh U (Unassemble)

- công dụng : in ra 32 bytes mã mãy của chương trình trong bộ nhớ ra màn hình döúi leänh göi nhöu.
- cú pháp : U [address]

Ex : U 100 119

In ra màn hình các leänh mã mãy töø ñòa chæ CS:100 ñeán CS:119

Leänh R (Register)

- Công dụng : xem vaø söûa noãi dung thanh ghi.
- Cuù phaùp : - R enter (xem táát câu thanh ghi)

xem thanh ghi AX : - R AX

xem thanh ghi côø : R F

Ex : muoán baät thanh ghi côø CF vaø ZF ta
nhaäp CY vaø ZR.

Leänh N (Name)

- Công dụng : tạo tập tin cần nhớ hay ghi trước khi dùng leänh L hay W.
- Cùu phaùp : - N <teän file> [thoäng soá] L [ñòà chæ]

Thí dụ minh họa lệnh N

Ex : tạo tập tin Love.txt .

- Dùng lệnh R để xác định vùng nhớ dành cho User.
- Dùng lệnh để đưa câu thông báo “ I love you more than I can say’ ô nhớ 2000:100.
- Dùng lệnh D để kiểm tra vùng nhớ tại nhớ 2000:100.
- Dùng lệnh N để đặt tên tập tin trên đó.
- N Love.txt
- Dùng lệnh R để định số byte cần thiết ghi lên đó trong 2 thanh ghi BX và CX. Cui thế trong trường hợp này số byte cần ghi là 1Eh byte.
BX = 0000 CX = 1E
- Dùng lệnh W 2000:100 để ghi dữ liệu đã nhập vào tập tin ô nhớ 2000:100.

- Thoát khỏi Debug và gọi lại tệp tin theo cách sau :
C :\> Debug Love.txt
tìm xem Debug nào nạp tệp tin Love.txt vào chỗ nào trong bộ nhớ.

Leänh W (Write)

■ Cuù phaùp : W [address]

Thööøng ñööïc söü düing chung vöüi leänh N

Ex : taïo taäp tin cöü tên Love.txt

Bööüc 1 : düøng leänh E ñeä ñöa câu 'I love you more than I can say'
væo oä nhöü öü ñöa chæ 100.

Bööüc 2 : düøng leänh D ñeä kieäm tra laiï ñöa chæ 100

Bööüc 3 : düøng leänh N ñeä ñæät tên taäp tin : - N Love.txt

Bööüc 4 : düøng leänh R ñeä ñönh soá byte càn ghi lên ñöa trong 2
thanh ghi BX væo CX. (BX chöüa 16 bit cao, CX chöüa 16 bit thaáp).

Öü ñây soá byte càn ghi læø 1Eh.

Bööüc 5 : düøng leänh W ñeä ghi câu trên ñäü nhaäp væo vöøng nhöü
cöü ñöa chæ baét ñäü læø 100.

Leãnh T (Trace) vaø P

- cuù phaùp : - T [= <ñiaï chæ>][soá laàn]
Mục đích : duøng ñeå chaïy 1 hay nhiều laàn cuùc leãnh trong boã nhòu

Ex : - T = 3000:1000

Ex : - T = 3000:1000 <soá laàn>

Leänh L (Load)

- naip taäp tin hoaëc naip sector luaän lyù töø ñóa vaøo boä nhôu.

Cuù phaùp : - L <ñòa chæ> [<ñóa> <sector><soá>]

Daing 1 : neáu chæcoù ñòa chæduøng ñeä naip taäp tin. Teän taäp tin phaui ñöôic gaùn tröôuc baèng leänh N.

Taäp tin luaän luaän ñöôic gaùn ôu ñòa chæoffset 100h

Daing 2 : neáu coù ñàày ñuû caùc thoäng soá , duøng ñeä ñöic sector luaän lyù treän ñóa vaøo boä nhôu.

Ñóa : = 0 oã ñóa A, =1 oã ñóa B, =2 oã ñóa C

Leänh H (Hex Arithmetic)

- thöic hieän pheùp coäng vaø tröø

heä 16
Cúu phäùp : - H <trò 1> <trò 2>

Keát quaû : hieän ra toäng vaø hieäu cuûa trò 1 vaø trò 2

Leãnh S (Search)

- Công dụng : tìm kiếm trò trong 1 vùng bộ nhớ.
- Cú pháp : - S <khoảng> <danh sách>
- Giới thích : tìm kiếm trò cụ thể hiển thị trong vùng bộ nhớ nào đó hay không? Nếu cụ thể Debug hiển thị các địa chỉ nào của những nội dung cụ thể danh sách.

Ex : - S 100 L 1000 'DOS'

18AF : 0154

18AF : 0823

Leänh M (Move)

- Công dụng : cheùp noäi dung vuøng nhòu ñeán 1 ñòa chæ khaùc.
- Cuù phaùp : - M <khoaúng>
- Ex : - M 100 105 200

Cheùp 5 bytes töø DS:100 ñeán DS:200

Ex2 : - M CS:100 L 50 ES:300

Cheùp 50 bytes töø CS:100 ñeán ES:300

Leänh I (Input)

- Công dụng : nhập 1 byte töø công xuất nhập vào hiän ra màn hình.
- Cùu phaùp : - I <ñòà chæ công>
ñòà chæ công laø soá heä 16 toái
ña 4 chöõ soá.
- Ex : - I 37E
EC

Leänh O (Output)

- Công dụng : xuaát 1 byte ra công xuaát nhaäp.
- Cùu phaùp :- O<ñòà chæ công> <trò>
ñòà chæ công laø soá heä 16 toái ñà 4 chöõ soá.
- Ex : - O 378 5E

Summary

- Dùng lệnh D để xem nội dung vùng nhớ tại địa chỉ của ROM BIOS F000:0000.
- Dùng để xem nội dung vùng nhớ RAM mẫu hình ô địa chỉ B800:0000; bảng vector ngắt qua cổng 0000:0000
- Gõ vào máy bằng lệnh A, soạn chương trình sau ô địa chỉ 2000:0100

Summary

```
2000:0100  MOV AL,32
2000:0102  MOV AH, 4F
2000:0104  MOV CX, [200]
2000:0108  MOV WORD PTR [1800], 1
2000:010E  MOV BYTE PTR [1800], 1
2000:0113
```

Xem lại nội dung chương trình vừa hiển thị trên bảng lệnh U. Chú ý quan sát phần mã máy. Tìm xem các toán hạng tức thời và các nhà chập xuất hiện ở đâu trong phần mã máy của lệnh.

Phần mã máy của 2 câu lệnh cuối có gì khác nhau khi dùng các toán tử WORD PTR và BYTE PTR.

Summary

■ Døng leänh E nhaäp vaøo ñoain vaên baün sau vaøo boä nhòu taii ñòa chæ DS:0100

8086/8088/80286 Assembly language.

Copyright 1988, 1886 by Brady Books, a division of Simon, Inc.

All right reserved, including the of reproduction in whole or in part, in any form.

(chuù yù kyù töi ñààu døng xuoáng døng coù mã ASCII laø 0D vaø 0A).