DEBUG 명령어와 어셈블리언어

어셈블리 언어 소개

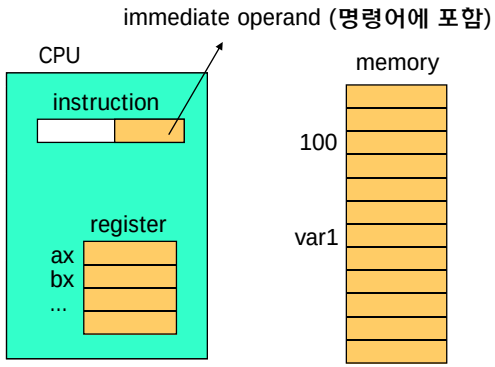
- 어셈블리 언어 명령어
  - 기계어 명령어를 심볼로 표기한 것
  - (1) 니모닉(mnemonic) (2) 피연산자(operand) 들로 구성됨
    - mnemonic: CPU 명령어의 기억을 돕는 짧은 이름
- Examples

```
clc                ; no operand, just a mnemonic
inc  ax            ; single operand
mov ax, bx         ; two operand
```

- 피연산자의 종류: (1) an immediate value (2) a register (3) a variable/a memory location

10	immediate value	
ax	register	
count	variable	memory
[200]	memory location	memory

Operand의 위치



DEBUG와 assembly program 작성

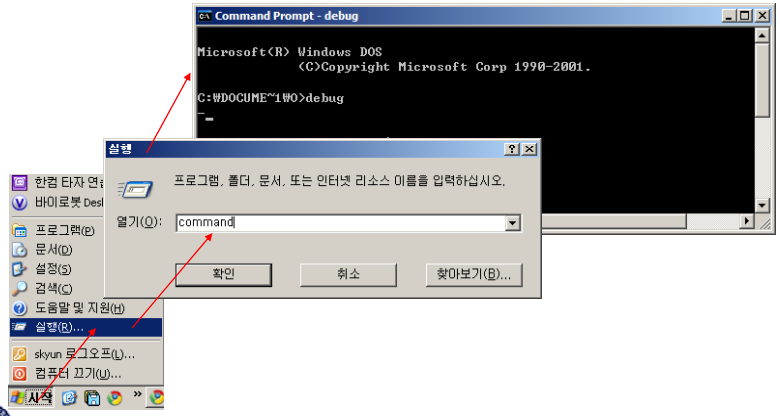
- debug
  - MS-DOS용 utility 프로그램
  - 16-bit x86용 프로그램의 디버깅 등의 기능 수행
  - 간단한 어셈블리 언어 프로그램을 입력하여 실행시킬 수 있음
    - (MASM 어셈블리 언어와 형식이 다름)
  - Windows-7에서는 제공하지 않을 수 있음
- Sample assembly language program for debug (DOS용)

```
mov ax, 5        ; ax ← 5h
add ax, 10       ; ax ← ax + 10h
sub ax, 6        ; ax ← ax – 1h
mov [120], ax    ; M[DS:120] ← ax
int 20           ; halt the program (DOS system call)
```

mov ax, 4c00 로 바꾸어도 됨
int 21

debug 명령어 실행 준비

- [시작 > 실행 > command 입력] 하여 command 창을 만듬
- debug 명령어 입력



DEBUG 내의 주요 명령어

- debug용 주요 명령어
  - program 작성 및 디버깅
    - a assemble
    - g go (execute)
    - r display registers
    - p proceed program
    - t trace
    - u unassemble
  - 도움말 및 종료
    - ? help
    - q quit
    - h hexadecimal addition & subtraction

DEBUG 내의 주요 명령어(2)

- 메모리 관련
  - d dump memory
  - e enter bytes
  - f fill a single value
  - c compare one memory range with another
  - m move bytes from one memory range
  - s search a memory range for a value
- 입출력
  - n file name (L, W command가 사용)
  - w write into file (cx: 저장되는 크기)
  - L load from disk
  - o output to a port
  - i input from a port

debug 실행

- debug 실행

```
C> debug
 - a                          ; 프로그램 입력 (현재의 IP부터)
 - a 100                      ; 100번지부터 프로그램 입력 (assemble)
1A3C:0100 mov ax,5
1A3C:0103 add ax,10
1A3C:0106 sub ax,4
1A3C:0109 mov [120], ax
1A3C:010C int 20
1A3C:010E
 - p 또는 t                   ; 프로그램 단계적 수행
AX=0005  BX=0000 CX=0000  DX=0000  SP=FFEE  BP=0000 SI=0000 DI=0000
DS=1A3C  ES=1A3C  SS=1A3C  CS=1A3C  IP=0103   NV UP EI PL NZ NA PE NC
1A3C:0103 051000       ADD     AX,0010
 - g                          ; 프로그램 실행 (현재의 IP부터)
 - g 100                      ; 100번지부터 실행
```

DEBUG 실행

- debug 실행 (계속)
  - d 120 ; 메모리 내용 출력 (DS)
  - d 120 121 ; 120번지부터 121번지까기 내용 출력
  - u ; 메모리 내용 unassemble (CS)
  - u 100 ; 100번지부터 unassemble
  - r ; register 내용 출력
  - r ax ; register AX 내용 변경

  AX 000F
  : 0015

  현재의 값
  (단순히 enter입력시 변경되지 않음)
  - q ; debug 종료
- debug 프로그램의 제한점
  - 복잡한 프로그램 작성 불가능
  - 80386이상에서 제공되는 명령어 사용 불가