

Assembly Language

Assignment 2

In this assignment you will figure out a simple Assembly language environment, common registers, and memory organization. First, apply the environment configuration to install an assembly utility called “Debug”. Then perform the exercise after.

Environment configuration:

- a. 32bit “x86” Windows (mostly winxp)
 - i. Start the command prompt [run utility>cmd]
 - ii. Run the following command “debug”.
- b. 64 bit windows
 - iii. Download DosBox ([download](#))
 - iv. Download debug.rar ([download](#))
 - v. Extract debug.rar to specific drive for example D:\
 - vi. Install and start DosBox and mount drive D as following [mount d d:\ ↵] *hint: note that C drive is mounted by default*
 - vii. Change directory to drive D as following [d: ↵]
 - viii. Run the command “debug”

Write a report with snapshots for the following procedure: (worth 20 points)

1. Run the command [? ↵] to list all the available commands with “debug” program
2. Run the command [r ↵] to list all the available registers
3. Record the contents of the following registers (CS, DS, IP, Flags: over flow, zero, carry) *Check hint 1*
4. Run the command [a 100 ↵] then write the following assembly program:

```
mov ax, 0001 ↵  
sub ax, 0001 ↵  
add ax, 0002 ↵  
sub ax, 0003 ↵  
add ax, 7fff ↵  
add ax, 7fff ↵
```

5. Press Enter again after the last instruction to end the “ a ” commands
6. Record the address in front of each instruction in the previous program
7. Run the command [p =100 ↵] to execute the first instruction at address 100
8. Record the contents of the following registers (AX, CS, DS, IP, Flag: over flow- sign-zero- carry).
9. Run the command [p ↵] 5 times to execute all the program instructions. In each time, record the contents of the following registers (AX, CS, DS, IP, Flag: over flow – sign- zero- carry).
10. Run the command [d 100 ↵] to dump (display) part of the memory contains the previous program.
11. From the first line in the dump, what is the machine code of the instruction (sub ax, 0003) ?

Hint 1: The following figure show the default values of the flags register

```
-r  
AX=0000 BX=0000 CX=0000 DX=0000 SP=00FD BP=0000 SI=0000 DI=0000  
DS=073F ES=073F SS=073F CS=073F IP=0100  OV UP EI PL NZ NA PO NC  
073F:0100 B80100 MDU AX,0001
```

Over flow flag	Sign flag	Zero flag	Carry flag
----------------	-----------	-----------	------------

Hint 2: for further help use the following tutorial
http://kipirvine.com/asm/debug/Debug_Tutorial.pdf