# SOLUTION TO MIDTERM

**GENERAL REMARKS ON STUDENT ANSWERS:** Please read the following carefully, not just for the correct answer but also for how you could go wrong. Some general and common errors include

- Not reading the question completely or not fully utilizing all the information given.
- English problems – either you do not understand the English instructions or you simply do not know how to construct proper English sentences to explain your ideas.
- Not showing your working or rough calculations. This way, we could not assign you partial credit.

1. **(5+5 POINTS)**

   Give one sentence explanations of these terms: (a) BIOS, (b) Register indirect mode.

   **ANSWER:**

   (a) Basic Input and Output System contains the DOS routines for Input and Output and other hardware dependent operations; this is stored in ROM and is used during bootup of machine.

   (b) This is the addressing mode in which the contents of a register is used as an offset of an operand. E.g., the source operand in `MOV AX,[BX]`.

   **PITFALLS:** (a) It is not enough to just say that BIOS stands for "Basic Input and Output System".

   (b) It is not true that you are always referring to the "contents of the memory location whose offset is in the specified register". For instance, if BX contains 2h, then in `MOV [BX],0` instruction, you are interested in the original contents of memory location DS:02h.

2. **(5+5 POINTS)**

   What are the physical addresses of the first and last byte in the segment whose number is 1234h?

   **ANSWER:** First byte is at 1234:0000=12340h. Last byte is at 12340:FFFF=2233Fh. **PITFALLS:** Offset of first byte is 0000h, not 0001h.

3. **(5+5 POINTS)**

   Give the decimal interpretation of the 12-bit number 8FEh:

(a) As an unsigned number.

(b) As a signed number.

**ANSWER:** (a) (unsigned) $(8 \times 16^2) + (15 \times 16) + (14) = 2302$. (b) (signed) 2's complement of 8FEh is 702h. This is 1026 (as a decimal number). So the answer is $-1026$.

**PITFALLS:** Some people still think that signed numbers are obtained by simply putting a 1 in the most significant bit.

4. **(15 POINTS)**

Assume a program has the following declarations at the beginning of the data segment, i.e. at offset 0000h.

```
var1  DB  -1
var2  DB 'ABCD'
var3  DW 0ABCDh
```

Draw a picture of memory at the beginning of the data segment, labeling the memory locations, the locations of the variables, and the contents of each byte.

**ANSWER:** Memory has this configuration:

```
var1, 0: 0FFh
var2, 1: 'A'
2,3,4: 'BCD'
var3, 5: 0CDh
6: 0ABh
```

**PITFALLS:** Some students thing that the entire string 'ABCD' is stored in the first word as the hexidecimal number 0ABCDh. You need 4 bytes for this! Conversely, some students confuse the word variable Var3 to be 4 bytes.

5. **(5+5+5 POINTS)**

For each of the following registers, name one instruction that *implicitly* uses the register:

(a) CX

(b) SP

(c) AX

**ANSWER:** (a) LOOP; (b) PUSH (or POP, CALL or RET); (c) MUL (or DIV, etc).

**PITFALLS:** An English problem – some students do not know what "implicit" means. But it is silly not to ask me to clarify if you do not understand the question! For (b), some offered `.STACK 100h`. You get partial credit here because .STACK is a pseudo-op. For (c), some have offered `INT` as an answer. You still get full credit, but I do not much like it because it depends on the conventions of the interrupt system.

6. **(10 POINTS)**

   Consider the code fragment:

```
.DATA
Values DB    5, 0FFh, 6, 7
...
.CODE
...
MOV AX, WORD PTR Values
MOV CL, 8
SAR AX, CL              ; shift arithmetic right
Contd:
...
```

   What is the contents of AX when the execution reaches Contd? Assume there is no jump into Contd.

   **ANSWER:** 0FFFFh. This is because AX is initially loaded with the word 0FF05h. After shifting right 8 times, while preserving sign bit, you get 0FFFFh.

   **PITFALLS:** You do not understand the pseudo-op "WORD PTR", which is meant to convert a variable into a word variable. Certainly it is nonsense to think that AX is initially loaded with 05FF0607h, as some students wrong, but you get partial credit if you think the initial value of AX is 05FFh.

7. **(15 POINTS)**

   Upon execution of the instruction `ADD AX,BX` the following status flags have the values

```
CF=1, OF=1, ZF=1, SF=0.
```

What can you say about the contents of registers AX and BX?

Are the values in AX and BX uniquely determined?

**ANSWER:** The values in AX and BX are both 8000h. Yes, these values are uniquely determined. REASONING: CF=1 implies a carry out from MSB.

OF=1 implies no carry into MSB.

These two facts imply that the MSB of AX and BX are 1.

ZF=1 implies all the other bits are zero.

NOTE: Not all the flag conditions necessary: `SF=0` is redundant.

**PITFALLS:** It is not really helpful to think of AX and BX as containing signed or unsigned numbers – they just contain bit patterns which you can interpret as signed or unsigned as you wish! Many student just look at one of these bit conditions and ignore the rest (e.g., you just say that CF=1 means there is "overflow" although this is not very accurate, and conclude that that AX+BX must be at least 10000h. You simply ignored the information about ZF and OF.)

8. **(20 POINTS)**

Write the assembly language statements corresponding to the following pseudo-Pascal code:

```
if ( ax < 0)
  then  if (ax > -10)
           then cx :=  0
           else cx := -1
        end_if
  else cx := 1
end_if
```

**ANSWER:** I will give you three solutions, which are increasing "compact". The first solution has 3 labels and 9 instructions.

```
; Solution 1
    CMP AX,0
    JGE One
    CMP AX,-10
    JLE MinusOne
    MOV CX,0
    JMP Done
```

```
MinusOne:
    MOV CX,-1
    JMP Done
One:
    MOV CX,1
Done:
```

The second solution has 2 labels and 8 instructions. We have also replaced moves into CX with INC and DEC of CX.

```
; Solution 2
    XOR CX,CX
    CMP AX,0
    JGE One
    CMP AX,-10
    JG  Done
    DEC CX
    JMP Done
One:
    INC CX
Done:
```

The third solution has 1 labels and 7 instructions.

```
; Solution 3
    MOV CX,1
    CMP AX,0
    JGE Done
    DEC CX
    CMP AX,-10
    JG  Done
    DEC CX
Done:
```

Which is the best solution? Which is the fastest solution?

**PITFALLS:** Many students do not insert the “JMP Done” instructions.