16.317: Microprocessor Systems Design I

Summer 2012

Lecture 5: Key Questions
July 23, 2012

1. Explain the operation of the bit test instructions (BT, BTR, BTS, BTC)

2. Explain the operation of the bit scan instructions (BSF, BSR).

3. **Example:** Given the following initial state, list all changed registers and/or memory locations and their new values. Where appropriate, you should also list the state of the carry flag (CF).

Initial state:

EAX: 00000000H
EBX: 0000000AH
ECX: 00000000H
EDX: 00000000H
CF: 0
ESI: 00000008H
EDI: FFFF0000H
EBP: 00000400H
ESP: 00002000H
DS: 2110H
SS: 1000H

Address		
21100H	04	00
21102H	10	10
21104H	89	01
21106H	20	40
21108H	02	00
2110AH	00	16
2110CH	17	03
2110EH	FF	00
21110H	1E	00
21112H	06	00
21114H	08	00
21116H	0A	00

Instructions:

```
BT    WORD PTR [02H], 4
BTC   WORD PTR [10H], 1
BTS   WORD PTR [04H], 1
BSF   CX, WORD PTR [0EH]
BSR   DX, WORD PTR [09H]
```

4. Explain the operations of the flag control instructions (LAHF/SAHF, CLC/STC/CMC, CLI/STI).

5. **Example:** Given the following initial state, list all changed registers and/or memory locations and their new values. Where appropriate, you should also list the state of the carry flag (CF).

Initial state:

EAX: 00000000H
EBX: 0000000AH
ECX: 00000005H
EDX: 00000000H
ESI: 00000008H
EDI: FFFF0000H
EBP: 00000400H
ESP: 00002000H
DS: 100FH
SS: 1000H
FLAGS: 00H

Address		
10110H	04	00
10112H	10	10
10114H	89	01
10116H	20	40
10118H	02	00
1011AH	00	16
1011CH	17	03
1011EH	FF	00
10120H	1E	00
10122H	06	00
10124H	08	00
10126H	0A	00

Instructions:

```
LAHF
MOV   [20H], AH
MOV   AH, [30H]
SAHF
MOV   AX, [26H]
CMC
RCL   AX, CL
```

6. Describe the operation of the compare instruction.

7. Complete the following table that describes the different x86 condition codes.

Mnemonic (cc)	Condition tested	Status flag setting for true condition
O		
NO		
B, NAE, C		
NB, AE, NC		
S		
NS		
P, PE		
NP, PO		
E, Z		
NE, NZ		
BE, NA		
NBE, A		
L, NGE		
NL, GE		
LE, NG		
NLE, G		

8. Describe the operation of the SETcc instruction. How can this instruction be used?

9. **Example:** Show the results of the following instructions, assuming that DS:100H = 0001H, DS:102H = 0003H, DS:104H = 1011H, DS:106H = 1011H, DS:108H = ABCDH, DS:10AH = DCBAH

   What complex condition does this sequence test?

```
MOV     AX, [100H]
CMP     AX, [102H]
SETLE   BL
MOV     AX, [104H]
CMP     AX, [106H]
SETE    BH
AND     BL, BH
MOV     AX, [108H]
CMP     AX, [10AH]
SETNE   BH
OR      BL, BH
```

10. Describe the two general classes of jump instruction.

11. Describe the different ways of specifying jump targets.

12. **Example:** Given CS = 1200H, IP = 0100H, and EBX = 14000020H, what are the target addresses of the following jump instructions?

- JMP 08H

- JPE FFF0H

- JE BX

- JNZ EBX

13. Given the instructions below, what are the resulting register values if:
    - AX = 0010H, BX = 0010H
    - AX = 1234H, BX = 4321H

What type of high-level program structure does this sequence demonstrate?

```
        CMP   AX, BX
        JE    L1
        ADD   AX, 1
        JMP   L2
L1:     SUB   AX, 1
L2:     MOV   [100H], AX
```

14. **Example:** Given the instructions below, what are the resulting register values if, initially, AX = 0001H?

What type of high-level program structure does this sequence demonstrate?

```
     MOV  CL, 5
L:   SHL  AX, 1
     DEC  CL
     JNZ  L
```

15. **Example:** Given the instructions below, what are the resulting register values if, initially, AX = 0001H?

What type of high-level program structure does this sequence demonstrate?

```
     MOV  CL, 5
L:   JZ   END
     ADD  AX, AX
     DEC  CL
     JMP  L
END: MOV  [10H], AX
```

16. Describe the 80386 loop instructions, as well as how these instructions can be used in a typical program.

17. Rewrite the post-tested loop example from earlier to use a loop instruction.

```
        MOV   CL, 5
L:      SHL   AX, 1
        DEC   CL
        JNZ   L
```

18. Describe the operation of the following program (Example 6.15-6.16).
    What is the final value of SI if the 15 bytes between 0A001 and 0A00F have the following values?
    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E

```
        MOV   DL, 05
        MOV   AX, 0A00
        MOV   DS, AX
        MOV   SI, 0000
        MOV   CX, 000F
AGAIN:  INC   SI
        CMP   [SI], DL
        LOOPNE AGAIN
```