Homework #4 Answer Key
Due: 07/14/2001

Problem 1) Consider the following fragment of 8088 assembly language code:

```
mov cx, 10    ; 4
xor ax, ax    ; 3
mov si, 0    ; 4
label: mov stuff[si], ax  ; 9 + 9 + 4 = 22
add si, 3    ; 4
shl ax    ; 2
inc ax    ; 2
loop label    ; 17/5
```

1a) (20 Points) How many clock cycles does this sequence of instructions take to execute on an 8088 processor? Assume that DS is loaded with the correct segment address, so that no segment overrides are required to access the array ‘stuff’.

Answer:

The code before the loop takes (4 + 3 + 4) = 11 clock cycles. The body of the loop takes (22 + 4 + 2 + 2) = 30 clock cycles. The loop executes 10 times, so for 9 of those iterations, the loop instruction will take 17 cycles. On the final iteration of the loop, it will take 5. So the total time will be: (11 + 10*30 + 9*17 + 5) = 409 clock cycles.

1b) (5 Points) Assuming that the clock frequency of the machine is 4.77 Mhz, how long (e.g. how many microseconds) will the above sequence of instructions take to execute?

Answer:

The time is the clock period times the number of clock cycles: (1/4.77*10^6)*469

\[ \text{Time} = \frac{1}{4.77 \times 10^6} \times 469 \approx 98.321 \text{ us} \]

Problem 2) When the assembler encodes the instruction: MOV FOO[BP+SI],DH, The resulting machine code will occupy 4 bytes of memory. The bytes will be as follows:

```
[opcode] [mod reg r/m] [low byte of offset of VAR] [high byte of offset of VAR]
```

2a) (5 Points) What will be the value encoded by the assembler for the opcode byte (i.e. what will be the value (in hex) of the first byte of the encoded instruction)?

 Opcode: 1 0 0 0 1 0 d w , “From Reg” => d=0, Byte instruction => w=0
2c) (5 Points) If the memory location for the label “FOO” is 3C90h, what will be the complete encoding for the above instruction in hex?

\[ \text{88 B2 90 3Ch} \]

Problem 3) (15 Points) The following shows two different instruction which will set the DX register to 0. What is the difference in code size and execution time of the two instructions on an 8088 processor?

- \text{xor dx,dx} \quad \text{2 bytes, 3 clock cycles}
- \text{mov dx,0} \quad \text{3 bytes, 4 clock cycles}
- \text{sub dx,dx} \quad \text{2 bytes, 3 clock cycles}

Problem 4) (40 Points) Write a procedure in assembly language to count the number of times that the DOS Function Calls (INT 21h) are performed. You are to “hook” into the existing interrupt so that the operation of the DOS function call occurs prior to your update of the count. Include the lines of code at the beginning of the main routine required to modify the interrupt vector table to point to your procedure, and at the end of the main routine for restoring the interrupt vector table to its original status.

You may assume the following:
- There are memory locations labeled “fcncount” where the total may be stored, “intaddr” where the code segment and offset of the original interrupt service routine may be stored.
- INT 21h will not be called more than \(2^{16}-1\) times by the main routine.
- Calls to INT 21h for the getting/setting of the interrupt vector table at the beginning and end of the main routine may be ignored in the count.

Answer:

\[
\begin{align*}
\text{Answer:} & & \cdots \\text{get int vector} \\
\text{mov } & \text{ah,35h} & \\
\text{mov } & \text{al,21h} & \text{int vector index} \\
\text{int } & \text{21h} & \\
\text{mov } & \text{intaddr,ds} & \text{save cs of int vector} \\
\text{mov } & \text{intaddr+2,dx} & \text{save ip of int vector} \\
\text{mov } & \text{es, cs} & \text{load current code seg.} \\
\text{mov } & \text{hx, offset fncntr} & \text{load offset of procedure}
\end{align*}
\]
call    word ptr intaddr ; perform call to original ISR
inc     fcncount ; count the function call
iret ; return to interrupted routine
fcncntr    endp

... 
mov    ah,25h
mov    es,intaddr
mov    bx,intaddr+2
int    21h
...