**Solution and comments on student work**

Fall 2020 CSC 332 Quiz 1 (Ch H) 300 Points 75 minutes

Each question is 100 Points.

Q1. Convert the following code fragment to assembly code fragment, using instructions discussed in class.

if X > Y then Y=X

else X=Y

Load X, R1

Load Y, R2

cmp R1, R2

jmpp L1

Store R2, X

Jmp L2

L1:Store R1, Y

L2:

Q2.

Suppose a user wants to do a system call. Assume that the service routine of this system call is at physical address 500.

Suppose the user knows this address of the service routine. So instead of executing a system call, the user simply jumps to this location 500

(by executing “JMP 500”).

Assume that logical and physical addresses are the same and no memory protection is in place, i.e., cpu does not check that this address 500 is beyond the user’s memory space.

Will something go wrong while the service routine executes?

Explain in less than 100 words.

Answer:

Yes, something will go wrong.

The service routine is executing in user mode since PSW was not changed. When the service routine executes a priviledged instruction (ex. RTI or something earlier), the CPU will not execute that instruction and generate an interrupt. The service routine of this interrupt would kill the user.

Q3.

1. Suppose content of a byte is AC in hexadecimal.

Write it down as an 8 bit sequence.

Answer:

10101100

1. What is the main motivation to have a DMA?

Answer:

To free the CPU from the task of moving data between an i/o module and memory.

**Comments on student work:**

Q1 Some of you were confused on the Go TO logic. Did X=Y instead of Y=X etc.

Some of you used jump instructions not defined in slides. Ex. JL. The question asked you to use an instruction discussed in lectures. There are millions of assembly languages and I do not want to guess what your new instruction really means.

Q2. Some of you said that the entire service routine was an instruction, and a PRIVILEGED one. And it could not be executed since mode=user. This is wrong. Service routine has many instructions in it. If the first few are non-privileged instructions, then they will get executed. The trouble would arise when you try to execute a privileged instruction in the service routine.

A couple of you said that a system call is a privileged instruction. Horrible!

I expected an exact place where the problem would arise. This would be the first privileged instruction executed within service routine.

Q3. Some of you were vague. Ex. They said that it lets DMA do all the work for i/o.

All the work also involves interrupt handling and that is actually still done by CPU at the end of final interrupt from DMA.