Last NAME: First Name:

Computer Science
C.Sc. 342

Quiz No.2
CSc or CPE

April 19, 2021

Please write your name on every page.
NO CORRECTIONS ARE ALLOWED !!!!! You may use back page for notes.
You can use any printed material (PDF FORMAT IS ALLOWED). No computers are allowed.
Please review the entire quiz first and then budget your time carefully.

Please hand write and sign statements affirming that you will not cheat:
"I will neither give nor receive unauthorized assistance on this exam.
I will use only one computing device to perform this test"

Please hand write and sign **here:**

This quiz has 9 pages.

Question	Your Grade	Max Grade
1.1		10
1.2		10
1.3		10
2.1		10
2.2		10
2.3		10
3.1		2
3.2		2
3.3		2
3.4		2
3.5		2
4.1		10
4.2		10
4.3		10

Total: **100**

Last NAME: First Name:

Question 1. A student is given IA-32 compiler generated listing as shown below, includes machine instructions, assembly instructions, and relative addresses of the instructions. The C source code is not displayed!

```
0001e  c7 45 f8 ffffffff    mov     DWORD PTR _i$[ebp], -1


00025  c7 45 ecfeffffff     mov     DWORD PTR _j$[ebp], -2


0002c  c7 45 e0 00 00 00 00 mov     DWORD PTR _k$[ebp], 0



00033  8b 45 f8 mov     eax, DWORD PTR _i$[ebp]
00036  03 45 ec  add    eax, DWORD PTR _j$[ebp]
00039  89 45 e0 mov      DWORD PTR _k$[ebp], eax
```

Please answer the following questions:

Question 1.1 (10 POINTS) What is the total length in bytes of the shown machine code. (Please give your answer using decimal numbers).

Question 1.2. (10 POINTS) Please write the corresponding C-code to the right of the assembly code.

Question 1.3 (10 POINTS) Do you have enough information to determine the values of the variables: **_i$, _j$, _k$?**

Please answer YES or NO.

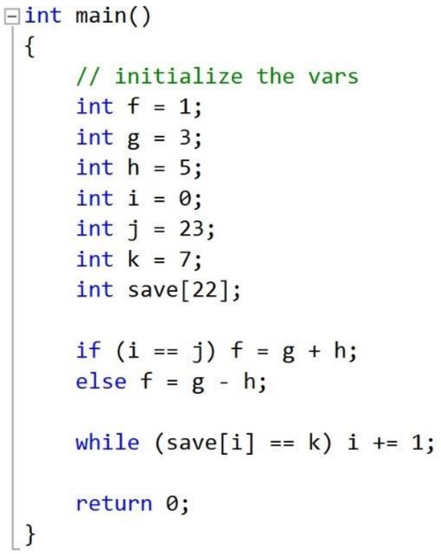
If your answer is **yes**

1.3.1 WHAT ARE THEIR `SIGNED DECIMAL VALUES:

1.3.2 How compiler generated variables: _i$, _j$, _k$ are used by the code? Please describe in 1sentence.

Last NAME: First Name:

Question 2. You are given the following C code and corresponding Disassembly window in .NET environment.



```c
int main()
{
    // initialize the vars
    int f = 1;
    int g = 3;
    int h = 5;
    int i = 0;
    int j = 23;
    int k = 7;
    int save[22];

    if (i == j) f = g + h;
    else f = g - h;

    while (save[i] == k) i += 1;

    return 0;
}
```

FIGURE 1. C- Source code.

Last   NAME: First Name:

Please answer the following questions:

Question 2.1. (10 POINTS) **Based on information displayed in Figure 2. Please the expression how addresses of variables f, g, h are computed at run –time.**

f

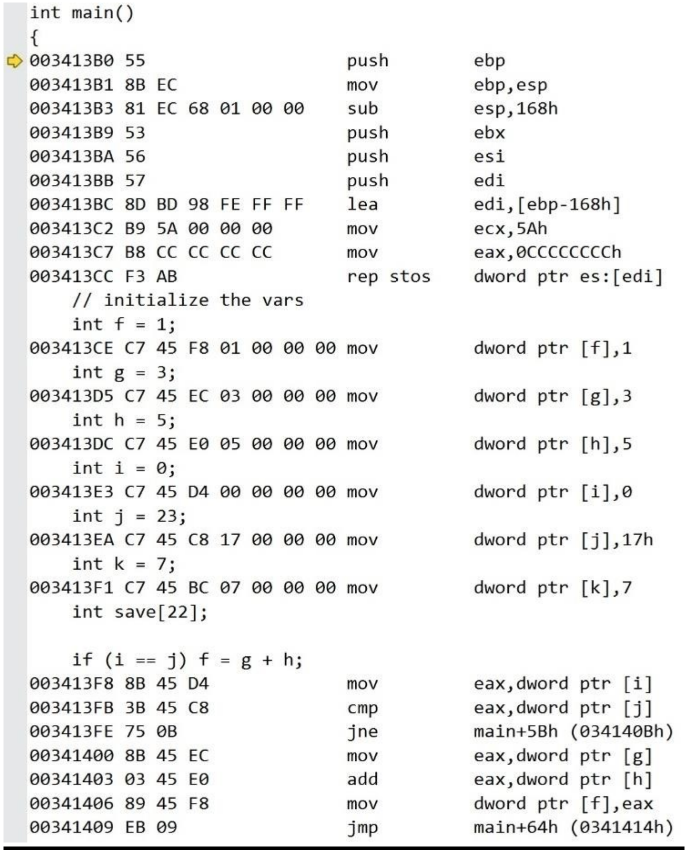
g

h

Question 2.2 (10 POINTS) **Can you determine the offsets to variables f, g, h ?**

Circle around YES or NO.

If your answer is YES , please list the offset value for each variable in hex and decimal.



```
int main()
{
⇨ 003413B0 55                   push        ebp
003413B1 8B EC                  mov         ebp,esp
003413B3 81 EC 68 01 00 00      sub         esp,168h
003413B9 53                     push        ebx
003413BA 56                     push        esi
003413BB 57                     push        edi
003413BC 8D BD 98 FE FF FF      lea         edi,[ebp-168h]
003413C2 B9 5A 00 00 00         mov         ecx,5Ah
003413C7 B8 CC CC CC CC         mov         eax,0CCCCCCCCh
003413CC F3 AB                  rep stos    dword ptr es:[edi]
    // initialize the vars
    int f = 1;
003413CE C7 45 F8 01 00 00 00 mov         dword ptr [f],1
    int g = 3;
003413D5 C7 45 EC 03 00 00 00 mov         dword ptr [g],3
    int h = 5;
003413DC C7 45 E0 05 00 00 00 mov         dword ptr [h],5
    int i = 0;
003413E3 C7 45 D4 00 00 00 00 mov         dword ptr [i],0
    int j = 23;
003413EA C7 45 C8 17 00 00 00 mov         dword ptr [j],17h
    int k = 7;
003413F1 C7 45 BC 07 00 00 00 mov         dword ptr [k],7
    int save[22];

    if (i == j) f = g + h;
003413F8 8B 45 D4               mov         eax,dword ptr [i]
003413FB 3B 45 C8               cmp         eax,dword ptr [j]
003413FE 75 0B                  jne         main+5Bh (034140Bh)
00341400 8B 45 EC               mov         eax,dword ptr [g]
00341403 03 45 E0               add         eax,dword ptr [h]
00341406 89 45 F8               mov         dword ptr [f],eax
00341409 EB 09                  jmp         main+64h (0341414h)
```

Figure 2. Disassembly window.

Offset to variable f is ……….

Offset to variable g is ……….

Offset to variable h is ……….

Question 2.3 (10 POINTS) After the instruction at the address 0x00341400 is executed.

What will be stored in *Register EAX if your answer is value write it, if – address write it*

*the **value** of variable **g** ?*   *or the **address** of variable **g** ?*

Question 3. (10 points)

Translate MIPS binary code into assembly language. Left column are addresses, right column are machine instructions. The third column is your answer- mips assembly instruction. Please justify your answer in the row below.

```
[0x00400054]   0x340f000f


[0x00400058]   0xafaf0028


[0x0040005c]   0x27a4002a


[0x00400060]   0x03e00008

[0x00400064]   0x27bdffd0
```

Question 4. (30 points)You are given a library in some directory. You know the source code of one function in the library.

```
Extern int main_stat=-11;
int  myadd(intx, inty)
{
      int i = 0x800000000000005;
      int t = main_stat;
      main_stat = -2;
      t = x+ y;
      y = t+main_stat;
      returny;
      }
```

You were able to link this library to your main project file. Main() in your project calls the procedure myadd().

On the next three pages you given three snapshots in debug

mode. ----Please answer questions on each page

You have displayed Register file **at INSTANCE_1**:

EAX = CCCCCCCC EBX = 7F9D8000 ECX = 00000000 EDX = 00000001 ESI = 00000000
EDI = 00E6F9C8 EIP = 002B104C ESP = 00E6F8E4 EBP = 00E6F9C8 EFL = 00000206

```
Int myadd(int, int);
static int main_stat =-7;
int main()
{
002B1020  push ebp
002B1021  mov ebp,esp
002B1023  sub         esp,0D8h
002B1029  push ebx
002B102A  push esi
002B102B  push edi
002B102C  lea edi,[ebp-0D8h]
002B1032  mov         ecx,36h
002B1037  mov         eax,0CCCCCCCCh
002B103C  rep stos dword ptr es:[edi]
       Int i = -2;
002B103E  mov dword ptr [i],0FFFFFFFEh
       int j = -3;
002B1045  mov dword ptr [j],0FFFFFFFDh
       main_stat = 13;
002B104C  mov dword ptr ds:[2B8000h],0Dh
       i=-1;
002B1056  movdwordptr [i],0FFFFFFFFh
       j =7;
002B105D  mov dword ptr [j],7
       // call function thatimplements addition
       // function myadd(int,int)
       j = myadd(i,j);
002B1064  mov eax,dword ptr [j]
002B1067  push eax
002B1068  mov ecx,dword ptr [i]
002B106B  push ecx
002B106C  call myadd (02B100Ah)
002B1071  add         esp,8
002B1074  mov dword ptr [j],eax
              i = main_stat;
002B1077  mov eax,dword ptr ds:[002B8000h]
002B107C  mov dword ptr [i],eax
       return 0;
002B107F  xor eax,eax

}
002B1081  pop edi
002B1082  pop esi
002B1083  pop ebx
002B1084  add         esp,0D8h
002B108A  cmp ebp,esp
002B108C  call        _RTC_CheckEsp (02B12B0h)
002B1091  mov esp,ebp
002B1093  pop ebp
002B1094  ret
```

Questions 4.1 What is the signed hexadecimal value of an integer at the address 0X002B8000h at the **instance_1 ?**

You have displayed Register file **at INSTANCE_2**:

```
EAX = 00000007 EBX = 7F9D8000 ECX = FFFFFFFF EDX = 00000001 ESI = 00000000 EDI = 00E6F9C8
EIP = 002B106C ESP = 00E6F8DC EBP = 00E6F9C8 EFL = 00000206

Int myadd(int, int);
Static int main_stat =-7;
int main()
{
002B1020  push ebp
002B1021  mov ebp,esp
002B1023  sub         esp,0D8h
002B1029  push ebx
002B102A  push esi
002B102B  push edi
002B102C  lea edi,[ebp-0D8h]
002B1032  mov         ecx,36h
002B1037  mov         eax,0CCCCCCCCh
002B103C  rep stos dword ptr es:[edi]
       Int i = -2;
002B103E  mov dword ptr [i],0FFFFFFFEh
       int j = -3;
002B1045  mov dword ptr [j],0FFFFFFFDh
       main_stat = 13;
002B104C  mov dword ptr ds:[2B8000h],0Dh
       i=-1;
002B1056  mov dword ptr [i],0FFFFFFFFh
       j =7;
002B105D  mov dword ptr [j],7
       // call function thatimplements addition
       // function myadd(int,int)
       j = myadd(i,j);
002B1064  mov eax,dword ptr [j]
002B1067  push eax
002B1068  mov ecx,dword ptr [i]
002B106B  push ecx
002B106C  call myadd (02B100Ah)
002B1071  add         esp,8
002B1074  mov dword ptr [j],eax
              i = main_stat;
002B1077  mov eax,dword ptr ds:[002B8000h]
002B107C  mov dword ptr [i],eax
       return 0;
002B107F  xo reax,eax

}
002B1081  pop edi
002B1082  pop esi
002B1083  pop ebx
002B1084  add         esp,0D8h
002B108A  cmp ebp,esp
002B108C  call        _RTC_CheckEsp (02B12B0h)
002B1091  mov esp,ebp
002B1093  pop ebp
002B1094  ret
```

Questions 4.2 What is the signed hexadecimal value of an integer at the address 0X002B8000h at the **instance_2** ?

Last   NAME: First Name:

You have displayed Register file **at INSTANCE_3**:

```
EAX = 00000004 EBX = 7F9D8000 ECX = 00000000 EDX = 00000001 ESI = 00000000 EDI = 00E6F9C8
EIP = 002B1077 ESP = 00E6F8E4 EBP = 00E6F9C8 EFL = 00000216

Int myadd(int, int);
Static int main_stat =-7;
int main()
{
002B1020  push ebp
002B1021  mov ebp,esp
002B1023  sub         esp,0D8h
002B1029  push ebx
002B102A  push esi
002B102B  push edi
002B102C  lea edi,[ebp-0D8h]
002B1032  mov         ecx,36h
002B1037  mov         eax,0CCCCCCCCh
002B103C  rep stos dword ptres:[edi]
       Int i = -2;
002B103E  mov dword ptr [i],0FFFFFFFEh
       int j = -3;
002B1045  mov dword ptr [j],0FFFFFFFDh
       main_stat = 13;
002B104C  mov dword ptr ds:[2B8000h],0Dh
       i=-1;
002B1056  mov dword ptr [i],0FFFFFFFFh
       j =7;
002B105D  mov dword ptr [j],7
       // call function thatimplements addition
       // function myadd(int,int)
       j = myadd(i,j);
002B1064  mov eax,dword ptr [j]
002B1067  push eax
002B1068  mov ecx,dword ptr [i]
002B106B  push ecx
002B106C  call myadd (02B100Ah)
002B1071  add         esp,8
002B1074  mov dword ptr [j],eax
              i = main_stat;
002B1077  mov eax,dword ptr ds:[002B8000h]
002B107C  mov dword ptr [i],eax
       return 0;
002B107F  xor eax,eax

}
002B1081  pop edi
002B1082  pop esi
002B1083  pop ebx
002B1084  add         esp,0D8h
002B108A  cmp ebp,esp
002B108C  call        _RTC_CheckEsp (02B12B0h)
002B1091  mov esp,ebp
002B1093  pop ebp
002B1094  ret
```

Questions 4.3 What is the signed hexadecimal value of an integer at the address 0X002B8000h at the **instance_3** ?