1 Pre-Check

This section is designed as a conceptual check for you to determine if you conceptually understand and have any misconceptions about this topic. Please answer true/false to the following questions, and include an explanation:

1.1 After calling a function and having that function return, the t registers may have been changed during the execution of the function, while a registers cannot.

1.2 Let a0 point to the start of an array x. lw s0, 4(a0) will always load x[1] into s0.

1.3 Assuming no compiler or operating system protections, it is possible to have the code jump to data stored at 0(a0) (offset 0 from the value in register a0) and execute instructions from there.

1.4 Assuming integers are 4 bytes, adding the ASCII character 'd' to the address of an integer array would get you the element at index 25 of that array (assuming the array is large enough).

1.5 jalr is a shorthand expression for a jal that jumps to the specified label and does not store a return address anywhere.

1.6 Calling j label does the exact same thing as calling jal label.
2 Basic Instructions

For your reference, here are some of the basic instructions for arithmetic operations and dealing with memory (Note: ARG1 is argument register 1, ARG2 is argument register 2, and DR is destination register):

<table>
<thead>
<tr>
<th>[inst]</th>
<th>[destination register] [argument register 1] [argument register 2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds the two argument registers and stores in destination register</td>
</tr>
<tr>
<td>xor</td>
<td>Exclusive or’s the two argument registers and stores in destination register</td>
</tr>
<tr>
<td>mull</td>
<td>Multiplies the two argument registers and stores in destination register</td>
</tr>
<tr>
<td>sll</td>
<td>Logical left shifts ARG1 by ARG2 and stores in DR</td>
</tr>
<tr>
<td>srl</td>
<td>Logical right shifts ARG1 by ARG2 and stores in DR</td>
</tr>
<tr>
<td>sra</td>
<td>Arithmetic right shifts ARG1 by ARG2 and stores in DR</td>
</tr>
<tr>
<td>slt/u</td>
<td>If ARG1 &lt; ARG2, stores 1 in DR, otherwise stores 0, u does unsigned comparison</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[inst]</th>
<th>[register] [offset]([register containing base address])</th>
</tr>
</thead>
<tbody>
<tr>
<td>sw</td>
<td>Stores the contents of the register to the address+offset in memory</td>
</tr>
<tr>
<td>lw</td>
<td>Takes the contents of address+offset in memory and stores in the register</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[inst]</th>
<th>[argument register 1] [argument register 2] [label]</th>
</tr>
</thead>
<tbody>
<tr>
<td>beq</td>
<td>If ARG1 == ARG2, moves to label</td>
</tr>
<tr>
<td>bne</td>
<td>If ARG1 != ARG2, moves to label</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>[inst]</th>
<th>[destination register] [label]</th>
</tr>
</thead>
<tbody>
<tr>
<td>jal</td>
<td>Stores the next instruction’s address into DR and moves to label</td>
</tr>
</tbody>
</table>

You may also see that there is an “i” at the end of certain instructions, such as addi, slli, etc. This means that ARG2 becomes an “immediate” or an integer instead of using a register. There are also immediates in some other instructions such as sw and lw. Note that the size (maximum number of bits) of an immediate in any given instruction depends on what type of instruction it is (more on this soon!).

2.1 Assume we have an array in memory that contains int *arr = {1,2,3,4,5,6,0}. Let register s0 hold the address of the element at index 0 in arr. You may assume integers are four bytes and our values are word-aligned. What do the snippets of RISC-V code do? Assume that all the instructions are run one after the other in the same context.
a) lw t0, 12(s0) -->
b) sw t0, 16(s0) -->
c) slli t1, t0, 2
   add t2, s0, t1
   lw t3, 0(t2) -->
   addi t3, t3, 1
   sw t3, 0(t2)
d) lw t0, 0(s0)
   xori t0, t0, 0xFFF -->
   addi t0, t0, 1
### 3 C to RISC-V

3.1 Translate between the C and RISC-V verbatim.

<table>
<thead>
<tr>
<th>C</th>
<th>RISC-V</th>
</tr>
</thead>
</table>
| // s0 -> a, s1 -> b  
// s2 -> c, s3 -> z  
int a = 4, b = 5, c = 6, z;  
z = a + b + c + 10;          | addi s0, x0, 0  
addi s1, x0, 1  
addi t0, x0, 30  
loop:  
    beq s0, t0, exit  
    add s1, s1, s1  
    addi s0, s0, 1  
    jal x0, loop  
exit: |
| // s0 -> int * p = intArr;  
// s1 -> a;  
*p = 0;  
int a = 2;  
p[1] = p[a] = a; | addi s0, x0, 0  
addi s1, x0, 1  
addi t0, x0, 30  
loop:  
    beq s0, t0, exit  
    add s1, s1, s1  
    addi s0, s0, 1  
    jal x0, loop  
exit: |
| // s0 -> a, s1 -> b  
int a = 5, b = 10;  
if(a + a == b) {  
    a = 0;  
} else {  
    b = a - 1;  
} | addi s0, x0, 0  
addi s1, x0, 1  
addi t0, x0, 30  
loop:  
    beq s0, t0, exit  
    add s1, s1, s1  
    addi s0, s0, 1  
    jal x0, loop  
exit: |
| // s0 -> n, s1 -> sum  
// assume n > 0 to start  
for(int sum = 0; n > 0; n--) {  
    sum += n;  
} | addi s0, x0, 0  
addi s1, x0, 1  
addi t0, x0, 30  
loop:  
    beq s0, t0, exit  
    add s1, s1, s1  
    addi s0, s0, 1  
    jal x0, loop  
exit: |
4  RISC-V with Arrays and Lists

Comment what each code block does. Each block runs in isolation. Assume that there is an array, `int arr[6] = {3, 1, 4, 1, 5, 9}`, which starts at memory address `0xBFFFFF00`, and a linked list struct (as defined below), `struct ll* lst`, whose first element is located at address `0xABCD0000`. Let `s0` contain `arr`'s address `0xBFFFFF00`, and let `s1` contain `lst`'s address `0xABCD0000`. You may assume integers and pointers are 4 bytes and that structs are tightly packed. Assume that `lst`'s last node's `next` is a NULL pointer to memory address `0x00000000`.

```c
struct ll {
    int val;
    struct ll* next;
}
```

4.1  
```
lw  t0, 0(s0)
lw  t1, 8(s0)
add  t2, t0, t1
sw  t2, 4(s0)
```

4.2  
```
loop:  beq  s1, x0, end
      lw  t0, 0(s1)
      addi t0, t0, 1
      sw  t0, 0(s1)
      lw  s1, 4(s1)
      jal  x0, loop
end:
```

4.3  
```
add  t0, x0, x0
loop:  slti t1, t0, 6
       beq  t1, x0, end
       slli t2, t0, 2
       add  t3, s0, t2
       lw  t4, 0(t3)
       sub  t4, x0, t4
       sw  t4, 0(t3)
       addi t0, t0, 1
       jal  x0, loop
end:
```

5  RISC-V Calling Conventions

5.1  How do we pass arguments into functions?
How are values returned by functions?

What is sp and how should it be used in the context of RISC-V functions?

Which values need to saved by the caller, before jumping to a function using jal?

Which values need to be restored by the callee, before returning from a function?

In a bug-free program, which registers are guaranteed to be the same after a function call? Which registers aren’t guaranteed to be the same?

Write a function `sumSquare` in RISC-V that, when given an integer `n`, returns the summation below. If `n` is not positive, then the function returns 0.

\[
\frac{n^2 + (n - 1)^2 + (n - 2)^2 + \ldots + 1^2}{n}.
\]

For this problem, you are given a RISC-V function called `square` that takes in a single integer and returns its square.

First, let’s implement the meat of the function: the squaring and summing. We will be abiding by the caller/callee convention, so in what register can we expect the parameter `n`? What registers should hold `square`’s parameter and return value? In what register should we place the return value of `sumSquare`?
Since `sumSquare` is the callee, we need to ensure that it is not overriding any registers that the caller may use. Given your implementation above, write a prologue and epilogue to account for the registers you used.