Tutorial: Stacks and Procedures

Stacks and Procedures: 1

12 points possible (ungraded)

Harry Hapless is a friend struggling to finish his Lab; knowing that you completed it successfully, he asks your help understanding the operation of the quicksort procedure, which he translated from the Python code given in the lab handout:

```
def quicksort(array, left, right):
   if left < right:
      pivotIndex = partition(array,left,right)
      quicksort(array,left,pivotIndex-1)
      quicksort(array,pivotIndex+1,right)
```

```
quicksort:
      PUSH(LP)
      PUSH(BP)
      MOVE(SP, BP)
      PUSH(R1)
      PUSH(R2)
      PUSH(R3)
      PUSH(R4)

      LD(BP, -12, R1)
      LD(BP, -16, R2)
aa:   LD(BP, -20, R3)

      CMPLT(R2, R3, R0)
      BF(R0, qx)

      PUSH(R3)
      PUSH(R2)
      PUSH(R1)
      BR(partition, LP)
      DEALLOCATE(3)
      MOVE(R0, R4)
xx:
      SUBC(R4, 1, R0)
      PUSH(R0)
      PUSH(R2)
      PUSH(R1)
      BR(quicksort, LP)
      DEALLOCATE(3)

      PUSH(R3)
      ADDC(R4, 1, R0)
      PUSH(R0)
      PUSH(R1)
      BR(quicksort, LP)
bb:   DEALLOCATE(3)

qx:   POP(R4)
      POP(R3)
      POP(R2)
      POP(R1)
cc:   MOVE(BP, SP)
      POP(BP)
      POP(LP)
      JMP(LP)
```

You recall from your lab that each of the three arguments and the local variable are 32-bit binary integers. You explain to Harry that quicksort returns no value, but is called for its effect on the contents of a region of memory dictated by its argument values. Harry asks some questions about the possible effect of the call **quicksort(0×1000, 0×10, 0×100)**:

0
9
0
$2F0$
$94C$
$F94$
1
2
3
4
8
0
$2F0$
$F24$
FCC
$2F0$
0
9
9
8
7
$2F0$
$F48$
$FF0$
$BP \rightarrow$ $2F0$
0
8
6
$SP \rightarrow$

1. Given the above call to **quicksort**, what is the region of memory locations (outside of the stack) that might be changed?
   Lowest memory address possibly effected: 0x

   Answer: 1040

Highest memory address possibly effected: 0x

Answer: 1400

Explanation

The lowest memory address where an element of the array is stored is array[left] = 0×1000 + 4*0×10 = 0×1040. The highest memory address of the array is array[right] = 0×1000 + 4*0×100 = 0×1400.

Harry's translation of quicksort to Beta assembly language appears above on the right.

2. What register did Harry choose to hold the value of the variable **pivotIndex**?

Register holding pivotIndex value: R

Answer: 4

Explanation

If you look at the **MOVE(R0, R4)** that comes 2 instructions after the call to partition, you see that the result of paritition (R0) is moved to R4. The variable that receives the result of partition is **pivotIndex**.

After loading and assembling this code in BSim, Harry has questions about its translation to binary.

3. Give the hex value of the 32-bit machine instruction with the tag **aa** in the program to the right.

Hex translation of instruction at aa: 0x

Answer: 607BFFEC

Explanation

The assembled format of the instruction **LD(BP,-20,R3)** is:

opcode | Rc | Ra | literal = LD | R3 | R27 | -20

= 011000 00011 11011 0xFFEC = 0110 0000 0111 1011 0xFFEC = 0×607BFFEC

Harry tests his code, which seems to work fine. He questions whether it could be shortened by simply eliminating certain instructions.

4. Would Harry's quicksort continue to work properly if the instruction at **bb** were eliminated? If the instruction at **cc** were eliminated? Indicate which, if any, of these instructions could be deleted.

OK to delete instruction at bb?

- Yes
- No ✔

OK to delete instruction at cc?

- Yes ✔
- No

Explanation

If you remove the DEALLOCATE instruction at label **bb**, then you would end up popping the wrong values at label **qx**.

If you remove the MOVE(BP, SP) instruction at label **cc**, everything will still work because there were no local variables allocated in the implementation of this procedure so SP already equals BP after you pop the used registers.

Harry runs his code on one of the Lab test cases, which executes a call to **quicksort(Y, 0, X)** via a **BR(quicksort, LP)** at address **0×948**. Harry halts its execution just as the instruction following the **xx** tag is about to be executed. The contents of a region of memory containing the topmost locations on the stack is shown to the right.

Calculator

5. What are the arguments to the current quicksort call? Use the stack trace shown above to answer this question.

Arguments: array = 0x

Answer: 2F0

left = 0x

Answer: 7

right = 0x

Answer: 8

Explanation

The stack frame for one call to **quicksort** is:

$$\begin{array}{l} Right \\ Left \\ Array \\ LP \\ BP \\ R1 \\ R2 \\ R3 \\ R4 \end{array}$$

The three arguments (array, left, and right) are put on the stack in reverse order. Then we store the LP, then the BP and then R1-R4 so that we can use those registers within our procedure.

Since we are told that the program halts at the **xx** label, we know that we just deallocated the 3 arguments for the partition procedure call and are now ready to continue with the recursive quicksort calls. This means that the SP is pointing immediately following a full stack frame. This information helps us label our stack as follows:

0	
9	Right
9	Left
$2F0$	Array
$94C$	LP
$F94$	BP
1	R1
2	R2
3	R3
4	R4
8	Right
0	Left
$2F0$	Array
$F24$	LP
FCC	BP
$2F0$	R1
0	R2
9	R3
9	R4
8	Right
7	Left
$2F0$	Array

Calculator

	$F48$	LP
	$FF0$	BP
$BP \rightarrow$	$2F0$	R1
	0	R2
	8	R3
	6	R4
$SP \rightarrow$		

The current quicksort call is the bottom most one. We see that the arguments for that call are array = 0×2F0, Left = 7, and Right = 8.

6. What is the value **X** in the original call **quicksort(Y, 0, X)**?
   Value of X in original call: 0x

   Answer: 9

   Explanation
   Since we are told that the original call to the **quicksort** procedure is from a branch instruction at address 0×948, we know that the LP register from that initial call holds the address of the instruction following that branch which is 0×94C. If we search our stack trace for LP = 0×94C, we see that the topmost stack frame corresponds to that original call to **quicksort**. The arguments in that stack frame are the arguments to the original call to **quicksort**. X is the value of right which is 9.

7. What were the contents of R4 when the original call to **quicksort(Y, 0, X)** was made?
   Contents of R4 at original call: 0x

   Answer: 4

   Explanation
   Since we know that the top stack frame corresponds to the original call to **quicksort**, we know that the original contents of register R4 was 4.

8. What is the address of the instruction tagged **bb:** in the program?
   HEX value of bb: 0x

   Answer: F48

   Explanation
   Looking at the various stack frames in our stack trace, we see that in one of the calls to quicksort LP = 0xF24 and in the other LP = 0xF48. The instruction tagged **bb** corresponds to the second call to **quicksort** where LP = 0xF48.

Submit

Answers are displayed within the problem

Stacks and Procedures: 2

11 points possible (ungraded)

The following C program implements a function (ffo) of two arguments, returning an integer result. The assembly code for the procedure is shown on the right, along with a partial stack trace showing the execution of **ffo(0xDECAF,0)**. The execution has been halted just as the Beta is about to execute the instruction labeled **rtn**, i.e., the value of the Beta's program counter is the address of the first instruction in POP(R1). In

$0x000F$
$0x001B$
$0x0208$
$0x012C$
$0x001B$

```
ffo:     PUSH(LP)
         PUSH(BP)
         MOVE(SP,BP)
         PUSH(R1)

         LD(BP,-16,
         LD(BP,-12,
```

Calculator

the C code below, note that "v>>1" is a logical right shift of the value v by 1 bit.

```
// bit position of left-most 1
int ffo(unsigned v, int b) {
    if (v == 0) ???;
    else return ffo(v>>1,b+1);
}
```

$0x0010$
$0x000D$
$0x0208$
$0x0140$
$0x000D$
$0x0011$
$0x0006$
$0x0208$
$0x0154$
$BP \rightarrow$ $0x0006$
$0x0012$
$0x0003$

```
xxx:    BEQ(R1,rtn)

        ADDC(R0,1,R0)
        PUSH(R0)
        SHRC(R1,1,R1)
        PUSH(R1)
        BR(ffo,LP)
        DEALLOCATE(2)

rtn:    POP(R1)
        MOVE(BP,SP)
        POP(BP)
        POP(LP)
        JMP(LP)
```

1. Examining the assembly language for ffo, what is the appropriate C code for ??? in the C representation for ffo?

   C code for ???:

   - return v
   - return b ✔
   - return 0
   - return ffo(v>>1,b)

   Explanation

   If we follow the assembly code, we see that the two **LD** operations load the arguments b into R0 and v into R1. At label 'xxx', we then check if R1 = 0 and if so return. The value returned is always in R0 which was just loaded with b, so that means that we are returning b when v = 0.

2. What value will be returned from the procedure call ffo(3,100)?

   Value returned from procedure call ffo(3,100):

   Answer: 102

   Explanation

   ffo(3,100) = ffo(1,101) = ffo(0,102) = 102.

3. What are the values of the arguments in the call to ffo from which the Beta is about to return? Please express the values in hex or write "CAN'T TELL" if the value cannot be determined.

   Value of argument v or "CAN'T TELL": 0x

   Answer: 6

   Value of argument b or "CAN'T TELL": 0x

   Answer: 11

   Explanation

   The stack frame for one call to **ffo** is:

   b
   v
   LP
   BP
   $R1$

   The two argument (v, b) are put on the stack in reverse order. Then we store the LP, then the BP and then any registers that we will use to compute intermediate data (R1) so that they can be restored at the end of the procedure call.

   We know that the value immediately above the current BP, is the old BP. Using that information, we can fill in the elements of each stack frame in our trace as follows.

   $0x000F$ b
   $0x001B$ v
   $0x0208$ LP

Calculator

	$0x012C$	BP
	$0x001B$	R1
	$0x0010$	b
	$0x000D$	v
	$0x0208$	LP
	$0x0140$	BP
	$0x000D$	R1
	$0x0011$	b
	$0x0006$	v
	$0x0208$	LP
	$0x0154$	BP
$BP \rightarrow$	$0x0006$	R1
	$0x0012$	
	$0x0003$	

The program stops just before we execute the instruction labelled **rtn**, this means that we have not yet popped R1 off of the stack. So we are at our bottom-most stack frame where v = 0×6 and b = 0×11.

4. Determine the specified values at the time execution was halted. Please express each value in hex or write "CAN'T TELL" if the value cannot be determined.

Value in R1 or "CAN'T TELL": 0x

Answer: 3

Value in BP or "CAN'T TELL": 0x

Answer: 168

Value in LP or "CAN'T TELL": 0x

Answer: 208

Value in SP or "CAN'T TELL": 0x

Answer: 16C

Value in PC or "CAN'T TELL": 0x

Answer: 20C

Explanation
Using the labeled stack trace that we just produced in part C, we can also determine the addresses where these stack trace elements are stored in memory by making use of the stored BP values.
Starting from the bottom of the trace, we find an old BP = 0×0154. The old BP points to the previous saved copy of R1, so we can label the previous R1 element, 0×000D as being at address 0×0154. From there, we can add/subtract 4 to determine the remaining addresses.
The resulting labeled stack with addresses is:

Hex Value	Variable	Hex address
$0x000F$	b	
$0x001B$	v	
$0x0208$	LP	
$0x012C$	BP	
$0x001B$	R1	
$0x0010$	b	
$0x000D$	v	

Calculator

	$0x000D$	v	
	$0x0208$	LP	
	$0x0140$	BP	
	$0x000D$	R1	0×154
	$0x0011$	b	0×158
	$0x0006$	v	0×15C
	$0x0208$	LP	0×160
	$0x0154$	BP	0×164
$BP \rightarrow$	$0x0006$	R1	0×168
	$0x0012$		0×16C
	$0x0003$		

This tells us that BP = 0×168, and LP = 0×208. We also know that just before executing the instruction at label **rtn**, we have not yet popped R1, so that means that the SP is one location below the current BP, and therefore SP = 0×16C. R1 contains the value of the previously popped R1, which means that if we are about to pop the value 0×0006 into R1, the previous value popped into R1 is 0×0006 shifted to the right by 1 which is 0×0003. Finally, we need to determine the value of PC. PC points to the **rtn** instruction. We know that LP stores the return address from the call to ffo (the address of the DEALLOCATE(2) instruction), since LP = 0208, we know that the DEALLOCATE instruction is at address 0×208. This means that the **rtn** label is at address 0×20C, so PC = 0×020C.

5. What is the address of the BR instruction for the original call to ffo(0xDECAF,0)? Please express the value in hex or “CAN'T TELL”.
   Address of the original BR, or “CAN'T TELL”: 0x

   Answer: CAN'T TELL

   Explanation
   From the stack trace we see that all the stored LP values are the same, 0×0208. We know that this is the return address of the recursive call to ffo, which means that we don't have any information in this stack trace about the return address of the original call to ffo, so the answer is CAN'T TELL.

6. A 6.004 student modifies ffo by removing the DEALLOCATE(2) macro in the assembly compilation of the ffo procedure, reasoning that the MOVE(BP,SP) will perform the necessary adjustment of stack pointer. She runs a couple of tests and verifies that the modified ffo procedure still returns the same answer as before. Does the modified ffo obey our procedure call and return conventions?
   Does modified ffo obey call/return conventions?

   No Answer: No

   Explanation
   Our procedure call and return conventions require all registers to be restored to their original value except for R0 which should contain the correct answer. If the DEALLOCATE(2) macro is removed from the code, then the value of R1 would not be restored correctly. The value of v would be popped into R1 upon each return sequence of ffo.

Submit

Answers are displayed within the problem

Stacks and Procedures: 3

13/13 points (ungraded)

It was mentioned in lecture that recursion became a popular programming construct following the adoption of the stack as a storage allocation mechanism, ca. 1960. But the Greek mathematician Euclid, always ahead of his time, used recursion in 300 BC to compute the greatest common divisor of two integers. His elegant algorithm, translated to C from the ancient greek, is shown below:

```
int gcd(int a, int b) {
   if (a == b) return a;
   if (a > b) return gcd(a-b, b);
```

Calculator

```
    else return gcd(a, b-a);
}
```

The procedure **gcd(a, b)** takes two positive integers **a** and **b** as arguments, and returns the greatest positive integer that is a factor of both **a** and **b**.

Note that the base case for this recursion is when the two arguments are equal (== in C tests for equality), and that there are two recursive calls in the body of the procedure definition.

Although Euclid's algorithm has been known for millennia, a recent archeological dig has uncovered a new document which appears to be a translation of the above C code to Beta assembly language, written in Euclid's own hand. The Beta code is known to work properly, and is shown below.

```
gcd:    PUSH(LP)
        PUSH(BP)
        MOVE(SP, BP)
        PUSH(R1)
        PUSH(R2)
        LD(BP, -12, R0)
        LD(BP, -16, R1)
        CMPEQ(R0, R1, R2)
        BT(R2, L1)
        CMPLE(R0, R1, R2)
xxx:    BT(R2, L2)
        PUSH(R1)
        SUB(R0, R1, R2)
        PUSH(R2)
        BR(gcd, LP)
        DEALLOCATE(2)
        BR(L1)

L2:     SUB(R1, R0, R2)
        PUSH(R2)
        PUSH(R0)
        BR(gcd, LP)
        DEALLOCATE(2)

L1:     POP(R2)
        POP(R1)
yyy:    MOVE(BP, SP)
        POP(BP)
        POP(LP)
        JMP(LP)
```

1. Give the 32-bit binary translation of the **BT(R2,L2)** instruction at the label **xxx**

   opcode (6 bits): 0b

   011101 ✔ Answer: 011101

   Rc (5 bits): 0b

   11111 ✔ Answer: 11111

   Ra (5 bits): 0b

   00010 ✔ Answer: 00010

   literal (16 bits): 0b

   00000000000010(✔ Answer: 0000000000001000

   Explanation

   The opcode for the **BT** instruction which is equivalent to a **BNE** instruction is 011101.

   Since there is no Rc specified in the instruction, it uses R31 so that the return address will just get

Calculator

Since there is no Rc specified in the instruction, it uses R31 so that the return address will just get ignored. To select R31 Rc = 11111.
The instruction specifies that Ra = R2, so Ra = 00010.
The literal in the branch instruction encodes the distance between PC + 4 and the destination address in words. Here PC + 4 is the address of the instruction following the **xxx** label, namely the address of the **PUSH(R1)**. Recall that the PUSH and POP are macros, each of which actually represents 2 instructions. Taking this into consideration, we see that the instruction at label L2 is 8 instructions away from the instruction following the **xxx** label, so the literal is 0000000000001000.

2. One historian studying the code, a Greek major from Harvard, questions whether the **MOVE(BP, SP)** instruction at **yyy** is really necessary. If this instruction were deleted from the assembly language source and re-translated to binary, would the shorter Beta program still work properly?
Still works?

Yes ✔ Answer: Yes

Explanation
The implementation of the gcd procedure does not store any temporary variables on the stack. This means that after popping the saved registers R2 and R1, the BP and SP are both pointing to the same location in the stack so the **MOVE(BP, SP)** instruction in this case is is unnecessary.

```
main:   CMOVE(0x104, SP)
        PUSH(R17)
        PUSH(R18)
        BR(gcd, LP)
zzz:    HALT()
```

At a press conference, the archeologists who discovered the Beta code give a demonstration of it in operation. They use the test program shown above to initialize SP to hex **0×104**, and call gcd with two positive integer arguments from **R17** and **R18**. Unfortunately, the values in these registers have not been specified.

Address in Hex	Data in Hex
$100:$	104
$104:$	18
$108:$	9
$10C:$	$D8$
$110:$	$D4$
$114:$	EF
$118:$	BA
$11C:$	F
$120:$	9
$124:$	78
$128:$	114
$12C:$	18
$130:$	F
$134:$	6
$138:$	9
$13C:$	78
$140:$	$12C$
$144:$	F
$148:$	6
$14C:$	6
$150:$	3
$154:$	58
$158:$	144
$SP \rightarrow 15C:$	6

They start their program on a computer designed to approximate the computers of Euclid's day (think of Moore's law extrapolated back to 300 BC!), and let it run for a while. Before the call to gcd returns, th

Calculator

stop the computation just as the instruction at **yyy** is about to be executed, and examine the state of the processor.

They find that **SP** (the stack pointer) contains **0x15C**, and the contents of the region of memory containing the stack as shown **(in HEX)** to the right.

You note that the instruction at **yyy**, about to be executed, is preparing for a return to a call from gcd(a,b).

3. What are the values of **a** and **b** passed in the call to gcd which is about to return? Answer in HEX.

Args to current call: a=0x

3 ✔ Answer: 3

b = 0x

6 ✔ Answer: 6

Explanation

To answer the stack related questions, the first thing to do is to label our stack. Based on the code, we know that a single stack frame contains the following elements:

b

a

LP

BP

$R1$

$R2$

We also know that execution is stopped just before the instruction at label **yyy** is executed. This means that we have just popped **R2** and **R1**, and the **BP** and **SP** are pointing to the same location because there are no temporary variables. It also means that the stack location just above the current **SP** and **BP** is the stored **BP**. Working backwards, we can label our full stack trace as follows:

Address in Hex	Data in Hex	
$100:$	104	
$104:$	18	b
$108:$	9	a
$10C:$	$D8$	LP
$110:$	$D4$	BP
$114:$	EF	R1
$118:$	BA	R2
$11C:$	F	b
$120:$	9	a
$124:$	78	LP
$128:$	114	BP
$12C:$	18	R1
$130:$	F	R2
$134:$	6	b
$138:$	9	a
$13C:$	78	LP
$140:$	$12C$	BP
$144:$	F	R1
$148:$	6	R2
$14C:$	6	b
$150:$	3	a
$154:$	58	LP
$158:$	144	BP
$SP \rightarrow 15C:$	6	

This labelling shows us that the values of **a** and **b** passed in to the most recent call to **gcd** are **a=0x3** **b=0x6**.

Calculator

4. What are the values of **a** and **b** passed in the *original* call to gcd, from registers **R17** and **R18**? Answer in HEX.
   Args to original call: a=0x

   9 ✔ Answer: 9

   b = 0x

   18 ✔ Answer: 18

   Explanation
   The labeled stack shows that the original values of **a** and **b** were **a=0×9** and **b=0×18**.

5. What is the address corresponding to the tag **zzz**: of the **HALT()** following the original call to **gcd**?
   Address of zzz: (HEX): 0x

   D8 ✔ Answer: D8

   Explanation
   The first stored LP holds the return address of the original call to gcd. This return address is the same as address corresponding to label **zzz**, so **zzz** = 0xD8.

6. What is the address corresponding to the tag **L1**: in the assembly b for **gcd**?
   Address of L1: (HEX): 0x

   7C ✔ Answer: 7C

   Explanation
   Gcd is initially called with **a** = 0×9 and **b** = 0×18. The result **CMPLE(R0, R1, R2)** is that R2 = 1 because a <= b, so the code branches to L2. This means that the next LP that gets stored on the stack is the address of the instruction above L1. So L1 = 0×78 + 4 = 0×7C.

7. What value will be returned (in R0) as the result of the original call to **gcd**?
   Value returned to original caller: (HEX): 0x

   3 ✔ Answer: 3

   Explanation
   The greatest common divisor of 0×18 = 24 and 0×9 = 9 is 3.

8. What was the value of R2 at the time of the original call to gcd?
   Original value in R2: (HEX): 0x

   BA ✔ Answer: BA

   Explanation
   The original value in R2 is the first R2 value stored on the stack and that is 0xBA.

Submit

Answers are displayed within the problem

Stacks and Procedures: 4

15/15 points (ungraded)
You are given the following listing of a C program and its translation to Beta assembly code:

```
int f(int x, int y)
  int a = x - 1; b = x + y;
  if (x == 0) return y;
  return f(a, ???)
```

```
f:    PUSH(LP)
```

Calculator

```
        PUSH(BP)
mm:     MOVE(SP, BP)
        PUSH(R1)
        PUSH(R2)
        LD(BP, -16, R0)
yy:     LD(BP, -12, R1)
        BEQ(R1, xx)
        SUBC(R1, 1, R2)
        ADD(R0, R1, R1)
        PUSH(R1)
        PUSH(R2)
        BR(f, LP)
zz:     DEALLOCATE(2)
        LD(BP, -16, R1)
        ADD(R1, R0, R0)
        PUSH(R0)
ww:     PUSH(R2)
        BR(f, LP)
        DEALLOCATE(2)
xx:     POP(R2)
        POP(R1)
        POP(BP)
        POP(LP)
        JMP(LP)
```

1. Fill in the binary value of the **LD** instruction stored at the location tagged **yy** in the above program.
   opcode (6 bits): 0b
   011000
   Answer: 011000

   Rc (5 bits): 0b
   00001
   Answer: 00001

   Ra (5 bits): 0b
   11011
   Answer: 11011

   literal (16 bits): 0b
   1111111111110100
   Answer: 1111111111110100

   Explanation
   The LD instruction tagged **yy** is **LD(BP, -12, R1)**.
   The opcode for the **LD** instruction is 011100.
   Register Rc is R1, or 00001 when encoded using 5 bits.
   Register Ra is the BP register which is register 27, or 11011.
   The literal is -12 which is 1111111111110100 using 16 bits of binary.

2. Suppose the MOVE instruction at the location tagged **mm** were eliminated from the above program. Would it continue to run correctly?
   Still works fine?
   - ( ) Yes
   - ( ) Can't Tell
   - (•) No

   Explanation
   The BP must be updated to the new value of the SP otherwise the arguments that will be fetched wi incorrect.

Calculator

3. What is the missing expression designated by **???** in the C program above.

- b
- y
- y + f(a,b)
- f(a,b)

Explanation
If x!=0, then the BEQ to **xx** is not taken, and instead f is called again with the arguments (a,b). The result of that is returned in R0. In the zz portion of the code y is added to R0, to produce the second argument for the final call to f. So that second argument is y + f(a,b).

The procedure f is called from location 0xFC and its execution is interrupted during a recursive call to f, just prior to the execution of the instruction tagged **xx**. The contents of a region of memory, including the stack, are shown to the left.

NB: All addresses and data values are shown in hex. The **BP** register contains **0×494**, and **SP** contains **0×49C**.

Address in Hex	Contents in Hex
448	2
$44C$	4
450	7
454	3
458	2
$45C$	100
460	$D4$
464	3
468	4
$46C$	5
470	1
474	50
478	$???$
$47C$	5
480	1
484	B
488	0
$48C$	70
490	$47C$
$BP \rightarrow 494$	5
498	0
$SP \rightarrow 49C$	

4. What are the arguments to the *most recent* active call to **f**?
Most recent arguments (HEX): x = 0x

0

Answer: 0

y = 0x

B

Answer: B

Explanation
If we label our stack with the elements of the stack frame that are represented by each location, we the following labelled stack table:

Calculator

Address in Hex	Contents in Hex	
448	2	
$44C$	4	
450	7	
454	3	y
458	2	x
$45C$	100	LP
460	$D4$	BP
464	3	R1
468	4	R2
$46C$	5	y
470	1	x
474	50	LP
478	$???$	BP
$47C$	5	R1
480	1	R2
484	B	y
488	0	x
$48C$	70	LP
490	$47C$	BP
$BP \rightarrow 494$	5	R1
498	0	R2
$SP \rightarrow 49C$		

The most recent active call to f uses the x and y at locations 0×488 and 0×484 as its arguments, so x = 0×0 and y = 0xB.

5. What value is stored at location **0×478**, shown as **???** in the listing to the left?
Contents 0×478 (HEX): 0x

464

Answer: 464

Explanation
For each stack frame, the base pointer points to the location that will hold R1. This means that the BP value stored at address 0×478 corresponds to the previous value of the BP which is 0×464.

6. What are the arguments to the *original* call to **f**?
Original arguments (HEX): x = 0x

2

Answer: 2

y = 0x

3

Answer: 3

Explanation
We are told that the original call to f is made from address 0xFC which means that the original LP pointed to the address immediately after that which is 0×100. The arguments that correspond to the stack frame whose LP value is 0×100 are x=0×2 and y=0×3.

7. What value is in the **LP** register?
Contents of LP (HEX): 0x

70

Answer: 70

Explanation
At the time execution is halted the value of the LP register is the same as the last LP value that was stored on the stack which is 0×70.

8. What value was in **R1** at the time of the original call?
Contents of R1 (HEX): 0x

Calculator

Contents of R1 (HEX): 0x

3

✔ Answer: 3

Explanation
The R1 stored in the first stack frame, at address 0×464, corresponds to the original value of R1. This value is 3.

9. What value is in **R0**?
   Value currently in R0 (HEX): 0x

   B

   ✔ Answer: B

   Explanation
   Since execution was halted at label **xx**, the value currently in R0 is the result of the most recent call to f whose arguments were x=0 y=0xB. When x = 0, the value of y is returned in R0, so R0 = 0xB.

10. What is the hex address of the instruction tagged **ww**
    Address of ww (HEX): 0x?

    64

    ✔ Answer: 64

    Explanation
    Based on the values of the stored LPs, we know that address 0×70 corresponds to the instruction immediately after the second recursive call to f which is the DEALLOCATE(2) instruction just above label **xx**. Counting backwards, this means that the BR instruction was at 0×6C, and since the PUSH is actually a macro corresponding to 2 instructions, that means that the address of label **ww** is 0×64.

Submit

Answers are displayed within the problem

Stacks and Procedures: 5

17 points possible (ungraded)
The **wfps** procedure determines whether a string of left and right parentheses is well balanced, much as your Turing machine of Lab 4 did. Below is the code for the **wfps** (“well-formed paren string”) procedure in C, as well as its translation to Beta assembly code.

```
int STR[100];               // string of parens

int wfps(int i,             // current index in STR
  int n)                    // LPARENs to balance

{ int c = STR[i];           // next character
  int new_n;                // next value of n
  if (c == 0)               // if end of string,
    return (n == 0);        //   return 1 iff n == 0
  else if (c == 1)          // on LEFT PAREN,
    new_n = n+1;            //    increment n
  else {                    // else must be RPAREN
    if (n == 0) return 0;   // too many RPARENS!
      xxxxx; }              // MYSTERY CODE!
  return wfps(i+1, new_n);  // and recurse.
}
```

```
STR:  . = .+4*100
wfps: PUSH(LP)
      PUSH(BP)
      MOVE(SP, BP)
      ALLOCATE(1)
      PUSH(R1)
      LD(BP, -12, R0)
      MULC(R0, 4, R0)
      LD(R0, STR, R1)
      ST(R1, 0, BP)
      BNE(R1, more)
```

Calculator

```
      BNE(R1, more)
      LD(BP, -16, R0)
      CMPEQC(R0, 0, R0)
rtn:  POP(R1)
      MOVE(BP, SP)
      POP(BP)
      POP(LP)
      JMP(LP)
more: CMPEQC(R1, 1, R0)
      BF(R0, rpar)
      LD(BP, -16, R0)
      ADDC(R0, 1, R0)
      BR(par)
rpar: LD(BP, -16, R0)
      BEQ(R0, rtn)
      ADDC(R0, -1, R0)
par:  PUSH(R0)
      LD(BP, -12, R0)
      ADDC(R0, 1, R0)
      PUSH(R0)
      BR(wfps, LP)
      DEALLOCATE(2)
      BR(rtn)
```

wfps expects to find a string of parentheses in the integer array stored at **STR**. The string is encoded as a series of **32-bit integers** having values of

- **1** to indicate a left paren,
- **2** to indicate a right paren, or
- **0** to indicate the end of the string.

These integers are stored in consecutive 32-bit locations starting at the address **STR**.

wfps is called with two arguments:

1. The first, **i**, is the index of the start of the part of **STR** that this call of **wfps** should examine. Note that indexes start at 0 in C. For example, if **i** is 0, then **wfps** should examine the entire string in **STR** (starting at the first character, or **STR[0]**). If **i** is 4, then **wfps** should ignore the first four characters and start examining **STR** starting at the fifth character (the character at **STR[4]**).
2. The second argument, **n**, is zero in the original call; however, it may be nonzero in recursive calls.

wfps returns 1 if the part of **STR** being examined represents a string of balanced parentheses if **n** additional left parentheses are prepended to its left, and returns 0 otherwise.

Note that the compiler may use some simple optimizations to simplify the assembly-language version of the code, while preserving equivalent behavior.

The C code is incomplete; the missing expression is shown as **xxxx**.

1. Fill in the binary value of the instruction stored at the location tagged **more** in the above assembly-language program.
   opcode (6 bits): 0b

   Rc (5 bits): 0b

   Ra (5 bits): 0b

   literal (16 bits): 0b

Calculator

2. Is the variable c from the C program stored as a local variable in the stack frame?

- Yes
- No

If so, give its (signed) offset from BP; else select "NA".

- $BP - 16$
- $BP - 12$
- $BP - 8$
- $BP + 0$
- $BP + 4$
- $BP + 8$
- NA

3. Is the variable new_n from the C program stored as a local variable in the stack frame?

- Yes
- No

If so, give its (signed) offset from BP; else select "NA".

- $BP - 16$
- $BP - 12$
- $BP - 8$
- $BP + 0$
- $BP + 4$
- $BP + 8$
- NA

4. What is the missing C source code represented by xxxxx in the given C program?

- n = n + 1
- n = n - 1
- new_n = n + 1
- new_n = n - 1

Calculator

◯ new_n = n

The procedure **wfps** is called from an external procedure and its execution is interrupted during a recursive call to **wfps**, just prior to the execution of the instruction labeled **rtn**. The contents of a region of memory are shown below. At this point, **SP** contains 0×1D8, and **BP** contains 0×1D0.

NOTE: All addresses and data values are shown in hexadecimal.

Address in Hex	Contents in Hex
188:	7
18C:	$4A8$
190:	0
194:	0
198:	458
19C:	$D4$
1A0:	1
1A4:	$D8$
1A8:	1
1AC:	1
1B0:	$3B8$
1B4:	$1A0$
1B8:	2
1BC:	1
1C0:	0
1C4:	2
1C8:	$3B8$
1CC:	$1B8$
BP⟶1D0:	2
1D4:	2
SP⟶1D8:	0

5. What are the arguments to the *most recent* active call to **wfps**?
Most recent arguments (HEX): i = 0x

n = 0x

6. What are the arguments to the *original* call to **wfps**?
Original arguments (HEX): i = 0x

n = 0x

7. What value is in **R0** at this point?
Contents of R0 (HEX): 0x

8. How many parens (left and right) are in the string stored at STR (starting at index 0)? Give a number, or "**CAN'T TELL**" if the number can't be determined from the given information.
Length of string, or "CAN'T TELL":

◯ 0

◯ 1

◯ 2

Calculator

2

3

Can't Tell

9. What is the hex address of the instruction tagged **par**?
   Address of par (HEX): 0x

10. What is the hex address of the **BR** instruction that called **wfps** originally?
    Address of original call (HEX): 0x

Submit

Stacks and Procedures: 6

13 points possible (ungraded)

You've taken a summer internship with BetaSoft, the worlds largest supplier of Beta software. They ask you to help with their library procedure **sqr(j)**, which computes the square of a non-negative integer argument **j**. Because so many Betas don't have a multiply instruction, they have chosen to compute **sqr(j)** by adding up the first **j** odd integers, using the C code below and its translation to Beta assembly language to the left.

```
int sqr(j) {
   int s = 0;
   int k = j;
   while (k != 0) {
      s = s + nthodd(k);
      k = k - 1;
   }
   return s;
}

int nthodd(n) {
   if (n == 0) return 0;
   return ???;
}
```

```
sqr:     PUSH (LP)
         PUSH (BP)
         MOVE (SP, BP)
         ALLOCATE(2)
         PUSH (R1)
         ST(R31, 0, BP)
         LD (BP, -12, R0)
         ST(R0, 4, BP)
loop:    LD(BP, 4, R0)
         BEQ(R0, done)
         PUSH(R0)
         SUBC(R0, 1, R0)
         ST(R0, 4, BP)
         BR(nthodd, LP)
         DEALLOCATE(1)
         LD(BP, 0, R1)
         ADD(R0, R1, R1)
         ST(R1, 0, BP)
         BR(loop)
done:    LD(BP, 0, R0)
         POP(R1)
         DEALLOCATE(2)
         MOVE(BP, SP)
         POP(BP)
         POP(LP)
         JMP(LP)

nthodd:  PUSH (LP)
         PUSH (BP)
         MOVE (SP, BP)
         LD (BP, -12, R0)
         BEQ(R0, zero)
         ADD(R0, R0, R0)
         SUBC(R0, 1, R0)
zero:    MOVE(BP, SP)
         POP(BP)
         POP(LP)
         JMP(LP)
```

You notice that the **sqr** procedure takes an integer argument j, and declares two local integer variables s and k (initialized to zero and j, respectively).

The body of **sqr** is a loop that is executed repeatedly, decrementing the value of k at each iteration, until k reaches zero. Each time through the loop, the local variable s incremented by the value of the kth odd integer, a value that is computed by an auxiliary procedure **nthodd**.

1. What is the missing expression shown as **???** in the C code defining **nthodd** above?
   What is the missing expression denoted ??? in above C code:

2. What variable in the C code, if any, is loaded into R0 by the LD instruction tagged **loop**? Answer "none" if no such value is loaded by this instruction.
   Value loaded by instruction at loop:, or "none":

Calculator

Using a small test program to run the above assembly code, you begin computing sqr(X) for some

Using a small test program to run the above assembly code, you begin computing **sqr(X)** for some positive integer **X**, and stop the machine during its execution. You notice, from the value in the PC, that the instruction tagged **zero** is about to be executed. Examining memory, you find the following values in a portion of the area reserved for the Beta's stack.

F0:	$F4$
F4:	5
F8:	EC
FC:	$D4$
100:	15
104:	1
108:	$DECAF$
10C	2
110	$4C$
114	100
$BP$118: $\rightarrow$	0

NB: All values are in HEX! Give your answers in hex, or write "CAN'T TELL" if you can't tell.

You notice that BP contains the value **0×118**.

3. What argument (in hex) was passed to the current call to **nthodd**? Answer "CAN'T TELL" if you can't tell.
   HEX Arg to nthodd, or "CAN'T TELL": 0x
4. What is the value **X** that was passed to the original call to **sqr(X)**? Answer "CAN'T TELL" if you can't tell.
   HEX Arg X to sqr, or "CAN'T TELL": 0x
5. What is the hex value in **SP?** Answer "CAN'T TELL" if you can't tell.
   HEX Value in SP, or "CAN'T TELL": 0x
6. What is the current value of the variable **k** in the C code for sqr? Answer "CAN'T TELL" if you can't tell.
   HEX Value of k in sqr, or "CAN'T TELL": 0x
7. The test program invoked **sqr(X)** using the instruction BR(sqr,LP). What is the address of that instruction? Answer "CAN'T TELL" if you can't tell.
   HEX Address of BR instruction that called sqr, or "CAN'T TELL": 0x
8. What value was in R1 at the time of the call to **sqr(X)**? Answer "CAN'T TELL" if you can't tell.
   HEX Value in R1 at call to sqr, or "CAN'T TELL": 0x

Your boss at BetaSoft, Les Ismoore, suspects that some of the instructions in the Beta code could be eliminated, saving both space and execution time. He hands you an annotated listing of the code (shown below), identical to the original assembly code but with some added tags.

```
sqr:    PUSH (LP)
        PUSH (BP)
        MOVE (SP, BP)
        ALLOCATE(2)
        PUSH (R1)
        ST(R31, 0, BP)
        LD (BP, -12, R0)
        ST(R0, 4, BP)
loop:   LD(BP, 4, R0)
        BEQ(R0, done)
        PUSH(R0)
        SUBC(R0, 1, R0)
        ST(R0, 4, BP)
        BR(nthodd, LP)
        DEALLOCATE(1)
```

Calculator

```
        LD(BP, 0, R1)
        ADD(R0, R1, R1)
        ST(R1, 0, BP)
        BR(loop)
done:   LD(BP, 0, R0)
        POP(R1)
q1:     DEALLOCATE(2)
        MOVE(BP, SP)
        POP(BP)
        POP(LP)
        JMP(LP)
nthodd: PUSH (LP)
q5:     PUSH (BP)
q2:     MOVE (SP, BP)
        LD (BP, -12, R0)
        BEQ(R0, zero)
        ADD(R0, R0, R0)
        SUBC(R0, 1, R0)
zero:   MOVE(BP, SP)
        POP(BP)
        POP(LP)
        JMP(LP)
```

Les proposes several optimizations, each involving just the deletion of one or more instructions from the annotated code. He asks, in each case, whether the resulting code would still work properly. For each of the following proposed deletions, select “OK” if the code would still work after the proposed deletion, or “NO” if not. For each question, **assume that the proposed deletion is the ONLY change** (i.e., you needn’t consider combinations of proposed changes).

9. Delete the instruction tagged **q1**.
Proposed deletion OK or NO?

- OK
- NO

10. Delete the instruction tagged **q2**.
Proposed deletion OK or NO?

- OK
- NO

11. Delete the instruction tagged **loop**.
Proposed deletion OK or NO?

- OK
- NO

12. Delete the instruction tagged **zero**.
Proposed deletion OK or NO?

- OK
- NO

After some back-and-forth with Les, he proposes to replace **nthodd** with a minimalist version that avoids much of the standard procedure linkage boilerplate:

```
nthodd: LD (SP, NNN, R0)
        BEQ(R0, zero)
        ADD(R0, R0, R0)
        SUBC(R0, 1, R0)
zero:   JMP(LP)
```

Calculator

He's quite sure this code will work, but doesn't know the appropriate value for **NNN**.

13. What is the proper value for the constant **NNN** in the shortened version of **nthodd**?

Appropriate value for NNN (in decimal):

Submit

Stacks and Procedures: 7

15 points possible (ungraded)

You are given the following listing of a C program and its translation to Beta assembly code:

```
// Mystery function:
int f(int x, int y) {
  int a = (x+y) >> 1;
  if (a == 0) return y;
  else return ???;
}
```

```
f:   PUSH(LP)
     PUSH(BP)
     MOVE(SP, BP)
     PUSH(R1)
     PUSH(R2)
     LD(BP, -12, R1)
     LD(BP, -16, R0)
     ADD(R0, R1, R2)
     SRAC(R2, 1, R2)

xx:  BEQ(R2, bye)

     SUB(R1, R2, R1)
     PUSH(R1)
     PUSH(R0)

yy:  BR(f, LP)
     DEALLOCATE(2)
     ADD(R2, R0, R0)

bye: POP(R2)
     POP(R1)
zz:  MOVE(BP, SP)
     POP(BP)
     POP(LP)
     JMP(LP)
```

(Recall that a >> b means a shifted b bits to the right, propagating – ie, preserving -- sign)

1. Fill in the binary value of the BR instruction stored at the location tagged **yy** in the above program.

   opcode (6 bits): 0b

   Rc (5 bits): 0b

   Ra (5 bits): 0b

   literal (16 bits): 0b

2. Suppose the MOVE instruction at the location tagged **zz** were eliminated from the above program. Would it continue to run correctly?

   Still works fine?

   - YES
   - NO

3. What is the missing expression designated by **???** in the C program above.

   - f(y, a)
   - a + f(y, x)

Calculator

- a + f(y, x-a)
- f(x, -a)
- f(y, -a)

The procedure **f** is called from an external procedure and its execution is interrupted during a recursive call to **f**, just prior to the execution of the instruction tagged **bye**. The contents of a region of memory are shown below.

NB: All addresses and data values are shown in hex. The **BP** register contains **0×250**, **SP** contains **0×258**, and **R0** contains **0×5**.

204:	CC
208:	4
20C:	7
210:	6
214:	7
218:	$E8$
21C:	$D4$
220:	BAD
224	$BABE$
228	1
22C	6
230	54
234	
238	1
23C	6
240	3
244	1
248	54
24C	238
$BP$250: $\rightarrow$	3
254	3
$SP$258: $\rightarrow$	-1

4. What are the arguments to the *most recent* active call to **f**?
   Most recent arguments (HEX): x = 0x

   y = 0x

5. Fill in the missing value in the stack trace.
6. What are the arguments to the *original* call to **f**?
   Original arguments (HEX): x = 0x

   y = 0x

7. What value is in the **LP** register?
   Contents of LP (HEX): 0x

Calculator

8. What value was in **R1** at the time of the original call?
   Contents of R1 (HEX): 0x

9. What value will be returned in R0 as the value of the original call? [HINT: You can figure this out without getting the C code right!].
   Value returned to original caller (HEX): 0x

10. What is the hex address of the instruction tagged **yy**?
    Address of yy (HEX): 0x

Submit

Stacks and Procedures: 8

15 points possible (ungraded)

You are given the following listing of a C program and its translation to Beta assembly code:

```
int f(int x, int y) {
  int a = (x+y) >> 2;
  if (a == 0) return x;
  else return y + f(a, x+a);
}
```

```
f:      PUSH(LP)
        PUSH(BP)
        MOVE(SP, BP)
        PUSH(R1)
        LD(BP, -12, R0)
        LD(BP, -16, R1)
        ADD(R0, R1, R1)
        SRAC(R1, 2, R1)
laby:   BEQ(R1, labx)

        ADD(R0, R1, R0)
        PUSH(R0)
        PUSH(R1)
        BR(f, LP)
        DEALLOCATE(2)

labz:   LD(BP, -16, R1)
        ADD(R1, R0, R0)

labx:   POP(R1)
        MOVE(BP, SP)
        POP(BP)
        POP(LP)
        JMP(LP)
```

(Recall that a >> b means a shifted b bits to the right, propagating – ie, preserving -- sign)

1. Fill in the binary value of the BEQ instruction stored at the location tagged **laby** in the above program.
   opcode (6 bits): 0b

   Rc (5 bits): 0b

   Ra (5 bits): 0b

   literal (16 bits): 0b

2. Is a location reserved for the argument **x** in **f**'s stack frame? Give its (signed) offset from **BP**, or **NONE** if there is no such location.
   Offset of x (in decimal), or "NONE":

3. Is a location reserved for the variable **a** in **f**'s stack frame? Give its (signed) offset from **BP**, or **NONE** if there is no such location.
   Offset of variable a, or "NONE":

Calculator

The procedure **f** is called from an external procedure and its execution is interrupted during a recursive call to **f**, just prior to the execution of the instruction tagged **labz**. The contents of a region of memory are shown below.

NB: All addresses and data values are shown in hex. The **SP** contains **0×1C8**.

184:	4
188:	7
18C:	3
190:	5
194:	$D0$
198:	$D4$
19C:	$D8$
1A0:	7
1A4	2
1A8	$4C$
1AC	$19C$
1B0	2
1B4	4
1B8	2
1BC	$4C$
1C0	$1B0$
1C4	2
$SP \rightarrow$ 1C8	3

4. What are the arguments to the *most recent* active call to **f**?
   Most recent arguments (HEX): x = 0x

   y = 0x

5. What are the arguments to the *original* call to **f**?
   Original arguments (HEX): x = 0x

   y = 0x

6. What value is in the **BP** register?
   Contents of BP (HEX): 0x

7. What value is in **R1** prior to the execution of the **LD** at **labz**?
   Contents of R1 (HEX): 0x

8. What value will be loaded into **R1** by the instruction at **labz** if program execution continues?
   Contents of R1 (HEX): 0x

9. What is the hex address of the instruction tagged **labz**?
   Address of labz (HEX): 0x

10. What is the hex address of the **BR** instruction that called **f** originally?
    Address of original call (HEX): 0x

Calculator

Submit

Discussion

Hide Discussion

Topic: 12. Procedures and Stacks / Tutorial: Stacks and Procedures

Add a Post

Show all posts by recent activity

- STACKS AND PROCEDURES 6: Why Mem[0x100] == 15?
  According to Question D in this problem, the value X that was passed to the original call to sqr(X) is 5. And here is the labeled stack... 3
- STACKS AND PROCEDURES: 8.G.
  Q: "What value is in R1 prior to the execution of the LD at labz?" A: "The value in R1 prior to executing the LD instruction is the result... 6
- Stacks and Procedures: 1-A. Highest memory address possibly effected
  Risking to sound pedantic, shouldn't I say the highest memory address effected is 0x1403, instead of 0x1400? 4
- Hmm This tutorial has many problems
  This tutorial has exceptionally high number of problems as compared to other topics. Any particular reason? 7

< Previous Next >

edX

- About
- Affiliates
- edX for Business
- Open edX
- Careers
- News

Legal

- Terms of Service & Honor Code
- Privacy Policy
- Accessibility Policy
- Trademark Policy
- Sitemap
- Cookie Policy
- Your Privacy Choices

Connect

- Idea Hub
- Contact Us
- Help Center
- Security

Calculator

Media Kit

GET IT ON Google play

Download on the App Store

Calculator