6.004 Flipped Section Worksheet
L12 – Procedures and Stacks

**PUSH(X):** Push Reg[x] onto stack
   ADDC(SP, 4, SP)
   ST(Rx, -4, SP)

**POP(X):** Pop value at top of stack into Reg[x]
   LD(SP, -4, RX)
   SUBC(SP, 4, SP)

**ALLOCATE(k):** Reserve k words of stack
   ADDC(SP, 4*k, SP)

**DEALLOCATE(k):** Release k words of stack
   SUBC(SP, 4*k, SP)

*Stack discipline:* Leave stack the way you found it => for every PUSH(), there’s a corresponding POP() or DEALLOCATE()

---

**CALLING SEQUENCE**

- PUSH(argn)  // push args, last arg first
- ...
- PUSH(arg1)
- BR(f, LP)    // call f, return addr in LP
- DEALLOCATE(n) // remove args from stack

**ENTRY SEQUENCE**

- f: PUSH(LP)  // save return addr
- PUSH(BP)    // save old frame pointer
- MOVE(SP,BP) // initialize new frame pointer
- ALLOCATE(nlocals) // make room for locals
- (push other regs) // preserve old reg vals

**EXIT SEQUENCE**

- // return value in R0
- MOVE(BP,SP) // remove locals
- POP(BP) // restore old frame pointer
- POP(LP) // recover return address
- JMP(LP) // resume execution in caller
Problem 1.

You are given an incomplete listing of a C program (shown below) and its translation to Beta assembly code (shown on the right):

```c
int fn(int x) {
    int lowbit = x & 1;
    int rest = x >> 1;
    if (x == 0) return 0;
    else return ???;
}
```

(A) What is the missing C source corresponding to ??? in the above program?

C source code: \[ \text{fn}(\text{rest}) + \text{lowbit} \]

(B) Suppose the instruction bearing the tag \('zz: '\) were eliminated from the assembly language program. Would the modified procedure work the same as the original procedure (circle one)?

- YES
- NO

**The \(\text{MOVE}(\text{BP}, \text{SP})\) is deallocating the local variables \text{lowbit} and \text{rest}**

(C) In the space below, fill in the binary representation for the instruction stored at the location tagged \('xx: '\) in the above program.

![Binary Representation](image)

(fill in missing 1s and 0s for instruction at \(xx:\))
The procedure \textit{fn} is called from an external procedure and its execution is interrupted just prior to the execution of the instruction tagged ‘yy:’. The contents of a region of memory are shown on the left below.

NB: All addresses and data values are shown in hex. The contents of BP are 0x1C8 and SP contains 0x1D4.

(D) What was the argument to the most recent call to \textit{fn}?

\begin{verbatim}
184:  4 from current stack frame
188:  7
18C:  47 \texttt{x}
190:  C4 saved LP looking at call:
194:  170 saved BP R1 held value of argument before the call
198:  1 labout
19C:  23 rest
1AC:  198 saved BP
\end{verbatim}

Contents of 1D0 (HEX): \underline{11}

(E) What is the missing value marked ??? for the contents of location 1D0?

\begin{verbatim}
1A0:  22 saved R1 saved LP is the address of mem location holding \texttt{DEALLOCATE} inst.
1A4:  23 \texttt{x}
1A8:  4C saved LP
1AC:  198 saved BP
\end{verbatim}

Address of \texttt{rtn} (HEX): \underline{58}

(F) What is the hex address of the instruction tagged \texttt{rtn}?

\begin{verbatim}
1B0:  1 labout find frame with saved LP \neq 0x4C.
1B4:  11 rest
1B8:  23 saved R1
1BC:  11 \texttt{x}
1C0:  4C saved LP (saved LP on oldest stack frame) - 4.
1C4:  1B0 saved BP
\end{verbatim}

Address of original call (HEX): \underline{C0}

(G) What was the argument to the original call to \textit{fn}?

\begin{verbatim}
1C8:  1 \leftarrow BP labout
1CC:  8 rest
1D0:  ??? saved R1
1D4:  0 \leftarrow SP
\end{verbatim}

Original R1 contents (HEX): \underline{22}

(H) What is the hex address of the BR instruction that called \textit{fn} originally?

\begin{verbatim}
1C8:  1 \leftarrow BP labout
1CC:  8 rest
1D0:  ??? saved R1
1D4:  0 \leftarrow SP
\end{verbatim}

Address of original call (HEX): \underline{C0}

(I) What were the contents of R1 at the time of the original call?

\begin{verbatim}
1C8:  1 \leftarrow BP labout
1CC:  8 rest
1D0:  ??? saved R1
1D4:  0 \leftarrow SP
\end{verbatim}

Original R1 contents (HEX): \underline{22}

(J) What value will be returned to the original caller?

\begin{verbatim}
1C8:  1 \leftarrow BP labout
1CC:  8 rest
1D0:  ??? saved R1
1D4:  0 \leftarrow SP
\end{verbatim}

Return value for original call (HEX): \underline{4}

\textit{fn} counts number of 1 bits in argument.
Problem 2.

You are given an incomplete listing of a C program (shown below) and its translation to Beta assembly code (shown on the right):

```c
int f(int x, int y) {
    x = (x >> 1) + y;
    if (y == 0) return x;
    else return ???;
}
```

(A) What is the missing C source corresponding to ??? in the above program?

C source code:

(B) Suppose the instruction bearing the tag ‘zz:’ were eliminated from the assembly language program. Would the modified procedure work the same as the original procedure?

Work the same (circle one)? YES ... NO

The procedure $f$ is called from an external procedure and then execution is stopped just prior to one of the executions of the instruction labeled ‘rtn:’. The addresses and contents of a region of memory are shown in the table on the right; all addresses and data values in the table are in hex. When execution is stopped BP contains the value 0x14C and SP contains the value 0x150.

(C) What are the arguments to the currently active call to $f$?

Most recent arguments (in hex): $x = 0x_{\_\_\_\_\_\_\_\_, y = 0x_{\_\_\_\_\_\_\_}$

(D) If you can tell from the information provided, specify the arguments to the original call to $f$, otherwise select CAN'T TELL.

Original arguments (in hex): $x = 0x_{\_\_\_\_\_\_\_, y = 0x_{\_\_\_\_\_\_\_}$, or CAN'T TELL

(E) What is the missing value in location 0x12C?

Contents of location 0x12C (in hex): 0x_{\_\_\_\_\_\_\_}

(F) What is the hex address of the instruction labeled rtn:?

Address of instruction labeled rtn: (in hex): 0x_{\_\_\_\_\_\_\_}

(G) What is the hex address of the BR instruction that called $f$ originally?

Address of original call (in hex): 0x_{\_\_\_\_\_\_\_}, or CAN'T TELL

(H) What value will be returned to the original caller?

Return value for original call (in hex): 0x_{\_\_\_\_\_\_\_}
Problem 3.

The following C program implements a function H(x,y) of two arguments, which returns an integer result. The assembly code for the procedure is shown on the right.

```c
int H(int x, int y) {
    int a = x - y;
    if (a < 0) return x;
    else return ???;
}
```

The execution of the procedure call H(0x68, 0x20) has been suspended just as the Beta is about to execute the instruction labeled “rtn:” during one of the recursive calls to H. A partial trace of the stack at the time execution was suspended is shown to the right below.

(A) Examining the assembly language for H, what is the appropriate C code for ??? in the C representation for H?

C code for ???: ___________

(B) Please fill in the values for the blank locations in the stack dump shown on the right. Express the values in hex or write “---” if value can’t be determined. Hint: Figure out the layout of H’s activation record and use it to identify and label the stack frames in the stack dump.

Fill in the blank locations with values (in hex!) or “---”

(C) Determine the specified values at the time execution was suspended. Please express each value in hex or write “CAN’T TELL” if the value cannot be determined.

Result of H(Bp+0): Value in R0 or “CAN’T TELL”: 0x ___________

Value in R1 or “CAN’T TELL”: 0x ___________

Value in BP or “CAN’T TELL”: 0x ___________

Value in LP or “CAN’T TELL”: 0x ___________

Value in SP or “CAN’T TELL”: 0x ___________

6.004 Worksheet - 5 of 6 - L12 – Procedures and Stacks
Problem 4.

The following C program computes the log base 2 of its argument. The assembly code for the procedure is shown on the right, along with a stack trace showing the execution of ilog2(10). The execution has been halted just as it’s about to execute the instruction labeled “rtn.”

```c
/* compute log base 2 of arg */
int ilog2(unsigned x) {
    unsigned y;
    if (x == 0) return 0;
    else {
        /* shift x right by 1 bit */
        y = x >> 1;
        return ilog2(y) + 1;
    }
}
```

(A) What are the values in R0, SP, BP and LP at the time execution was halted? Please express the values in hex or write “CAN’T TELL”.

- Value in R0: 0x1c 1c
- Value in SP: 0x29c
- Value in BP: 0x244
- Value in LP: 0x1a8

(B) Please fill in the values for the five blank locations in the stack trace shown on the right. Please express the values in hex.

```
Fill in values (in hex!) for 5 blank locations
```

(C) In the assembly language code for ilog2 there is the instruction “LD(BP,-12,R0)”. If this instruction were rewritten as “LD(SP,NNN,R0)” what is correct value to use for NNN?

```
Correct value for NNN: 0x2c
```

(D) In the assembly language code for ilog2, what is the address of the memory location labeled “xxx”? Please express the value in hex.

```
Address of location labeled “xxx”: 0x18b
```