Q1 Calling Conventions

10 Points

Q1.1 Stack layout

10 Points

Imagine you break right on the printf() line below in the following xv6 program (specifically right on the call instruction that is about to call the printf function inside the bar function):

```
int bar(int x, int y) {
  printf(1, "x:%d, y:%d\n", x, y);
  return x;
}
int foo(int a, int b, int c) {
  return bar(a + b, c);
}
main() {
  foo(1, 2, 3);
  exit(0);
}
```

Please draw the stack and explain every value on the stack. Assume that compiler does not use stack alignment, but maintains stack frames. You can make up any values for the return addresses.

No files uploaded

Q2 Processes

30 Points

Q2.1

5 Points

Draw and explain organization of the process address space in the xv6 system. Be specific. ASCII drawing that you can copy as a skeleton for your answer.

```
0                                       4GB
------------------------------------------
|   foo | bar | ....  | heap | stack     |
------------------------------------------
```

No files uploaded

Q2.2
5 Points

Alice executes the following xv6 program

```c
#include "types.h"
#include "stat.h"
#include "user.h"

int
main(int argc, char *argv[])
{

  char *msg = "bar\n";
  int pid = fork();
  if (pid)
    msg = "foo\n";
  else
    msg = "baz\n";
  write(1, msg, 4);
  exit();
}
```

What are all possible outputs of this program? Explain your answer.

No files uploaded

Q2.3
5 Points

Bob argues with Alice that there will never be an output with interleaving characters? E.g., “fbaozo” Is he correct? Explain your answer?

No files uploaded

Q2.4
10 Points

Alice continues experimenting with xv6. She writes the following xv6 program to test recursive invocation of functions.

```c
#include "types.h"
#include "stat.h"
#include "user.h"


int foo(char *p) {
  write(1, "hello\n", 6);
  foo(p);
  return 0;
}

int
main(int argc, char *argv[])
{
   char a[4096];
   foo(a);
   exit();
}
```

How many times Alice will see "hello" on the screen? Explain your answer.

No files uploaded

Q2.5
5 Points

Alice is running an xv6 system with two CPUs. Is it possible for the `init()` process which is created on the first CPU to run on the second CPU at some point in time? Be specific, explain why this may or may not happen.

No files uploaded

Q3 Context switch

20 Points

Q3.1

10 Points

Explain how xv6 switches from one process to another? Be specific, refer to the source code and function that implement the context switch.

No files uploaded

Q3.2

5 Points

During the context switch the register `EBX` gets saved twice, once by the `popal` instruction in the `alltraps()` function and second in the `swtch()` function. Can you explain why do we need to save it
twice?

No files uploaded

Q3.3

5 Points

Explain the role of the `context` field in the `proc` data structure in xv6. How is it used during the context switch?

No files uploaded

Q4 File systems

15 Points

Q4.1

5 Points

Can you explain what operations the xv6 file system performs when Bob invokes the following xv6 command

```
ln README foobar
```

Be specific

No files uploaded