Lab 10: Axiomatic Semantics

csi 3120

Recall the Rules of Hoare Logic

$$\frac{}{\{Q_{x \to E}\}\ \mathtt{x := E}\ \{Q\}}\ \text{Assignment}$$

$$\frac{\{P\}S\{Q\} \qquad P' \Rightarrow P \qquad Q \Rightarrow Q'}{\{P'\}S\{Q'\}}\ \text{Consequence}$$

$$\frac{\{P_1\}S_1\{P_2\} \qquad \{P_2\}S_2\{P_3\}}{\{P_1\}S_1; S_2\{P_3\}}\ \text{Sequence}$$

$$\frac{\{B \text{ and } P\}S_1\{Q\} \qquad \{(\text{not } B) \text{ and } P\}S_2\{Q\}}{\{P\}\ \mathtt{if}\ B\ S_1\ \mathtt{else}\ S_2\ \{Q\}}\ \text{If Rule}$$

$$\frac{\{I \wedge B\}S\{I\}}{\{I\}\ \mathtt{while}\ B\ \mathtt{do}\ S\ \mathtt{end}\{I \text{ and } (\text{not } B)\}}\ \text{While Rule}$$

Problem 1

(a) Find the weakest precondition of the following "if" statement, using the given postcondition.


```
if x > y then z := x else z := y
```

$\{x > 0 \textit{ and } y > 0 \textit{ and } z \geq x \textit{ and } z \geq y\}$

(b) Bonus (save for last): Prove the following Hoare triple. (In other words, prove that this program is correct.)

$\{x > 0 \textit{ and } y > 0\}$

```
if x > y then z := x else z := y
```

$\{x > 0 \textit{ and } y > 0 \textit{ and } z \geq x \textit{ and } z \geq y\}$

Problem 2

Below is another program to compute factorial (a minor modification of the one proved correct in class).

$\{n \geq 0\}$

```
fact := n;
count := n-1;
while count <> 1 do
        fact := fact * count;
        count := count-1;
end
```


$\{fact = n!\}$

(a) Find a loop invariant for this version that will lead to a proof.

(b) Does the precondition guarantee termination? If not replace the precondition with another one that guarantees termination.

Problem 3

Consider the tail recursive OCaml program below.

```
let mult_tr (a:int) (b:int) =
  let rec mult' (a:int) (b:int) (result:int) =
    if a = 0 then 0
    else if a = 1 then b + result
    else mult' (a-1) b (result+b)
  in
  mult' a b 0
```


Translate this program to an equivalent one that uses a while loop instead of recursion. (See page 62 of the course notes for Chapter 7 of the Mitchell textbook.) Use the programming language that was defined in the course notes on Axiomatic Semantics (assignment statements, if statements, while loops, and sequences of statements separated by a semi-colon). Let P be the name of your program. The following Hoare triple should be true about your program: $\{a \geq 0\}P\{n = a * b\}$. You don't have to prove it. Just make sure that your program is correct, and terminates whenever the precondition is satisfied.