Copyright ©2018

Due Wednesday, Nov. 21, by 4:00pm, to Crowdmark.

All submitted work must be the student's own.

Notes for this assignment: For this assignment, to prove partial correctness, give the required program annotations and any proofs of "implied" conditions. For "implied" proofs, use ordinary arithmetic laws. (As you would have in MATH 135.)

Question 1 (10 marks).
[Learning Goals: Fix a Hoare triple to be partially correct and annotate a code containing a while loop.]
Consider the following specification for the code C given below:

$(\!| (y \geq 0) |\!)$

```
z = 1 ;
while ( y > 0 ) {
    z = z * x ;
    y = y - 1 ;
}
```

$(\!| (z = x^y) |\!)$

[2] (a) The above code C is attempting to compute x^y however the given Hoare triple contains an error. Identify the error and give a corrected pre and post condition fixing the problem with neither pre or post condition being equivalent to `T` or `F` (true or false). In other words, correct the mistake in the Hoare triple nontrivially and do not modify the code.

[2] (b) Prove that this code terminates if given a state satisfying the precondition you created from the previous part.

[6]

(c) Prove that this specification is satisfied under both partial and total correctness. Show all the needed details of your program annotation, and explicitly prove any implications required by your annotation.

Question 2 (10 marks).
Show that the following Hoare triple is satisfied under partial correctness.

$(\!|\ \text{true}\ |\!)$

```
if ( z < y ) {

    if (z < x) {

        m = z;

    } else {

        m = x;

    }

} else {

    m = y;

    if (x < y){

        m = x;

    }

}
```

$(\!|\ \big((m \leq x) \wedge \big((m \leq y) \wedge (m \leq z)\big)\big)\ |\!)$

Question 3 (8 marks).
Show that each of the following Hoare triples is satisfied under partial correctness. Give the required program annotations and any proofs of "implied" conditions.

For "implied" proofs, use ordinary arithmetic laws. (As you would have in MATH 135.)

$\llparenthesis\ \big(((y = y_0) \wedge (y > 0)) \wedge (s = 0)\big)\ \rrparenthesis$

```
n = 1;

while (y > 0) {

    s = s + n;

    n = n + 2;

    y = y - 1;

}
```

$\llparenthesis\ (s = (y_0 \times y_0))\ \rrparenthesis$

Question 4 (10 marks).
Show that the following Hoare triple is satisfied under partial correctness.
Hint: Translate the modulus condition into one about parity using $E(z) \stackrel{\text{def}}{=} (\exists u\, ((u+u) = z))$. For a nonnegative integer `a` and a positive integer `b` , `a % b` is the remainder when dividing `a` by `b`.

$\llparenthesis\ (((y = y_0) \wedge (y > 0)) \wedge ((s = 0) \wedge E(y_0)))\ \rrparenthesis$

```
while (y != 0) {

    if ( y % 2 == 0 ) {

        s = s + y

    } else {

        s = s - y

    }

    y = y - 1;

}
```

$\llparenthesis\ ((2 \times s) = y_0)\ \rrparenthesis$