Assignment 5

Due: Nov 8th, 2024

(Ethics: Any behavior on any homework or exam that could be considered copying or cheating will result in an immediate zero on the assignment for all parties involved and will be reported to academichonesty@iit.edu. See the IIT Code of Academic Honesty, https://web.iit.edu/student-affairs/handbook/fine-print/code-academic-honesty)

1. For formal proof in Assignment 4, Question 10:
   a. Create a corresponding full proof outline under partial correctness.
   b. Create a corresponding minimal proof outline under partial correctness.

2. Consider the minimal proof outline in Lecture 15, Example 3. Expand it to a full proof outline under partial correctness that is different from the one in Lecture 15, Example 4: please use the Backward Assignment Axiom to prove assignment statements before the loop and use the Forward Assignment Axiom to prove assignment statements in the loop body. Give a brief explanation on each logical implication used in the proof outline.

3. Give a full proof outline under partial correctness obtained by expansion of the partial proof outline below. Please use the Forward Assignment Axiom to prove all the assignment statements. Give a brief explanation on each logical implication used in the proof outline.

   $\{y \geq 1\}\ x := 0; r := 1;$
   $\{\mathbf{inv}\ 1 \leq r = 2\text{^}x \leq\ y\}$
   $\mathbf{while}\ 2 * r \leq y\ \mathbf{do}\ r := 2 * r;\ x := x + 1\ \mathbf{od}$
   $\{r = 2\text{^}x \leq y \leq 2\text{^}(x + 1)\}$

4. Find a reasonable bound expression for the while loop in Question 3, then create a full proof outline **under total correctness** for the partial proof outline in Question 3. Please use the Backward Assignment Axiom to prove all the assignment statements. Give a brief explanation on each logical implication used in the proof outline.

5. Under total correctness, find a reasonable precondition p and create a full proof outline for the following provable triple:

   $$\{p\}\ \mathbf{if}\ sqrt(x) > y\ \mathbf{then}\ x := b[x - y]\ \mathbf{else}\ y := b[y - x]\ \mathbf{fi}\ \{x = y\}$$

   Hint: Using Conditional Rule 2 can avoid calculating the domain predicate for a conditional statement.

6. Under total correctness, find a reasonable postcondition q and create a full proof outline for the following provable triple:

   $$\{sqrt(x) \leq y\}\ x := x * y; x := 1 \div x\ \{q\}$$

   Hint: Since the precondition and the statement are not safe, we should include their domain predicates in the precondition for total correctness. Be careful of the domain predicate for a sequence statement.

7. Let $W \equiv \{\mathbf{inv}\ p\}\{\mathbf{bd}\ t\}\ \mathbf{while}\ B\ \mathbf{do}\ S\ \mathbf{od}$ and $\vdash_{tot} \{\mathbf{inv}\ p\}\{\mathbf{bd}\ t\}\ \mathbf{while}\ B\ \mathbf{do}\ S\ \mathbf{od}\ \{p \wedge \neg B\}$. For each of the following statements about bound expression, decide true or false and justify your answer briefly.
   a. Let $\sigma \vDash p$, then $\perp_d \notin M(W, \sigma)$.
   b. The value of t can be negative after the execution the last iteration of W.
   c. $sp(p \wedge B \wedge t = t_0, S\ ) \Rightarrow t < t_0$
   d. $p \wedge t > 0 \Rightarrow B$
   e. $t < 0 \Rightarrow \neg p$

8. Let $W \equiv \{\mathbf{inv}\, p\}\{\mathbf{bd}\, t\}\ \mathbf{while}\ k \le n\ \mathbf{do}\ x := x - 2; k := k + 1\ \mathbf{od}$, and we know that $p \Rightarrow n \ge 0\ \wedge\ 0 < C \le k \le n + C$, where C is a constant. For each of the following expressions, decide whether it can be the bound expression for W and justify your answer briefly.
   a. $x - k + n$
   b. $n - k$
   c. $n - k + C$
   d. $k - C$
   e. $2\text{^}n \cdot 2\text{^}(C - k)$

9. Consider predicate $q \equiv y \ge 0 \wedge x = 2 * y \le n < 3 * (y + 1)$, where n is a named constant and x and y are variables, as the postcondition of a loop. Using the technique **replacing a constant in *q* by a variable**, create 5 possible candidates for the loop invariant p and their corresponding loop condition B.

10. Consider predicate $q \equiv (y \ge 0) \wedge (z\ = 2\text{^}y) \wedge (2\text{^}y \le x) \wedge (x < 2\text{^}(y + 1))$ as the postcondition of a loop. Using the technique **dropping off one conjunct in *q***, create 4 possible candidates for the loop invariant p and their corresponding loop condition B.