Assignment 4

Due: Oct 25th, 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. Let predicate $p \equiv w * x \neq 0 \wedge z \leq 2 \rightarrow f(w) > 0 \wedge \forall x. \exists y. 0 \leq y \leq x \wedge f(w \div x) + y > f(z)$. Here, w, x, y and z are integer variables. Finish the following syntactic substitutions and show your work.
   a. $p\ [y + z \ / \ x]$
   b. $p\ [x + z \ / \ w]$
   c. $p\ [x + y \ / \ z]$

2. Let x and y be two different integer variables. A student gave the following conjecture:
$$(x * y)[e \ / \ x][e' \ / \ y] \equiv (x * y)[e' \ / \ y][e \ / \ x]$$
   a. Show an example (with some e and some e') in which the above conjecture works.
   b. Disprove the above conjecture with a counterexample (with some e and some e').

3. Answer the following questions about the relationship between wlp and sp.
   a. Prove that "If $p \Leftrightarrow wlp(S, q)$, then $sp(p, S) \Rightarrow q$".
   b. Disprove that "If $p \Leftrightarrow wlp(S, q)$, then $q \Rightarrow sp(p, S)$" with a counterexample.

4. For predicate p and statement S, let $s \Leftrightarrow sp(p, S)$. For each of the following, decide whether it is true or false then justify your answer briefly.
   a. $\vDash_{tot} \{p\}\ S\ \{s\}$
   b. There exists some $\sigma \vDash p$ such that $\sigma \nvDash \{p\}\ S\ \{s\}$.
   c. For each state $\sigma \vDash p$, we have that $M(S, \sigma) \vDash s$.
   d. If $M(S, \sigma) - \bot \vDash s$, then $\sigma \vDash p$.
   e. If $\sigma \vDash \neg p$, then $\sigma \vDash \{\neg p\}\ S\ \{\neg s\}$

Questions 5 and 6 are about calculating the strongest postconditions. You don't have to logically simplify your solutions to questions 5 and 6.

5. Calculate $sp(x = y,\ \mathbf{if}\ x \geq 0 \rightarrow x := y + 1; z := x\ \ \square\ x \leq 0 \rightarrow y := x - 1; z := y\ \mathbf{fi})$.

6. Calculate $sp(y = x + 1,\ \ y := y + 1; \mathbf{if}\ x < 0\ \mathbf{then}\ y := -y\ \mathbf{fi})$.

7. Under partial correctness, show a formal proof of Conditional Rule 1 given all other rules. In other word, given provable triples $\{p \wedge B\}\ S_1\ \{q_1\}$ and $\{p \wedge \neg B\}\ S_2\ \{q_2\}$, prove that $\vdash \{p\}\ \mathbf{if}\ B\ \mathbf{then}\ S_1\ \mathbf{else}\ S_2\ \mathbf{fi}\ \{q_1 \vee q_2\}$; and you cannot use Conditional Rule 1 itself in your proof.

   Hint: Remind that, in Lecture 11 we have seen that $(B \rightarrow p) \wedge (\neg B \rightarrow q) \Leftrightarrow (B \wedge p) \vee (\neg B \wedge q)$; this logically equivalence can be useful here.

8. Given that $S \equiv x := x * x; y := 2 * y$, calculate $wlp(S,\ x = y)$ and then show a formal proof for $\vdash \{p\}\ S\ \{x = y\}$ where $p \Leftrightarrow wlp(S,\ x = y)$.

9. Let $p \equiv x = 2\textasciicircum k \wedge k \leq n$. Complete the following formal proof by calculating predicates p_1 to p_4, and completing the rule references R_1 to R_5. ("$2\textasciicircum k$" means "2 to the power of k".)

1. $\{p_1\}\ x \coloneqq x * 2\ \{p_2\}$	R_1
2. $\{p_2\}\ k \coloneqq k + 1\ \{p_3\}$	R_2
3. $\{p_1\}\ x \coloneqq x * 2; k \coloneqq k + 1\ \{p_3\}$	R_3
4. $p_3 \rightarrow p$	predicate logic
5. $\{p_1\}\ x \coloneqq x * 2; k \coloneqq k + 1\ \{p\}$	R_4
6. $\{\mathbf{inv}\ p\}\ \mathbf{while}\ k < n\ \mathbf{do}\ x \coloneqq x * 2; k \coloneqq k + 1\ \mathbf{od}\ \{p_4\}$	R_5

10. Complete the following formal proof by completing the rule references R_1 to R_{11}.

1. $\{n > 0\}\ k \coloneqq n - 1\ \{n > 0 \wedge k = n - 1\}$	R_1
2. $\{n > 0 \wedge k = n - 1\}\ x \coloneqq n\ \{n > 0 \wedge k = n - 1 \wedge x = n\}$	R_2
3. $n > 0 \wedge k = n - 1 \wedge x = n \Rightarrow p$	predicate logic
# Where $p \equiv 1 \leq k \leq n \wedge x = n!\ /\ k!$	
4. $\{n > 0 \wedge k = n - 1\}\ x \coloneqq n\ \{p\}$	R_3
5. $\{n > 0\}\ k \coloneqq n - 1;\ x \coloneqq n\ \{p\}$	R_4
6. $\{p\ [x * k\ /\ x]\}\ x \coloneqq x * k\ \{p\}$	R_5
7. $\{p\ [x * k\ /\ x]\ [k - 1\ /\ k]\}\ k \coloneqq k - 1\ \{p\ [x * k\ /\ x]\}$	R_6
8. $p \wedge k > 1 \Rightarrow p\ [x * k\ /\ x]\ [k - 1\ /\ k]$	predicate logic
9. $\{p \wedge k > 1\}\ k \coloneqq k - 1\ \{\ p\ [\ x * k\ /\ x\ ]\ \}$	R_7
10. $\{p \wedge k > 1\}\ k \coloneqq k - 1;\ x \coloneqq x * k\ \{p\}$	R_8
11. $\{\mathbf{inv}\ p\}\ W\ \{p \wedge k\ \leq 1\}$	R_9
# Where $W \equiv \mathbf{while}\ k > 1\ \mathbf{do}\ k \coloneqq k - 1;\ x \coloneqq x * k\ \mathbf{od}$	
12. $\{n > 0\}\ k \coloneqq n - 1;\ x \coloneqq n\ \{\mathbf{inv}\ p\}\ W\ \{p \wedge k\ \leq 1\}$	R_{10}
13. $p \wedge k \leq 1 \Rightarrow\ x =\ n\,!$	predicate logic
14. $\{n > 0\}\ k \coloneqq n - 1;\ x \coloneqq n\ \{\mathbf{inv}\ p\}\ W\ \{x =\ n\,!\}$	R_{11}