Assignment 2: Program it Out
15-414/15-424 Bug Catching: Automated Program Verification

Due: **11:59pm**, Thursday 9/14/17
Total Points: 50

1. **Follow your state (3 points)** Give the full sequence of all intermediate and final states that this program passes through while executing from initial state ω with $\omega(x) = 1$ and $\omega(y) = 2$:

$$x := x + 1; \texttt{while}(x < 5)\ \{y := y + x \cdot x; x := x + 1\}; x := -x;$$

2. **Program counting (3 points)** How many intermediate and final states does the following program pass through while executing from initial state ω with $\omega(x) = 1$ and $\omega(y) = 2$:? Why?

$$x := x + 1; \texttt{while}(x < 100)\ \{y := y + x \cdot x; x := x + 1\}; x := -x;$$

3. **Outside in (5 points)** In class we discussed a way of proving the swap program correct by working inside out starting from the innermost assignment first. Show how to complete the proof when working outside in starting from the outermost assignment first.

$$\text{→R}\,\dfrac{\text{[;]}\,\dfrac{\text{[;]}\,\dfrac{\text{[:=]}\,\dfrac{\dots}{x{=}a \land y{=}b \vdash [x := x + y][y := x - y][x := x - y](x = b \land y = a)}}{x{=}a \land y{=}b \vdash [x := x + y][y := x - y; x := x - y](x = b \land y = a)}}{x{=}a \land y{=}b \vdash [x := x + y; y := x - y; x := x - y](x = b \land y = a)}}{\vdash x = a \land y = b \to [x := x + y; y := x - y; x := x - y](x = b \land y = a)}$$

4. **Backflip (5 points)** Conduct a proof in sequent calculus with the axioms of of dynamic logic of the following formula. Be sure to say which proof rule you apply at each step.

$$x = a \land y = b \to [x := x + y; y := x - y; x := x - y; x := x + y; y := x - y; x := x - y](x = a \land y = b)$$

As always, you are allowed to be clever about how you do a proof, but still have to rigorously justify each step.

5. **Missing condition (7 points)** Fill in the missing condition in the `if` statement to make the following dynamic logic formula valid. Then use the axioms of dynamic logic in sequent calculus to prove it.

$$[\texttt{if}(\ldots)\{r := r - w; q := q + 1\}\ \texttt{else}\ \{?\texttt{false}\}](wq + r = x \land 0 \leqslant r)$$

You may find it useful to begin proving the formula first, and using this to find the right condition.

6. **Soundness of [?] (5 points)** Prove that the [?] axiom is sound. That is, using the semantics of modalities and tests, prove the validity of the following formula instance:

$$[?Q]P \leftrightarrow (Q \to P)$$

7. **Conditional assignments (3 points)** When rummaging through the syntax manual of other imperative programming language and comparing them to the while language considered in class, a clever student found that we totally neglected his favorite feature of conditional assignments. Indeed, the conditional assignment $x := Q\,?\,e1\ :\ e2$ that assigns term $e1$ to variable x if formula Q is true and otherwise assigns term $e2$ to x is missing. Your job is to define a semantics $\llbracket x := Q\,?\,e1\ :\ e2 \rrbracket$ for the conditional assignment $x := Q\,?\,e1\ :\ e2$ as the set of all pairs of initial and final states of running $x := Q\,?\,e1\ :\ e2$.

8. **Conditional assignment axioms (3 points)** After now having added the conditional assignment $x := Q \,?\, e1 \,:\, e2$ as a statement to the programming language, your next task is to design an axiom for it:

   $$([:=?:])\quad [x := Q \,?\, e1 \,:\, e2]p(x) \leftrightarrow \dots$$

9. **Use it! (5 points)** Use your proof axiom [:=?:] to conduct a sequent calculus proof for the formula:

   $$x = y \rightarrow [x := x \cdot x;\ x := x > 0 \,?\, -x \,:\, 0]\, x = -y \cdot y$$

10. **Soundness of** [:=?:] **(11 points)** It's not just proof rules but axioms too that cannot be used unless they are accompanied by a soundness proof. Quickly before anybody notices your answer to the previous task, use the semantics of the conditional assignment $x := Q \,?\, e1 \,:\, e2$ to prove soundness of your axiom [:=?:].

    Hint: First show a logical formula that is equivalent to $[x := Q \,?\, e1 \,:\, e2]p(x)$ but does not use conditional assignments and prove both equivalent. Then use the other axioms to establish that this formula is equivalent to your right hand side of the new axiom [:=?:].