Assignment 3: Program with Loops
15-414/15-424 Bug Catching: Automated Program Verification

Due: **11:59pm**, Thursday 9/20/10
Total Points: 50

1. **Prove another factorial (10 points)** Give a sequent calculus proof, using the axioms of dynamic logic, that the following formula is valid.

$$0 \leqslant x \rightarrow [y := 0; r := 1; \texttt{while}(y < x)\, \{y := y + 1; r := r * y](r = x!)$$

   You should assume that $x!$ refers to the standard factorial function of x:

$$x! = \begin{cases} 1 & \text{if } x = 0 \\ (x-1)!\ x & \text{otherwise} \end{cases}$$

2. **Find the invariants (10 points)** Provide loop invariants P and Q that are sufficient to prove validity of the following dynamic logic formula. You do not need to formally prove that the formula is valid, but you should succinctly explain why your invariants are correct.

$$\begin{array}{l} 0 \leqslant x \wedge 0 < y \rightarrow [q := 0; \\ \qquad r := x; \\ \qquad \texttt{while}(y \leqslant r)\, \texttt{invariant}(P)\ \{ \\ \qquad\quad r := r - y; \\ \qquad\quad q := q + 1; \\ \qquad \} \\ \qquad](0 \leqslant r < y \wedge q * y + r = x) \end{array}$$

$$\begin{array}{l} 0 < a \wedge 0 < b \rightarrow [c := a; \\ \qquad d := b; \\ \qquad \texttt{while}(c \neq d)\, \texttt{invariant}(Q)\ \{ \\ \qquad\quad \texttt{if}(c > d)\ \{ \\ \qquad\qquad c := c - d; \\ \qquad\quad \}\ \texttt{else}\ \{ \\ \qquad\qquad d := d - c; \\ \qquad\quad \} \\ \qquad](c = gcd(a, b)) \end{array}$$

   You should assume that *gcd* is the standard greatest common divisor function. *Hint: you may find the following fact about greatest common divisors useful.*

$$\forall a, b\ gcd(a, b) = gcd(a, b - a)$$

3. **While is just another repetition (10 points)** Lecture 3 defined a semantics $[\![\texttt{while}(Q)\, \alpha]\!]$ for the while loop $\texttt{while}(Q)\, \alpha$. Lecture 5 defined a semantics $[\![\alpha^*]\!]$ for the nondeterministic repetition α^* and then went on to claim the following equivalence of programs:

$$\texttt{while}(Q)\, \alpha \ \equiv\ \{?Q; \alpha\}^*; ?\neg Q$$

   Use the semantics of programs to show that both programs are indeed equivalent by showing that the semantics of the left hand side is equal to the semantics of the right hand side, so both have the same reachability relation:

$$[\![\texttt{while}(Q)\, \alpha]\!] \ =\ [\![\{?Q; \alpha\}^*; ?\neg Q]\!]$$

4. **Soundness of while invariants (10 points)** Loop invariants are the most important reasoning technique for while loops. To disambiguate, this question will call their proof rule wloop:

$$\text{(wloop)}\ \frac{\Gamma \vdash J, \Delta \quad J, Q \vdash [\alpha]J \quad J, \neg Q \vdash P}{\Gamma \vdash [\texttt{while}(Q)\,\alpha]P, \Delta}$$

Since we will be using the wloop invariant proof rule for while loops a lot throughout the whole semester, it is crucial to make sure—once and for all—that the proof rule is sound. Otherwise we would be conducting all kinds of formal sequent calculus proofs that do not actually imply validity of their conclusion, which would be rather futile. So before things go wrong, this is your chance to prove that the wloop rule is sound, which you will then be able to remember forever.

Recall that the lecture notes have proved soundness of a related invariant rule for nondeterministic repetition α^*, which are closely related to while loops:

$$\text{(loop)}\ \frac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash P}{\Gamma \vdash [\alpha^*]P, \Delta}$$

Prove soundness of the loop invariant rule wloop for while loops.

Hint: you may want to benefit from the fact that the lecture notes showed the loop rule for nondeterministic repetitions to be a derived rule.

5. **Unsoundness of while invariants (10 points)** Consider the following modified formulation of the while loop rule (changes highlighted in bold):

$$\text{(R3)}\ \frac{\Gamma \vdash J, \Delta \quad J, Q \vdash [\alpha]J \quad J, \neg Q \vdash P, \mathbf{\Delta}}{\Gamma \vdash [\texttt{while}(Q)\,\alpha]P, \Delta}$$

Show that rule R3 is unsound. That is, give an instance of rule R3 with concrete formulas in which all premises are valid but the conclusion is not valid. Briefly explain why that happens. Where in your proof of Task 4 do you rule out this counterexample?