Assignment 4
Termination & Transformers

15-414: Bug Catching: Automated Program Verification

Due 23:59pm, Friday, March 14, 2025
50 pts

This assignment is due on the above date and it must be submitted electronically on Gradescope. Please carefully read the policies on collaboration and credit on the course web pages at http://www.cs.cmu.edu/~15414/assignments.html.

What To Hand In

You should hand in the following files on Gradescope:

- Submit a PDF containing your answers to the written questions to Assignment 4. You may use the file `asst4.tex` as a template and submit `asst4.pdf`.

Using LaTeX

We prefer the answer to your written questions to be typeset in LaTeX, but as long as you hand in a readable PDF with your solutions it is not a requirement. We package the assignment source `asst4.tex` to get you started on this.

1 Convergence (25 pts)

Recall the axiom of convergence from Lecture 10 using a *variant predicate* $V(n)$:

$$\begin{array}{rcl}\langle\alpha^*\rangle Q & \leftarrow & (\exists n.\, n \geq 0 \wedge V(n)) \\ & & \wedge\, \Box(\forall n.\, n > 0 \wedge V(n) \rightarrow \langle\alpha\rangle V(n-1)) \\ & & \wedge\, \Box(V(0) \rightarrow Q) \\ & & (n \text{ not in } \alpha \text{ or } Q)\end{array}$$

Prove the following in dynamic logic, using the axioms for $\langle\alpha\rangle Q$ as appropriate.

$$\langle x \leftarrow 0 \;;\; (x \leftarrow x+1)^* \;;\; ?(x \geq 17)\rangle\,(x = 17)$$

Task 1 (5 pts). State your predicate $V(n)$.

Task 2 (5 pts). State suitable pre- and post-conditions P and Q such that $P \rightarrow \langle(x \leftarrow x+1)^*\rangle Q$.

Task 3 (10 pts). Show the proof of $P \rightarrow \langle(x \leftarrow x+1)^*\rangle Q$ for the P and Q from Task 2 and the $V(n)$ from Task 1.

Justify each step that requires merely arithmetic reasoning with "by arithmetic" and each step that requires an axiom of dynamic logic with "by axiom *name*" where *name* is among the following: $\langle\,\rangle(\leftarrow)$ (assignment), $\langle\,\rangle(;)$ (sequential composition), $\langle\,\rangle(\cup)$ (nondeterministic choice), $\langle\,\rangle(?)$ (guard) and $\langle\,\rangle(*)$ (convergence).

Task 4 (5 pts). Show the proof of the original formula, with justifications as in Task 3 or "by Task 3".

2 Weakest Precondition (25 pts)

Task 5 (10 pts). Calculate the weakest precondition in each of the following examples. Simplify your answer by eliminating unnecessary quantifiers from the weakest precondition when possible, maintaining logical equivalence. For readability, you may write $Q(e)$ for $(e/x)(Q(x))$ (and similary, $Q(e_1, e_2)$ for $(e_1/x, e_2/y)(Q(x,y))$). You only need to show your final answer.

(ii) $\mathsf{wp}((x \leftarrow x+1) \cup (x \leftarrow x-2))(Q(x))$

(iii) $\mathsf{wp}(\mathsf{if}\ (x \geq 0)\ (y \leftarrow x)\ (y \leftarrow -x))(Q(x,y))$

Task 6 (15 pts). Phrased in Dynamic Logic terms, the rule for sequential composition in Hoare logic would be $\models P \rightarrow [\alpha]R$ and $\models R \rightarrow [\beta]Q$ then $\models P \rightarrow [\alpha\,;\,\beta]Q$. Notice that this is not a purely logical formula in NDL, but rather a statement about how the validity of these formulas relate to each other.

As a purely logical formula, we might be tempted to try writing the sequential composition rule as $\models ((P \rightarrow [\alpha]R) \wedge (R \rightarrow [\beta]Q)) \rightarrow (P \rightarrow [\alpha\,;\,\beta]Q)$. Show via a counterexample that this is not valid. That is, provide α, β, P, Q, and R such that this formula is *not* valid.