Assignment 4
Proofs and Refutations

15-414: Bug Catching: Automated Program Verification

Due 23:59pm, Wednesday, March 22, 2023
70 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 (20 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 (5 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 (10 pts). Using the semantic definition of $\models$ for NDL, prove the soundness of the rule for sequential composition in Hoare logic, that is, $\models P \rightarrow [\alpha]R$ and $\models R \rightarrow [\beta]Q$ then $\models P \rightarrow [\alpha \; ; \; \beta]Q$.

Task 7 (5 pts). Show via a counterexample that we cannot formulate this as purely logical question in NDL in the form of $\models ((P \rightarrow [\alpha]R) \wedge (R \rightarrow [\beta]Q)) \rightarrow (P \rightarrow [\alpha \; ; \; \beta]Q)$. That is, provide α, β, P, Q, and R such that this formula is not valid.

3 Encodings (25 pts)

Task 8 (10 pts). For Boolean variables, x_1, x_2, x_3, and x_4, write a CNF which is satisfied if and only if at least two of the variables are set to *true*.

Colorings. Consider a 2-coloring problem for numbers 1 to 5 such that for every integer solution $a + b = c$ with $1 \leq a < b < c \leq n$ holds that a, b, and c do not have the same color. Note that the possible sums with numbers 1 to 5 under these conditions are:

- 1 + 2 = 3
- 1 + 3 = 4
- 1 + 4 = 5
- 2 + 3 = 5

Task 9 (8 pts). Write a CNF encoding for this problem where each color is represented in unary, i.e., use one Boolean variable per color and number. Explain your reasoning for the different clauses that you added to the formula.

Task 10 (7 pts). Write a CNF encoding for this problem where each color is represented in binary, i.e., use one Boolean variable per number representing its color. Explain your reasoning for the different clauses that you added to the formula.