Assignment 4
Proofs and Refutations

15-414: Bug Catching: Automated Program Verification

Due 23:59pm, Friday, March 15, 2024
65 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-sol.tex` as a template and submit `asst4-sol.pdf`. You can generate this file by running `make` (assuming you have pdflatex in your system).

  Make sure your PDF solution files are up to date before you create the handin file.

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` and a solution template `asst4-sol.tex` in the handout to get you started on this.

1 Box vs. Diamond (25 pts)

In dynamic logic, we define the semantics of negation

$$\omega \models \neg P \quad \text{iff} \quad \omega \not\models P$$

Under this definition it is easy to check, for example, that $\neg\neg P \leftrightarrow P$ is valid. In the tasks below you may use this and the other usual De Morgan laws for (classical) propositional reasoning with negation. Like the $[\alpha]$ and $\langle\alpha\rangle$, we follow the convention that the unary operators bind more tightly than binary ones, so $[\alpha]\neg P \rightarrow \neg Q$ stands for $([\alpha](\neg P)) \rightarrow (\neg Q)$.

For each of the following two implications, either prove its validity or find a counterexample.

Task 1 (5 pts). $\neg[\alpha]P \rightarrow \langle\alpha\rangle\neg P$

Task 2 (5 pts). $\neg\langle\alpha\rangle P \rightarrow [\alpha]\neg P$

Task 3 (5 pts). What can you conclude about the relationship of $[\alpha]$ and $\langle\alpha\rangle$ in dynamic logic in general? In order words, can you describe $[\alpha]P \leftrightarrow \ldots$ using $\langle\alpha\rangle$ and $\langle\alpha\rangle P \leftrightarrow \ldots$ using $[\alpha]$?

Task 4 (10 pts). In view of what you discovered in Tasks 1–3, can you justify the axioms regarding the following constructs directly from the axioms for $[-]Q$, without explicitly referencing the semantic definitions?

(i) $\langle\alpha\,;\,\beta\rangle Q$

(ii) $\langle ?P\rangle Q$

(iii) $\langle\alpha \cup \beta\rangle Q$

2 Weakest Precondition (15 pts)

Task 5 (15 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.

(i) $\mathsf{wp}(x \leftarrow x \times x)(x > 0)$

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

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

3 Strongest Postcondition (15 pts)

Task 6 (15 pts). Calculate the strongest postcondition in each of the following examples. Simplify your answer by eliminating unnecessary quantifiers from the strongest postcondition when possible, maintaining logical equivalence. For readability, you may write $P(e)$ for $(e/x)(P(x))$ (and similary, $P(e_1, e_2)$ for $(e_1/x, e_2/y)(P(x, y))$). You only need to show your final answer.

(i) $\mathsf{sp}(x \leftarrow x \times x)(x > 0)$

(ii) $\mathsf{sp}((x \leftarrow x + 1) \cup (x \leftarrow x - 2))(P(x))$

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

4 Sequent Calculus (10 pts)

Task 7 (10 pts). Show using the inference rules for sequent calculus for first-order logic in Lecture Notes 12 (page 9) that the following holds. Some examples of using inference rules for sequent calculus to prove the validy of formulas can be found in Section 8 of Lecture Notes 12.

(i) $(P \to Q) \land (R \to W) \vdash (P \lor R) \to (Q \lor W)$

(ii) $\forall x.(P(x) \to Q(x)) \vdash \exists x.P(x) \to \exists x.Q(x)$