Assignment 7
Time Flies, (temporal) Logic Abides

15-414: Bug Catching: Automated Program Verification

Due Friday, May 5, 2023
80 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 7 (Written). You may use the file `asst7.tex` as a template and submit `asst7.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 `asst7.tex` with handout to get you started on this.

1 SAT Certificates

Consider the formula:

$$\underbrace{(\neg p_1 \lor \neg p_2)}_{C_1} \land \underbrace{(\neg p_2 \lor p_3)}_{C_2} \land \underbrace{(p_1 \lor \neg p_3 \lor \neg p_5)}_{C_3} \land \underbrace{(\neg p_5 \lor p_2)}_{C_4} \land \underbrace{(p_5 \lor p_2)}_{C_5} \land \underbrace{(p_1 \lor \neg p_3 \lor p_5)}_{C_6}$$

Task 1 (8 pts). Which of the following are correct clausal certificates for this formula? Explain your answer in terms of the reverse unit propagation property.

1. $[p_5 \lor p_2, \neg p_5 \lor p_2, \bot]$
2. $[\neg p_1, \neg p_2, \bot]$

Task 2 (10 pts). Resolution certificates are composed of a list of proof steps, which are of the form:

$$\begin{array}{lll} \textit{Step}\ \#: & \textbf{Assume} & C \\ \textit{Step}\ \#: & \textbf{Resolve} & C \quad [\textit{Step}\ \#, \textit{Step}\ \#, \ldots] \end{array}$$

The **Resolve** steps give the result C of applying resolution on the sequence of clauses, identified by step numbers, obtained at earlier steps. The last step should be $\bot$.

Explain how to obtain a resolution certificate from a clausal certificate. That is, explain how each step of the clausal proof corresponds to a sequence of resolution steps involving clauses from the original formula, as well as earlier clauses in the certificate.

Task 3 (10 pts). Provide a resolution certificate corresponding to the clausal certificate $[p, \bot]$ on the following formula:

$$\underbrace{(p \lor q)}_{C_1} \land \underbrace{(\neg p \lor q)}_{C_2} \land \underbrace{(\neg r \lor \neg q)}_{C_3} \land \underbrace{(r \lor \neg q)}_{C_4}$$

2 Computation Tree Logic

Task 4 (12 pts). Draw a Kripke structure that satisfies the formula $\mathbf{A}[a\ \mathbf{U}\ \mathbf{AF}\ b] \land \mathbf{EX}\ \neg b$.

Task 5 (15 pts). For each state in your answer to Task 4, label which of the formulas $\mathbf{AF}\ b$, $\mathbf{EX}\ \neg b$, and $\mathbf{A}[a\ \mathbf{U}\ \mathbf{AF}\ b]$ are satisfied. You may refer to them as P, Q, and R, respectively.

3 Linear Time Logic

Task 6 (15 pts). Your job is to design a specification for a basic elevator system that services four floors. There is a door at each floor, with a call button and an indicator light that indicates whether the elevator has been called to that floor. Describe a set of atomic propositions and LTL formulas to specify the following properties of the elevator.

1. On each floor, a door will open eventually.
2. A door never opens if the elevator is not present at the corresponding floor.
3. Pushing a call button results in the elevator eventually servicing the corresponding floor.

4. The elevator returns to floor 0 infinitely often.
5. When the call button on floor 4 is pressed, the elevator serves it without stopping at any other floors along the way.

Task 7 (10 pts). Consider a temporal operator with the following semantics on traces σ:

$$\sigma \models P\,\mathbf{W}\,Q \text{ iff, for all } i \geq 0, \text{ if } \sigma^i \models \neg P\,, \text{ then there exists } k \leq i \text{ such that } \sigma^k \models Q$$

This is a weaker version of the normal LTL until operator, in that it doesn't require Q to eventually hold as long as P always does. Show that $\mathbf{W}$ can be expressed in terms of the LTL operators discussed in lecture by writing an equivalence, and use the semantics of LTL to demonstrate that your equivalence is correct.