Assignment 7: Temporal Properties, Model Checking
15-414/15-424 Bug Catching: Automated Program Verification

Due: 11:59pm, Friday 12/1/17
Total Points: 50

1. Computation tree semantics (5 points). Consider the computation structure $K$ below, and the CTL formula:

$$A(p_0 U p_1) \lor EX(AG p_1)$$

For each state in the computation structure, write down the subformulas of the above CTL satisfied by the state. Then, say whether the structure satisfies the formula, i.e. $K \models A(p_0 U p_1) \lor EX(AG p_1)$.

```
\begin{center}
\begin{tikzpicture}
\node[draw,circle] (p1) at (0,0) {$p_1$};
\node[draw,circle] (p2) at (0,-1.5) {$p_2$};
\node[draw,circle] (p0) at (0,-3) {$p_0$};
\node[draw,circle] (p0p1) at (0,-1.5) {$p_0, p_1$};
\draw[->] (p1) to (p0p1);
\draw[->] (p1) to (p2);
\draw[->] (p2) to (p0);
\end{tikzpicture}
\end{center}
```

2. Temporal distinctions (10 points). Show that the following pair of CTL and LTL formulas are not equivalent:

$$AF(a \land AXa) \quad \Diamond (a \land a)$$

To do so, write down a computation structure that satisfies one but not the other. Show that this is the case by providing a counterexample path for the non-satisfied formula, and explaining why the other is modeled by your system.

3. Distributing correctly (15 points). Consider the following LTL equivalences that characterize distributive properties of temporal operators:

$$\Diamond (P \lor Q) \leftrightarrow \Diamond P \lor \Diamond Q$$
$$\Diamond (P \land Q) \leftrightarrow \Diamond P \land \Diamond Q$$
$$\Box (P \lor Q) \leftrightarrow \Box P \lor \Box Q$$
$$\Box (P \land Q) \leftrightarrow \Box P \land \Box Q$$

First, identify which of those equivalences are correct and which are not. Then use the semantics of LTL given in lecture 15 to justify your answer with a proof. For the formulas that are not correct, describe an infinite trace that satisfies one side of the equivalence but not the other, i.e., provide a counterexample.

4. Both $P$ and $\neg P$ (10 points). Recall that a computation structure $K = (W, \sim, v)$ with initial states $W_0 \subseteq W$ satisfies a CTL formula $P$ if and only if each initial state $s \in W_0$ satisfies $P$:

$$K \models P \text{ if and only if } \forall s_0 \in W. s_0 \models P$$
This definition has a strange property, where it is possible that a given structure \( K \) there exists a formula \( P \) where \( K \not\models P \) and \( K \not\models \neg P \). Find a CTL formula and (simple) transition system for which this is the case.

5. **Until, weakly (10 points).** Consider a temporal operator with the following semantics on traces \( \sigma \):

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

This is a weaker version of the normal until operator, in that it doesn’t require \( Q \) to eventually hold as long as \( P \) always does. Show that \( W \) can be expressed in terms of the temporal operators discussed in lecture 15 by writing an equivalence, and use the semantics of LTL to prove that your equivalence is correct.

*Hint: you might find it helpful to consider two cases, one in which \( \sigma \models \Diamond Q \), and another where \( \sigma \models \neg \Diamond Q \).*