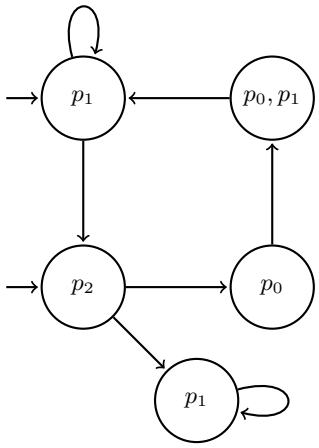
Assignment 7: Temporal Properties, Model Checking
15-414/15-424 Bug Catching: Automated Program Verification

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:

   $$\mathbf{A}(p_0 \mathbf{U} p_1) \vee \mathbf{EX}(\mathbf{AG} p_1)$$

   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. $K \models \mathbf{A}(p_0 \mathbf{U} p_1) \vee \mathbf{EX}(\mathbf{AG} p_1)$.



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

   $$\mathbf{AF}(a \wedge \mathbf{AX} a) \qquad \Diamond(a \wedge \circ a)$$

   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-statisfied 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:

   $$\Diamond(P \vee Q) \leftrightarrow \Diamond P \vee \Diamond Q$$
   $$\Diamond(P \wedge Q) \leftrightarrow \Diamond P \wedge \Diamond Q$$
   $$\Box(P \vee Q) \leftrightarrow \Box P \vee \Box Q$$
   $$\Box(P \wedge Q) \leftrightarrow \Box P \wedge \Box Q$$

   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 $K = (W, \rightharpoonup, v)$ 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 σ:

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

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* $\sigma \models \neg\Diamond Q$