ECE/CS 584: Embedded and cyberphysical system verification	Fall 2019
Dawei Sun, daweis2	*Homework 3: Temporal logics and composition*
	Due October 17^{th}

Typeset your solutions using LaTeX zip your writeup (.pdf) and code (.py) in a single file called `nedid-584-F19.zip` *and upload this file through Compass.*

Problem 1. CTL reductions (20 points) Convert the following CTL formulas to equivalent formulas that use only **E**, **X**, and **U**:

- $\mathbf{AF}\ f_1$ (infinitely often)
- $\mathbf{AG}\ f_1$ (invariance)
- $\mathbf{AFAG}\ f_1$ (stabilization)
- $\mathbf{A} f_1\ \mathbf{U}\ f_2$,

Solution

(a) $\mathbf{AF}\ f_1 \equiv \neg \mathbf{EG}\ \neg f_1$

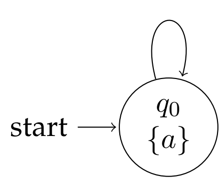
(b) $\mathbf{AG}\ f_1 \equiv \neg \mathbf{E}(\text{true}\mathbf{U}\neg f_1)$

(c) $\mathbf{AFAG}\ f_1 \equiv \neg \mathbf{EG}\ \neg(\mathbf{AG} f_1) \equiv \neg \mathbf{EG}\ \mathbf{E}[\text{true}\mathbf{U}\neg f_1]$

(d) $\mathbf{A} f_1\ \mathbf{U}\ f_2 \equiv \neg \mathbf{E}[(\neg f_2)\mathbf{U}(\neg(f_1 \vee f_2))] \vee \mathbf{EG}\neg f_2$

Problem 2. CTL to automata (8 points) Draw a finite automaton with labeled states that satisfies the CTL formula: $\mathbf{AF}(a \wedge \mathbf{AX}a)$.

Solution



Problem 3. CTL model checking (32 points) Consider the following automaton $= \langle Q, Q_0, T, L \rangle$. The set of states $Q = \{s_0, \ldots, s_4\}$, initial states $Q_0 = \{s_0, s_3\}$, the set of atomic propositions $AP = \{a, b\}$, transitions T, and the state labels L are shown in the figure.

Consider the following CTL formulas:

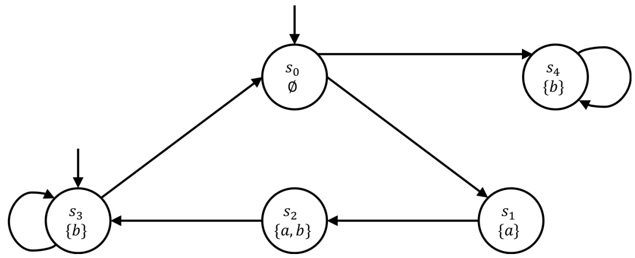


Figure 1: Automaton with state $Q = \{s_1, \ldots, s_4\}$. State labels (atomic propositions) are shown under each state.

1. $\phi_1 = \mathbf{A}(a\mathbf{U}b) \vee \mathbf{EX}(\mathbf{AG}b)$
2. $\phi_2 = \mathbf{AGA}(a\ \mathbf{U}\ b)$
3. $\phi_3 = (a \wedge b) \Rightarrow \mathbf{E\ G\ E\ X\ A}(a\ \mathbf{U}\ b\ \vee\ \mathbf{G}\ a)$
4. $\phi_4 = \mathbf{A\ G\ E\ F}\phi_3$.

For each formula ϕ_i, determine the set of states that satisfy it, and state whether satisfies it. (Problem 6.3 from [**?**])

Solution

1. For every sub-formula we write the states satisfing it.
   $\mathbf{AG}b$: s_4;
   $\mathbf{EXAG}b$: $s_0,\ s_4$;
   $\mathbf{A}(a\mathbf{U}b)$: $s_1,\ s_2,\ s_3,\ s_4$;
   ϕ_1: $s_0,\ s_1,\ s_2,\ s_3,\ s_4$; The automaton satisfies it.
2. For every sub-formula we write the states satisfing it.
   $\mathbf{A}(a\mathbf{U}b)$: $s_1,\ s_2,\ s_3,\ s_4$;
   ϕ_2: s_4; The automaton doesn't satisfy it.
3. For every sub-formula we write the states satisfing it.
   $\mathbf{A}(a\mathbf{U}b \vee \mathbf{G}a)$: $s_1,\ s_2,\ s_3,\ s_4$; $\mathbf{EXA}(a\mathbf{U}b \vee \mathbf{G}a)$: $s_0,\ s_1,\ s_2,\ s_3,\ s_4$;
   $\mathbf{EGEXA}(a\mathbf{U}b \vee \mathbf{G}a)$: $s_0,\ s_1,\ s_2,\ s_3,\ s_4$;
   $\phi_3 = \neg(a \wedge b) \vee \mathbf{EGEXA}(a\mathbf{U}b \vee \mathbf{G}a)$: $s_0,\ s_1,\ s_2,\ s_3,\ s_4$; The automaton satisfies it.
4. For every sub-formula we write the states satisfing it.
   ϕ_4: $s_0,\ s_1,\ s_2,\ s_3,\ s_4$; The automaton satisfies it.

Problem 4. CTL equivalences (30 points) Let ϕ, ψ be arbitrary CTL formulas. Which of the following equivalences for CTL formulas are correct. Either give a proof or a counterexample.

1. $\mathbf{AXAF}\ \phi \equiv \mathbf{AFAX}\ \phi$
2. $\neg\mathbf{A}(\ \phi\ \mathbf{U}\ \psi) \equiv \mathbf{E}(\ \phi\ \mathbf{U}\ \neg\psi)$
3. $(\phi \Rightarrow \mathbf{AX}\phi) \wedge (\psi \Rightarrow \mathbf{AX}\psi) \equiv (\phi \wedge \psi) \Rightarrow \mathbf{AX}(\phi \wedge \psi)$

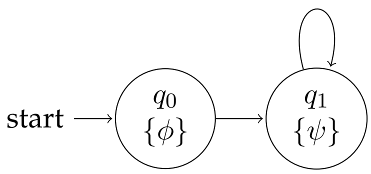
Solution

1. True. First, for state q, we write the semantic of the LHS and RHS. LHS $\iff$ "$\forall\alpha$ such that $\alpha[0] = q$ and $\forall\beta$ such that $\beta[0] = \alpha[1]$, we have $\exists i \geq 0$, $\beta[i] \models \phi$" $\iff$ "$\forall\alpha$ such that $\alpha[0] = q$, we have $\exists i \geq 1$, $\alpha[i] \models \phi$". RHS $\iff$ "$\forall\alpha$ such that $\alpha[0] = q$, $\exists i \geq 0$, $\forall\beta$ such that $\beta[0] = \alpha[i]$, we have $\beta[1] \models \phi$".

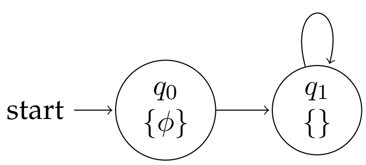
   Then we prove RHS $\implies$ LHS. For all path starting from q, suppose for some $i \geq 0$, $\forall\beta$ such that $\beta[0] = \alpha[i]$, we have $\beta[1] \models \phi$. We can simplily choose β as the suffix of α, then we get $\alpha[i+1] \models \phi$, which implies the LHS.

   Finally, we prove LHS $\implies$ RHS. We preceeds by contradiction. Suppose there exists a path α such that $\forall i \geq 0$, $\alpha[i]$ always has a next state which doesn't satisfy ϕ. Then, we can always follow these next states which don't satisfy ϕ, and thus we find a path where ϕ is never satisfied, which is contradicted to the LHS. Thus, we proved LHS $\implies$ RHS.

2. False. This is a counterexample satisfying the RHS while not satisfying the LHS.



3. False. This is a counterexample satisfying the RHS while not satisfying the LHS.



Problem 5. Composition (10 points) Give an example of a pair of compatible HIOAs whose composition is a not an HIOA.

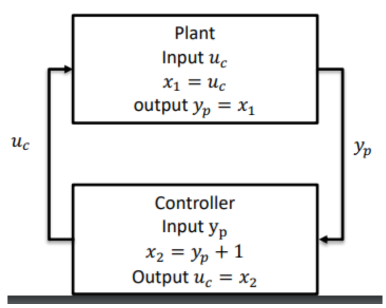


Figure 2: Composition of two HIOA's is not an HIOA.

Solution As shown in Fig. 2, "Plant" and "Controller" are two compatible HIOA's. However, after composition, we have $x_1 = x_1 + 1$, which is because there is a cyclic dependence in the variables.