Basics of Verification

Midterm exam, November 15, 2019

Duration: 2H

Authorized documents: all.
All answers should be rigorously and clearly justified.
Questions are independent.
The number in front of each question gives an indication on its length or difficulty.

1 CTL and CTL^*

Fix $\text{AP} = \{p, q, r\}$. The goal is to see whether the CTL^* formula

$$\varphi_1 = \mathsf{E}((p \,\mathsf{U}\, q) \,\mathsf{U}\, r)$$

can be expressed in CTL. Consider the following CTL formulæ:

$$\varphi_2 = \mathsf{E}((p \vee q) \,\mathsf{U}\, r)$$
$$\varphi_3 = \mathsf{E}((p \vee q) \,\mathsf{U}\, (r \wedge \mathsf{E}(p \,\mathsf{U}\, q)))$$

Let ψ_1, ψ_2 be two CTL^* *state* formulæ. Recall that ψ_1 implies ψ_2 (resp. ψ_1 and ψ_2 are equivalent) if for all models M and all states s of M, we have $M, s \models \psi$ implies $M, s \models \psi_2$ (resp. $M, s \models \psi_1$ if and only if $M, s \models \psi_2$).

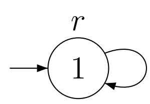
[4] **a)** Show that φ_1 implies φ_2, but φ_1 and φ_2 are not equivalent.
Show that φ_3 implies φ_1, but φ_1 and φ_3 are not equivalent.

Answer: We have $p \,\mathsf{U}\, q$ implies $p \vee q$, hence also $(p \,\mathsf{U}\, q) \,\mathsf{U}\, r$ implies $(p \vee q) \,\mathsf{U}\, r$. It follows that φ_1 implies φ_2.

The converse is false. Consider the model $M_1 =$

We have $M_1, 1 \models \varphi_2$ but $M_1, 1 \not\models \varphi_1$.
We show now that φ_3 implies φ_1. Let M be a model and s a state such that $M, s \models \varphi_3$. There is a run σ starting from s and $j \geq 0$ such that $M, \sigma, j \models r \wedge \mathsf{E}(p \,\mathsf{U}\, q)$ and $M, \sigma, i \models p \vee q$ for $0 \leq i < j$.
There is a run σ' with $\sigma[j] = \sigma'[j]$ (same prefix up to j) such that $M, \sigma', j \models p \,\mathsf{U}\, q$. Using $\sigma[j] = \sigma'[j]$ and $M, \sigma, i \models p \vee q$ for $i < j$, we deduce that $M, \sigma', i \models p \,\mathsf{U}\, q$ for $i < j$. Since $M, \sigma', j \models r$ we obtain $M, s \models \varphi_1$.

Once again, the converse is false. Consider the model $M_2 =$



.
We have $M_2, 1 \models \varphi_1$ but $M_2, 1 \not\models \varphi_3$.

[5] **b)** Prove that φ_1 can be expressed in CTL, i.e., give a CTL formula φ_4 and show that φ_1 and φ_4 are equivalent.

> **Answer:** $\varphi_4 = r \vee \varphi_3 \vee \varphi_5$ where $\varphi_5 = \mathsf{E}(p \vee q) \,\mathsf{U}\, (q \wedge \mathsf{EX}\, r)$.
> We show now that φ_1 implies φ_4. Let M be a model and s a state such that $M, s \models \varphi_1$. There is a run σ starting from s and $j \geq 0$ such that $M, \sigma, j \models r$ and $M, \sigma, i \models p \,\mathsf{U}\, q$ for $0 \leq i < j$.
> If $j = 0$ then $M, s \models r$, hence $M, s \models \varphi_4$. We assume below that $j > 0$.
> If $M, \sigma, j-1 \models q$ then $M, \sigma, 0 \models (p \vee q) \,\mathsf{U}\, (q \wedge \mathsf{EX}\, r)$ and $M, s \models \varphi_5$.
> Otherwise, $M, \sigma, j-1 \models p \wedge \neg q$. Since $M, \sigma, j-1 \models p \,\mathsf{U}\, q$ we deduce $M, \sigma, j \models p \,\mathsf{U}\, q$. Therefore, $M, s \models \varphi_3$.
> Conversely, r clearly implies φ_1 and we have seen above that φ_3 implies φ_1. It remains to show that φ_5 implies φ_1. If $M, s \models \varphi_5$, there is a run σ starting from s and some $j \geq 0$ with $M, \sigma, j+1 \models r$, $M, \sigma, j \models q$ and $M, \sigma, i \models p \vee q$ for $i < j$. We deduce that $M, \sigma, i \models p \,\mathsf{U}\, q$ for all $i < j+1$. Hence, $M, s \models \varphi_1$.

2 LTL and Büchi transducers

The flow of time is $(\mathbb{N}, <)$, AP $\neq \emptyset$ is the set of atomic propositions and $\Sigma = 2^{\mathrm{AP}}$.

In addition to the usual LTL future modalidies X and U, we define two new binary modalities, U_2 and U'_2.

The semantics is defined as follows. Let $w = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ be an infinite word and $i \in \mathbb{N}$.

$$
\begin{array}{ll}
w, i \models \varphi \,\mathsf{U}_2\, \psi & \text{if } \exists k \geq 0 \text{ with } w, i+2k \models \psi \text{ and } w, i+2j \models \varphi \text{ for all } 0 \leq j < k \\
w, i \models \varphi \,\mathsf{U}'_2\, \psi & \text{if } \exists k \geq 0 \text{ with } w, i+2k \models \psi \text{ and } w, i+j \models \varphi \text{ for all } 0 \leq j < 2k
\end{array}
$$

As usual, we denote by $\mathcal{L}(\varphi) = \{w \in \Sigma^\omega \mid w, 0 \models \varphi\}$. Also, we let $\mathsf{F}_2\, \varphi = \top \,\mathsf{U}_2\, \varphi$.

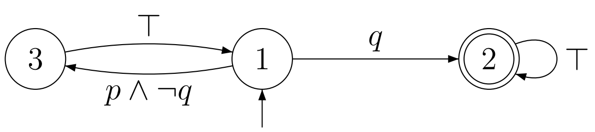
Remark: $F_2\, q$ cannot be expressed in LTL(X, U).

[2] **a)** Show that $\varphi \,\mathsf{U}'_2\, \psi$ can be expressed in LTL($\mathsf{X}, \mathsf{U}, \mathsf{U}_2$).
Show that $\varphi \,\mathsf{U}\, \psi$ can be expressed in LTL(X, U_2).

> **Answer:** $\varphi \,\mathsf{U}'_2\, \psi \equiv (\varphi \wedge \mathsf{X}\,\varphi) \,\mathsf{U}_2\, \psi$ and $\varphi \,\mathsf{U}\, \psi \equiv \varphi \,\mathsf{U}'_2\, (\psi \vee (\varphi \wedge \mathsf{X}\,\psi))$.

[1] **b)** Let $p, q \in$ AP. Give a deterministic Büchi automaton which recognizes $\mathcal{L}(p \,\mathsf{U}_2\, q)$.

> **Answer:**



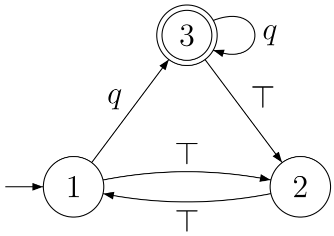
[2] **c)** Let $p, q \in$ AP. Give an MSO(AP, $<$) formula $\Phi(x)$ with one (first-order) free variable which is equivalent to $p \,\mathsf{U}_2\, q$, i.e., for all $w \in \Sigma^\omega$ and all $i \in \mathbb{N}$, we have

$$w, i \models p \,\mathsf{U}_2\, q \text{ iff } w, [x \mapsto i] \models \Phi.$$

> **Answer:** $\Phi(x) = \exists z \exists Y,\ q(z) \wedge z \in Y \wedge \forall y \in Y \setminus \{x\}, \exists y_1, y_2\ (p(y_1) \wedge y_1 \lessdot y_2 \lessdot y)$
> where $u \lessdot v = u < v \wedge \neg \exists w (u < w < v)$.

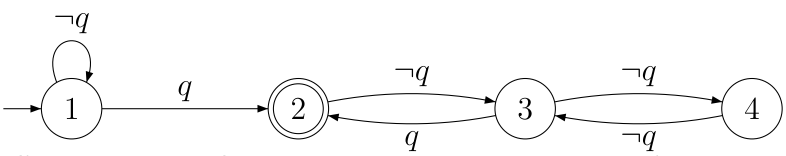
[3] **d)** Let $q \in \mathrm{AP}$. Give a Büchi automaton $\mathcal{A}_1$ which recognizes $L_1 = \mathcal{L}(\mathsf{G}\,\mathsf{F}_2\, q)$.
Hint: Give a non-deterministic Büchi automaton with 3 states.

Answer: Notice that $w \in L_1$ iff w contains infinitely many odd positions satisfying q and infinitely many even positions satisfying q. Hence $L_1 = ((\Sigma\Sigma)^*\Sigma_q)^\omega$. Hence,

$\mathcal{A}_1 =$ 

[3] **e)** Let $q \in \mathrm{AP}$ and consider the language $L_2 = \Sigma_{\neg q}^*(\Sigma_q\Sigma_{\neg q}(\Sigma_{\neg q}\Sigma_{\neg q})^*)^\omega$.
Give a deterministic Büchi automaton $\mathcal{A}_2$ which recognizes L_2.
Give a formula $\varphi_2 \in \mathrm{LTL}(\mathsf{X}, \mathsf{U}_2)$ which defines L_2.

Answer:



Notice that $w \in L_2$ iff w contains infinitely many odd positions satisfying q **or** infinitely many even positions satisfying q **but not both**.

$$\begin{aligned}\varphi_2 &= (\neg q \,\mathsf{U}\, (q \wedge \neg\,\mathsf{X}\,\mathsf{F}_2\; q)) \wedge \mathsf{G}(q \to \mathsf{X}\,\mathsf{X}\,\mathsf{F}_2\; q)\\ &\equiv \mathsf{F}\, q \wedge \mathsf{G}(q \to \mathsf{X}\,\mathsf{X}\,\mathsf{F}_2\; q) \wedge \neg\,\mathsf{G}\,\mathsf{F}_2\; q\end{aligned}$$

[3] **f)** Let $q \in \mathrm{AP}$ and consider $\varphi = \mathsf{G}(q \to \mathsf{X}\,\mathsf{X}\,\mathsf{F}_2\; q)$.
Show that $L_1 \cap L_2 = \emptyset$ and $L_1 \cup L_2 \subseteq L = \mathcal{L}(\varphi)$.
Give a Büchi automaton $\mathcal{A}_3$ which recognizes $L_3 = L \setminus (L_1 \cup L_2)$.

Answer: From the discussion above, we know that $L_1 \cap L_2 = \emptyset$.
Now, $\mathcal{L}(\varphi)$ is the set of words w such that if w satisfies q in some position i (odd or even) then it contains infinitely many positions satisfying q **with the same parity as** i. We deduce that $L_1 \cup L_2 \subseteq L$ and that L_3 is the set of words which never satisfy q: $L_3 = \mathcal{L}(\mathsf{G}\,\neg q) = (\Sigma_{\neg q})^\omega$. Therefore, $\mathcal{A}_3 =$