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

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

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

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

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.

[4] **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.

2 LTL and Büchi transducers

The flow of time is $(\mathbb{N}, <)$, $\mathrm{AP} \neq \emptyset$ 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 $\mathrm{LTL}(\mathsf{X}, \mathsf{U})$.

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

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

[2] **c)** Let $p, q \in \mathrm{AP}$. Give an $\mathrm{MSO}(\mathrm{AP}, <)$ 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

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

[2] **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.

[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.

[2] **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 $L_3 = L \setminus (L_1 \cup L_2)$.