Basics of Verification

Written exam, November 30, 2011

3 hours

The lecture notes are the only authorized documents.
Exercises are independent.
All answers should be rigorously and clearly justified.
The number in front of each question gives an indication on its length or difficulty.

Warning: In the whole problem, F, G, U, S and R denote the *non-strict* versions of these modalities. The *strict* versions of until and since are denoted $\mathsf{U}_<$ and $\mathsf{S}_<$.

1 Reduction of LTL formulæ

Fix a set AP of atomic propositions and let $\Sigma = 2^{\mathrm{AP}}$.

The class of *eventuality* formulæ is defined by the syntax

$$\alpha ::= \mathsf{F}\,\varphi \mid \alpha \vee \alpha \mid \alpha \wedge \alpha \mid \mathsf{X}\,\alpha \mid \varphi\,\mathsf{U}\,\alpha \mid \alpha\,\mathsf{R}\,\alpha$$

where φ ranges over all LTL formulæ.

[2] **a)** Show that for all eventuality formulæ α, for all $w \in \Sigma^\omega$ and all $0 \leq i \leq j$ we have

$$w, j \models \alpha \quad \Longrightarrow \quad w, i \models \alpha$$

The class of *alternating* formulæ is defined by the syntax

$$\beta ::= \mathsf{G}\,\alpha \mid \neg\beta \mid \beta \vee \beta \mid \mathsf{X}\,\beta \mid \varphi\,\mathsf{U}\,\beta$$

where α ranges over all eventuality formulæ and φ ranges over all LTL formulæ.

[2] **b)** Show that for all alternating formulæ β, for all $w \in \Sigma^\omega$ and all $0 \leq i \leq j$ we have

$$w, j \models \beta \quad \Longleftrightarrow \quad w, i \models \beta$$

[1] **c)** Show that for all alternating formulæ β and all LTL formulæ φ the formulæ β, $\mathsf{X}\,\beta$, $\varphi\,\mathsf{U}\,\beta$ and $\varphi\,\mathsf{R}\,\beta$ are all equivalent, i.e., for all $w \in \Sigma^\omega$ and all $i \geq 0$ we have

$$w, i \models \beta \quad \Longleftrightarrow \quad w, i \models \mathsf{X}\,\beta \quad \Longleftrightarrow \quad w, i \models \varphi\,\mathsf{U}\,\beta \quad \Longleftrightarrow \quad w, i \models \varphi\,\mathsf{R}\,\beta$$

2 Ehrenfeucht-Fraïssé games

The aim is to show that X cannot be expressed in $\mathrm{TL}(\mathrm{AP}, \mathsf{S}, \mathsf{U})$ over $(\mathbb{N}, <)$.

Let $\mathrm{AP} = \{p\}$ so that $\Sigma = 2^{\mathrm{AP}} = \{a, b\}$ with $a = \emptyset$ and $b = \{p\}$.

Fix some $n \geq 2$ and consider the infinite word $w = a^n b^\omega \in \Sigma^\omega$.

[4] **a)** Show that, for all $k \in \mathbb{N}$, for all $i_0, i_1 \in \mathbb{N}$ such that either $i_0, i_1 < n$ or $i_0, i_1 \geq n$, we have $(w, i_0) \sim_k (w, i_1)$ in the EF-game using only S and U moves.

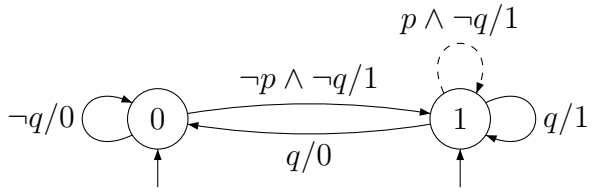
[1] **b)** Show that $\mathsf{X}\,p$ is not expressible in $\mathrm{TL}(\mathrm{AP}, \mathsf{S}, \mathsf{U})$ over $(\mathbb{N}, <)$.

3 LTL and automata

Fix $\mathrm{AP} = \{p, q\}$ and let $\Sigma = 2^{\mathrm{AP}}$.

[4] **a)** Give an unambiguous synchronous Büchi transducer (SBT) $\mathcal{A} = (Q, \Sigma, I, T, F, \mu)$ with 4 states ($|Q| = 4$) and a single acceptance condition on states ($F \subseteq Q$) for the formula $\mathsf{G}\,\mathsf{F}\,q$: prove that $\mathcal{A}$ is unambiguous and that $[\![\mathcal{A}]\!] = [\![\mathsf{G}\,\mathsf{F}\,q]\!]$.

Consider the SBT $\mathcal{A} = (Q, \Sigma, I, T, S, \mu)$ with a single acceptance condition on transitions ($S \subseteq T$) described below:



The only non accepting transition of $\mathcal{A}$ is the dashed loop on state 1 labeled $p \wedge \neg q/1$.

Let $w = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ be an infinite word with $a_i \in \Sigma$ for $i \geq 0$.

[3] **b)** Show that if $q_0, a_0, q_1, a_1, q_2, \ldots$ is an accepting run of $\mathcal{A}$ then, for all $i \geq 0$, we have

$$q_i = \begin{cases} 1 & \text{if } w, i \models p\,\mathsf{U}\,q \\ 0 & \text{otherwise.} \end{cases}$$

[3] **c)** Show that there exists an accepting run of $\mathcal{A}$ on the word w.

[2] **d)** Show that $[\![\mathcal{A}]\!] = [\![p\,\mathsf{U}_<\,q]\!]$.
Deduce that for any formula $\xi \in \mathrm{TL}(\mathrm{AP}, \mathsf{S}_<, \mathsf{U}_<)$ we can construct a *generalized* SBT $\mathcal{A}_\xi$ with acceptance *on transitions*, having at most $2^{|\xi|_{\mathsf{S}_<} + |\xi|_{\mathsf{U}_<}}$ states and such that $[\![\mathcal{A}_\xi]\!] = [\![\xi]\!]$.

4 CTL **and** CTL*

Fix $\mathrm{AP} = \{p, q, r\}$. The aim 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:

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

Recall that a state formula $\psi \in \mathrm{CTL}^*$ is valid if $M, s \models \psi$ for all models M and all states s of M. Moreover, two state formulæ $\psi_1, \psi_2 \in \mathrm{CTL}^*$ are equivalent if $\psi_1 \leftrightarrow \psi_2$ is valid.

[4] **a)** Show that the formula $\varphi_1 \to \varphi_2$ is valid, but φ_1 and φ_2 are not equivalent.
Show that the formula $\varphi_3 \to \varphi_1$ is valid, but φ_1 and φ_3 are not equivalent.

[3] **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.