# Basics of Verification

Written exam, November 27, 2013

2 hours 30

*The lecture notes are the only authorized documents.*
*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 LTL and automata

Fix $\mathrm{AP} = \{p, q, r\}$ and let $\Sigma = 2^{\mathrm{AP}}$. We assume the flow of time to be $(\mathbb{T}, <) = (\mathbb{N}, <)$, hence the models are words $w \in \Sigma^\omega$. Consider the formulæ

$$\varphi = p \,\mathsf{SS}\, (q \,\mathsf{SU}\, r)$$
$$\alpha = p \,\mathsf{SS}\, (p \wedge r \wedge \mathsf{Y}\top)$$
$$\beta = \mathsf{Y}\top \wedge q \,\mathsf{U}\, r$$

[5] **a)** Show that the formulæ $\varphi$ and $\alpha \vee \beta$ are equivalent, i.e.,
$w, i \models \varphi$ if and only if $w, i \models \alpha \vee \beta$ for all words $w \in \Sigma^\omega$ and time points $i \in \mathbb{N}$.
Give a syntactically separated formula $\varphi'$ which is equivalent to $\varphi$.

[5] **b)** Give a deterministic and complete synchronous Büchi transducer $\mathcal{A}$ for the formula $\alpha$.
The SBT should have at most 3 states, all being final: $F = Q = \{1, 2, 3\}$.
Prove that the automaton is correct, i.e., $[\![\mathcal{A}]\!] = [\![\alpha]\!]$.
Hint for the proof of correctness: Give a clear semantics to each state of the automaton. For instance, give 3 LTL formulæ $\alpha_1$, $\alpha_2$, $\alpha_3$ such that for all words $w = a_0 a_1 a_2 \cdots \in \Sigma^\omega$, if $s_0, a_0, s_1, a_1, s_2, a_2, \ldots$ is the unique run of $\mathcal{A}$ on the input word $w$ then

$$\forall i \in \mathbb{N},\ \forall \ell \in Q = \{1, 2, 3\}, \qquad s_i = \ell \iff w, i \models \alpha_\ell \,.$$

## 2 CTL and CTL*

Recall that two state formulæ $\psi$ and $\psi'$ in CTL* are equivalent if for all models $M$ and all states $s$ of $M$ we have $M, s \models \psi$ if and only if $M, s \models \psi'$.

[2] **a)** Prove that the CTL* formula $\psi_1 = \mathsf{E}(p \,\mathsf{U}\, (q \,\mathsf{U}\, r))$ can be expressed in CTL, i.e., give a CTL formula $\psi_1'$ which is equivalent to $\psi_1$.

[3] **b)** Prove that the CTL* formula $\psi_2 = \mathsf{E}((p \,\mathsf{U}\, q) \wedge (r \,\mathsf{U}\, s))$ can be expressed in CTL, i.e., give a CTL formula $\psi_2'$ which is equivalent to $\psi_2$.

[5] **c)** Consider the CTL* formulæ $\psi_3 = \mathsf{AF}(p \wedge \mathsf{G}\, q)$ and $\psi_4 = \mathsf{AF}(p \wedge \mathsf{AG}\, q)$.
Show that $\psi_4$ implies $\psi_3$, i.e., for all models $M$ and all states $s$ of $M$ we have $M, s \models \psi_4$ implies $M, s \models \psi_3$.
Show that the formulæ $\psi_3$ and $\psi_4$ are not equivalent by giving a model $M$ with at most 4 states and a state $s$ of $M$ such that $M, s \models \psi_3$ but $M, s \not\models \psi_4$.

# 3 Ehrenfeucht-Fraïssé games

The aim is to show that $\mathsf{X}$ 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 $\mathsf{S}$ and $\mathsf{U}$ moves.

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