Basics of Verification

Written exam, November 28, 2012

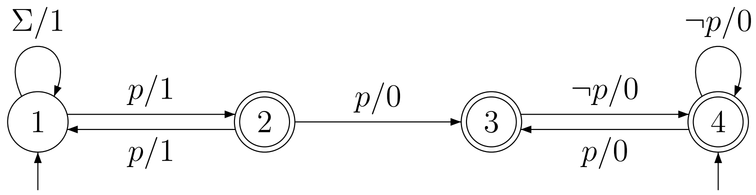
2 hours 30

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.

Each automaton should be *drawn neatly*. Hence, it is advised to draw the automaton first on the draft sheet and to think about the placement of states before drawing the automaton on the answer sheet.

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

Consider the synchronous Büchi transducer (SBT) $\mathcal{A} = (Q, \Sigma, I, T, F, \mu)$ described below:



[5] **a)** Show that $\mathcal{A}$ is ambiguous, i.e., give two accepting runs of $\mathcal{A}$ over the same infinite word $u \in \Sigma^\omega$.
Show that $\mathcal{A}$ is complete, i.e., there is an accepting run of $\mathcal{A}$ for each input infinite word $u \in \Sigma^\omega$.
Let $(u, v) \in [\![\mathcal{A}]\!] \subseteq \Sigma^\omega \times \{0,1\}^\omega$ with $u = a_0a_1a_2\cdots$ and $v = b_0b_1b_2\cdots$. Show that for all $i \geq 0$, we have $b_i = 1$ if and only if $u, i \models \mathsf{F}(p \wedge \mathsf{X}\, p)$.

[4] **b)** Give an unambiguous SBT $\mathcal{A}_1$ with two states such that $[\![\mathcal{A}_1]\!] = [\![p \wedge \mathsf{X}\, p]\!]$, i.e., such that for all $(u, v) \in [\![\mathcal{A}_1]\!]$ with $u = a_0a_1a_2\cdots$ and $v = b_0b_1b_2\cdots$ and all $i \geq 0$, we have $b_i = 1$ if and only if $u, i \models p \wedge \mathsf{X}\, p$.
Give an unambiguous SBT $\mathcal{A}_2$ such that $[\![\mathcal{A}_2]\!] = [\![\mathsf{F}(p \wedge \mathsf{X}\, p)]\!]$ by composing $\mathcal{A}_1$ with the 3-states SBT for the F modality.

We introduce now a new modality U_1 which constrains the eventuality to occur after an *odd* number of steps. Formally, given an infinite word $u \in \Sigma^\omega$ and a position $i \geq 0$, we define the semantics as follows

$$u, i \models \varphi \,\mathsf{U}_1\, \psi \text{ if } \exists k \; \big[i \leq k \;\;\&\;\; k - i \text{ is odd } \;\&\;\; w, k \models \psi \;\;\&\;\; \forall j \; (i \leq j < k \rightarrow w, j \models \varphi)\big]$$

For instance, with $u = cbbdbbdbacbbbbbca^\omega$ where $a = \emptyset$, $b = \{p\}$, $c = \{q\}$ and $d = \{p, q\}$, we have $[\![p \,\mathsf{U}_1\, q]\!](u) = 01110100001010100^\omega$.

[4] **c)** Show that $\varphi \,\mathsf{U}_1\, \psi \equiv (\varphi \wedge \mathsf{X}\,\psi) \vee (\varphi \wedge \mathsf{X}\,\varphi \wedge \mathsf{X}\,\mathsf{X}(\varphi \,\mathsf{U}_1\, \psi))$.
Show that $\neg(\varphi \,\mathsf{U}_1\, \psi) \equiv \neg\varphi \vee \mathsf{X}(\neg\psi \wedge (\neg\varphi \vee \mathsf{X}\,\neg(\varphi \,\mathsf{U}_1\, \psi)))$.
Give a Büchi automaton (BA) $\mathcal{B}_1$ with at most 3 states which accepts the language $\mathcal{L}(\mathcal{B}_1) = \{u \in \Sigma^\omega \mid u, 0 \models p \,\mathsf{U}_1\, q\}$.
Give a Büchi automaton (BA) $\mathcal{B}_2$ with at most 3 states which accepts the language $\mathcal{L}(\mathcal{B}_2) = \{u \in \Sigma^\omega \mid u, 0 \models \neg(p \,\mathsf{U}_1\, q)\}$.

[5] **d)** Here, we consider the formula $\mathsf{F}_1\, p = \top \,\mathsf{U}_1\, p$.
Give an unambiguous SBT $\mathcal{A}_3$ which computes $[\![\mathsf{F}_1\, p]\!]$.

[6] **e)** For $n \geq 0$, let $w_n = a^n b a^\omega$ with $a = \emptyset$ and $b = \{p\}$. In this question, we consider Ehrenfeucht-Fraïssé games (EF-games) using only SU-moves.
Show that spoiler has a winning strategy starting from $(w_3, 0, w_n, 0)$ in the 3-round EF-game when $n \neq 3$, i.e., $(w_3, 0) \not\sim_3 (w_n, 0)$.
Show that duplicator has a winning strategy starting from $(w_m, 0, w_n, 0)$ in the k-round EF-game when $m, n > k$, i.e., $(w_m, 0) \sim_k (w_n, 0)$.
Show that $\mathsf{F}_1\, p$ is not expressible in $\mathrm{TL}(\mathrm{AP}, \mathsf{SU})$.
Show (without using further EF-games) that $\mathsf{F}_1\, p$ is not expressible in $\mathrm{TL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$.

We turn now to the extension of CTL with formulae of the form $\mathsf{E}\,\varphi \,\mathsf{U}_1\, \psi$ and $\mathsf{E}\,\varphi \,\mathsf{U}_0\, \psi$. We first give the semantics. Let $M = (S, T, I, \mathrm{AP}, \ell)$ be a Kripke structure without deadlocks and let $s \in S$.

$$\begin{aligned} s \models \mathsf{E}\,\varphi \,\mathsf{U}_1\, \psi \quad &\text{if} \quad \exists s = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \cdots s_k \text{ finite path of } M \text{ with } k \text{ odd} \\ &\qquad\qquad \text{such that } s_k \models \psi \;\;\&\;\; s_j \models \varphi \text{ for all } 0 \leq j < k \\ s \models \mathsf{E}\,\varphi \,\mathsf{U}_0\, \psi \quad &\text{if} \quad \exists s = s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \cdots s_k \text{ finite path of } M \text{ with } k \text{ even} \\ &\qquad\qquad \text{such that } s_k \models \psi \;\;\&\;\; s_j \models \varphi \text{ for all } 0 \leq j < k \end{aligned}$$

[6] **f)** Show that $\mathsf{E}\,\varphi \,\mathsf{U}\, \psi \equiv \mathsf{E}\,\varphi \,\mathsf{U}_0\, \psi \vee \mathsf{E}\,\varphi \,\mathsf{U}_1\, \psi$.
Show that $\mathsf{E}\,\varphi \,\mathsf{U}_1\, \psi \equiv \varphi \wedge \mathsf{EX}(\mathsf{E}\,\varphi \,\mathsf{U}_0\, \psi)$.
Is the formula $\mathsf{E}\,p \,\mathsf{U}_0\, q \wedge \mathsf{E}\,p \,\mathsf{U}_1\, q$ satisfiable?
Modify the procedure given in the lecture which computes the semantics of $\mathsf{E}\,\varphi_1 \,\mathsf{U}\, \varphi_2$ in order to compute simultaneously the semantics of the two formulae $\mathsf{E}\,\varphi_1 \,\mathsf{U}_0\, \varphi_2$ and $\mathsf{E}\,\varphi_1 \,\mathsf{U}_1\, \varphi_2$. The new algorithm should run in time $\mathcal{O}(|S| + |T|)$ (assuming the semantics of φ_1 and φ_2 have already been computed). Prove that your algorithm is correct.