Basics of Verification

Midterm exam, November 9, 2017

2 hours

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 FO and MSO

The flow of time is $(\mathbb{N}, <)$ and AP is the set of atomic propositions.

[1] **a)** Let $\psi(x, y) \in \mathrm{FO}(\mathrm{AP}, <)$ be a first-order formula with two free variables x and y. Give an $\mathrm{MSO}(\mathrm{AP}, <)$ formula $\psi^+(x, y)$ defining the transitive closure of the relation defined by ψ.

Below, we fix $\mathrm{AP} = \{p, q\}$, $a = \{p\}$ and $b = \{q\}$.

[1] **b)** Give an $\mathrm{FO}(\mathrm{AP}, <)$ formula $\varphi(x, y)$ with two free variables x and y defining the following binary relation:

- x is labeled b, y is labeled a and y is on the left of x, or
- x is labeled a and y is the first position on the right of x which is labeled b.

[3] **c)** Show that the transitive closure of the binary relation defined above can be defined with an $\mathrm{FO}(\mathrm{AP}, <)$ formula $\varphi^\oplus(x, y)$ and give this formula $\varphi^\oplus(x, y)$.

2 LTL

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

[2] **a)** Given $p \in \mathrm{AP}$ and $\varphi \in \mathrm{TL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$, construct a formula $\widetilde{\varphi} \in \mathrm{TL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$ such that

$$\forall u \in \Sigma_{\neg p}^* \Sigma_p, \forall v \in \Sigma^\omega, \forall i \geq 0: \qquad v, i \models \varphi \quad \text{iff} \quad uv, |u| + i \models \widetilde{\varphi}\,.$$

[1] **b)** Given $p \in \mathrm{AP}$ and $\varphi \in \mathrm{TL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$, construct a formula $\overline{\varphi} \in \mathrm{TL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$ such that

$$\forall u \in \Sigma_{\neg p}^* \Sigma_p, \forall v \in \Sigma^\omega: \qquad v, 0 \models \varphi \quad \text{iff} \quad uv, 0 \models \overline{\varphi}\,.$$

3 CTL and CTL*

Let ψ and ψ' be two state formulæ in CTL*. Recall that ψ implies ψ' if for all models M and all states s of M we have $M, s \models \psi$ implies $M, s \models \psi'$.

Given $p \in \mathrm{AP}$, we consider the formulæ

$$\varphi_1 = \mathsf{AF}(p \wedge \mathsf{X}\, p) \qquad \varphi_2 = \mathsf{AF}(p \wedge \mathsf{EX}\, p) \qquad \varphi_3 = \mathsf{AF}(p \wedge \mathsf{AX}\, p)\,.$$

[5] **a)** For each pair of indices $(i, j) \in \{1, 2, 3\}$, either prove that φ_i implies φ_j or give a model and a state showing that φ_i does not imply φ_j.

4 LTL and Büchi transducers

The flow of time is $(\mathbb{N}, <)$, $\mathrm{AP} = \{p, q\}$ is the set of atomic propositions and $\Sigma = 2^{\mathrm{AP}}$. Let $a = p \wedge \neg q$, $b = \neg p \wedge q$, $c = p \wedge q$ and $d = \neg p \wedge \neg q$.

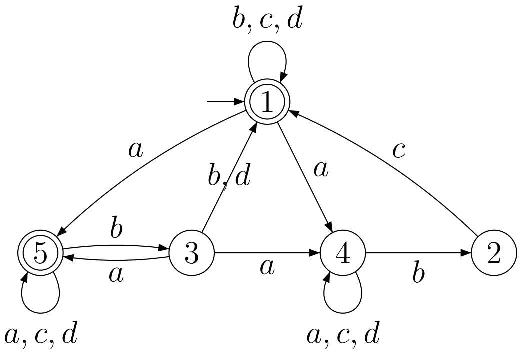
The goal is to construct an unambiguous sequential Büchi transducer $\mathcal{A}$ for the $\mathrm{TL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ formula $\varphi = a \wedge (\neg b \,\mathsf{U}\, (b \wedge \mathsf{X}\, c))$.

Consider the $\mathrm{TL}(\mathrm{AP}, \mathsf{SU}, \mathsf{SS})$ formulæ

$$\begin{aligned} \varphi_1 &= \neg(\varphi_2 \vee \varphi_3 \vee \varphi_4 \vee \varphi_5) & & \\ \varphi_2 &= c \wedge \mathsf{Y}(b \wedge \varphi_4) & \varphi_4 &= (\neg b \,\mathsf{SS}\, a) \wedge (\neg b \,\mathsf{U}\, (b \wedge \mathsf{X}\, c)) \\ \varphi_3 &= \neg c \wedge \mathsf{Y}(b \wedge \varphi_5) & \varphi_5 &= (\neg b \,\mathsf{SS}\, a) \wedge \neg(\neg b \,\mathsf{U}\, (b \wedge \mathsf{X}\, c))\,. \end{aligned}$$

[2] **a)** Show that the formulæ $\varphi_2, \varphi_3, \varphi_4, \varphi_5$ are mutually exclusive, i.e., show that for all $2 \leq k < \ell \leq 5$ the formula $\varphi_k \wedge \varphi_\ell$ is not satisfiable.

We consider the following Büchi automaton $\mathcal{A}$.



[6] **b)** Prove 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 an accepting run of $\mathcal{A}$ on the input word w then

$$\forall i \in \mathbb{N},\ \forall \ell \in Q = \{1, 2, 3, 4, 5\}, \qquad s_i = \ell \Longrightarrow w, i \models \varphi_\ell\,.$$

[2] **c)** Prove that $\mathcal{A}$ is unambiguous and that $\mathcal{L}(\mathcal{A}) = \Sigma^\omega$.

[2] **d)** Add outputs in $\{0, 1\}$ to transitions of $\mathcal{A}$ in order to get a sequential Büchi transducer $\mathcal{B}$ such that $[\![\mathcal{B}]\!] = [\![\varphi]\!]$.