Basics of Verification

Midterm exam, November 8, 2018

Duration: 2H30

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

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

We consider the LTL formulæ

$$\varphi_1 = (p \mathsf{U} q) \mathsf{U} r \qquad \varphi_2 = (p \vee q) \mathsf{U} r \qquad \varphi_3 = (p \vee q) \mathsf{U} (r \wedge (p \mathsf{U} q)) .$$

[3] **a)** Compare the formulæ (φ_1, φ_2) and (φ_1, φ_3), i.e., for $(i, j) \in \{(1, 2), (2, 1), (1, 3), (3, 1)\}$ either prove that φ_i implies φ_j or give a word and a position showing that φ_i does not imply φ_j.

[2] **b)** Give a formula $\varphi_4 \in \mathrm{LTL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ which is equivalent to φ_1 and with no until nested on the left, i.e., if $\alpha \mathsf{U} \beta$ is a subformula of φ_4 then $\alpha \in \mathrm{LTL}(\mathrm{AP}, \mathsf{X})$.

2 CTL and CTL*

We are only interested in runs visiting finitely often states satisfying some $c \in \mathrm{AP}$. Hence, we define path quantifiers E_c and A_c as

$$\mathsf{E}_c \varphi = \mathsf{E}(\mathsf{F}\mathsf{G} \neg c \wedge \varphi) \qquad \mathsf{A}_c \varphi = \mathsf{A}(\mathsf{F}\mathsf{G} \neg c \implies \varphi) .$$

We consider $\mathrm{CTL}_c(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ defined by the syntax

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathsf{E}_c \mathsf{X} \varphi \mid \mathsf{E}_c \varphi \mathsf{U} \varphi \mid \mathsf{E}_c \mathsf{G} \varphi$$

where $p \in \mathrm{AP}$.

[1] **a)** Show that we can add $\mathsf{A}_c \mathsf{X} \varphi$ and $\mathsf{A}_c \varphi \mathsf{U} \varphi$ to the syntax above without changing the expressive power of $\mathrm{CTL}_c(\mathrm{AP}, \mathsf{X}, \mathsf{U})$.

[3] **b)** Prove that $\mathrm{CTL}_c(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ formulæ can be expressed in $\mathrm{CTL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$, i.e., for all formula $\varphi \in \mathrm{CTL}_c(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ we can construct an equivalent formula $\overline{\varphi} \in \mathrm{CTL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$.

[2] **c)** Prove that $\mathrm{CTL}(\mathrm{AP}, \mathsf{X}, \mathsf{U})$ is more expressive than $\mathrm{CTL}_c(\mathrm{AP}, \mathsf{X}, \mathsf{U})$.

3 LDL and Büchi transducers

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

We define the Linear Dynamic Logic (LDL). In LDL, we have *position* formulæ σ and *path* formulæ π. The syntax is given by

$$\sigma ::= p \mid \sigma \vee \sigma \mid \neg\sigma \mid \langle\pi\rangle$$
$$\pi ::= \mathsf{test}(\sigma) \mid \leftarrow \mid \rightarrow \mid \pi + \pi \mid \pi \cdot \pi \mid \pi^*$$

where $p \in \mathrm{AP}$. The semantics is defined as follows. Let $w = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ be an infinite word and $i, j \in \mathbb{N}$. Position formulæ have one implicit free variable, so we define when $w, i \models \sigma$, whereas path formulæ have two implicit free variables (the endpoints of the path) and we define when $w, i, j \models \pi$.

$$\begin{array}{rl}
w, i \models p & \text{if } p \in a_i \\
w, i \models \sigma_1 \vee \sigma_2 & \text{if } w, i \models \sigma_1 \text{ or } w, i \models \sigma_2 \\
w, i \models \neg\sigma & \text{if } w, i \not\models \sigma \\
w, i \models \langle\pi\rangle & \text{if } w, i, j \models \pi \text{ for some } j \in \mathbb{N} \\
w, i, j \models \mathsf{test}(\sigma) & \text{if } j = i \text{ and } w, i \models \sigma \\
w, i, j \models \leftarrow & \text{if } j = i - 1 \\
w, i, j \models \rightarrow & \text{if } j = i + 1 \\
w, i, j \models \pi_1 + \pi_2 & \text{if } w, i, j \models \pi_1 \text{ or } w, i, j \models \pi_2 \\
w, i, j \models \pi_1 \cdot \pi_2 & \text{if } w, i, k \models \pi_1 \text{ and } w, k, j \models \pi_2 \text{ for some } k \in \mathbb{N} \\
w, i, j \models \pi^* & \text{if } \exists i = i_0, i_1, \ldots, i_k = j \text{ such that } w, i_{\ell-1}, i_\ell \models \pi \text{ for all } 0 < \ell \leq k
\end{array}$$

Notice that in the semantics of π^* we may have $k = 0$ and this implies $j = i$. We often simply write $\pi_1\pi_2$ instead of $\pi_1 \cdot \pi_2$.

[1] **a)** With $\mathrm{AP} = \{p, q, r\}$, we consider the formula $\pi = (\mathsf{test}(p){\rightarrow}{\rightarrow} + \mathsf{test}(q){\rightarrow})^*\mathsf{test}(r)$ and the word $w = \{q\}\{p\}\emptyset\{p,q\}\{p\}\{p\}\{p\}\{p\}\{p,r\}(\{q\}\{p\}\{r\}\{p\}\{q\}\{r\})^\omega$. Give all positions $i \in \mathbb{N}$ such that $w, i \models \langle\pi\rangle$.

[2] **b)** Give an LDL position formula σ such that for all $i \in \mathbb{N}$ and $w \in \Sigma^\omega$ we have $w, i \models \sigma$ iff w initially satisfies $p \,\mathsf{SU}\, q$, i.e., $w, 0 \models p \,\mathsf{SU}\, q$.

[1] **c)** Consider the $\mathrm{FO}(\mathrm{AP}, <)$ formula

$$\varphi(x) = r(x) \wedge \exists y(x < y \wedge p(y) \wedge \exists z(z < y \wedge q(z) \wedge \exists x(x < z \wedge r(x))))$$

Give an LDL position formula σ which is equivalent to $\varphi(x)$.

[2] **d)** Show that every formula in $\mathrm{LTL}(\mathrm{AP}, \mathsf{SS}, \mathsf{SU})$ can be expressed in LDL, i.e., for all $\varphi \in \mathrm{LTL}(\mathrm{AP}, \mathsf{SS}, \mathsf{SU})$ we can construct an equivalent LDL position formula $\overline{\varphi}$.

[1] **e)** Consider the $\mathrm{MSO}(\mathrm{AP}, <)$ formula (where $\lessdot$ denotes the successor relation)

$$\varphi(x) = \exists X(x \in X \wedge \forall y \forall z(y \lessdot z \implies (y \in X \iff z \notin X)) \wedge \exists y(y \in X \wedge p(y)))$$

Give an LDL position formula σ which is equivalent to $\varphi(x)$.

[2] **f)** Give an LDL position formula σ such that for all $w \in \Sigma^\omega$ we have $w, 0 \models \sigma$ iff for all pairs $i < j$ of positions satisfying p ($w, i \models p$ and $w, j \models p$) we have $j - i$ even or $w, k \models p \vee q$ for some $i < k < j$.

Now, given an LDL position formula σ, the goal is to construct an unambiguous sequential Büchi transducer $\mathcal{A}_\sigma$ such that $[\![\mathcal{A}_\sigma]\!] = [\![\sigma]\!]$. Recall that for a position formula, we have $[\![\sigma]\!] \colon \Sigma^\omega \to \{0,1\}^\omega$ defined for all $w \in \Sigma^\omega$ by $[\![\mathcal{A}_\sigma]\!](w) = b_0 b_1 b_2 \cdots$ with

$$\forall i \in \mathbb{N}, \qquad b_i = \begin{cases} 1 & \text{if } w, i \models \sigma \\ 0 & \text{otherwise} \end{cases}$$

We assume below that $\mathrm{AP} = \{p, q, r\}$ and we let $\pi = (\mathsf{test}(p){\to}{\to} + \mathsf{test}(q){\to})^*\mathsf{test}(r)$. We will construct $\mathcal{A}_\sigma$ where $\sigma = \langle \pi \rangle$. We define the LDL position formulæ

$$\begin{aligned}
\sigma_1 &= r \wedge \langle {\to}\pi \rangle & \qquad \sigma_2 &= r \wedge \neg\langle {\to}\pi \rangle \\
\sigma_3 &= \neg r \wedge \langle \pi \rangle \wedge \langle {\to}\pi \rangle & \qquad \sigma_4 &= \neg r \wedge \langle \pi \rangle \wedge \neg\langle {\to}\pi \rangle \\
\sigma_5 &= \neg\langle \pi \rangle \wedge \langle {\to}\pi \rangle & \qquad \sigma_6 &= \neg\langle \pi \rangle \wedge \neg\langle {\to}\pi \rangle\,.
\end{aligned}$$

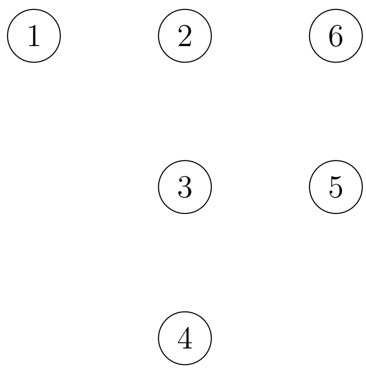
[2] **g)** Show that the formulæ $(\sigma_i)_{1 \le i \le 6}$ form a partition, i.e., the formula $\bigvee_{i=1}^{6} \sigma_i$ is valid and for all $1 \le k < \ell \le 6$ the formula $\sigma_k \wedge \sigma_\ell$ is not satisfiable.

[8] **h)** Construct a prophetic Büchi automaton $\mathcal{A}$ with 6 states $Q = \{1,2,3,4,5,6\}$ 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 a final run of $\mathcal{A}$ on the input word w then

$$\forall i \in \mathbb{N},\ \forall \ell \in Q, \qquad s_i = \ell \iff w, i \models \sigma_\ell\,.$$

Prove that your automaton is correct.

You will imperatively draw the automaton with the states placed as on the right (with a larger scale). Transitions should be labeled with boolean combinations of atomic propositions, e.g., p or $\neg p \wedge q$ or $(p \vee q) \wedge \neg r$, etc. The final states for the single Büchi condition should be indicated with double circles.



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