Principles of Model Checking
Solutions to exercise class 2

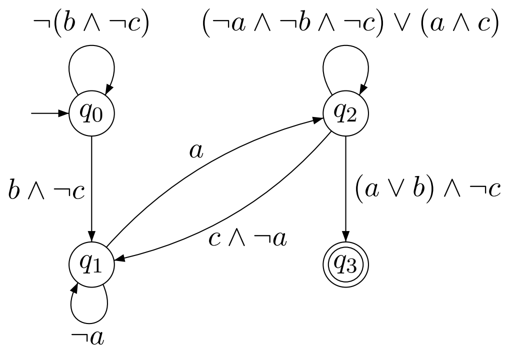
Verification of regular linear time properties

Prof. Dr. Joost-Pieter Katoen, Dr. Taolue Chen, and Ir. Mark Timmer

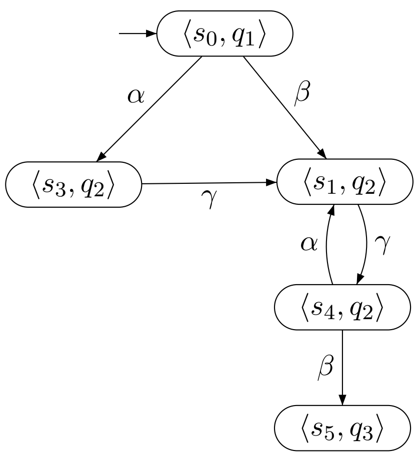
September, 21, 2012

Problem 1

1. An NFA that accepts the set of minimal bad prefixes:



2. First we apply the $TS \otimes \mathcal{A}$ construction, which yields:



A counterexample to $TS \models P_{safe}$ is given by the following initial path fragment in $TS \otimes \mathcal{A}$:

$$\pi_{\otimes} = \langle s_0, q_1 \rangle \langle s_3, q_2 \rangle \langle s_1, q_2 \rangle \langle s_4, q_2 \rangle \langle s_5, q_3 \rangle$$

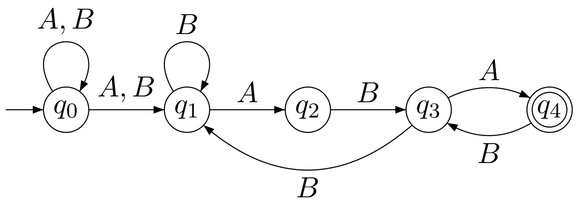
By projection on the state component, we get a path in the underlying transition system TS:

$$\pi = s_0 s_3 s_1 s_4 s_5 \text{ with } \mathit{trace}(\pi) = \{a, b\}\{a, c\}\{a, b, c\}\{a, c\}\{a, b\}$$

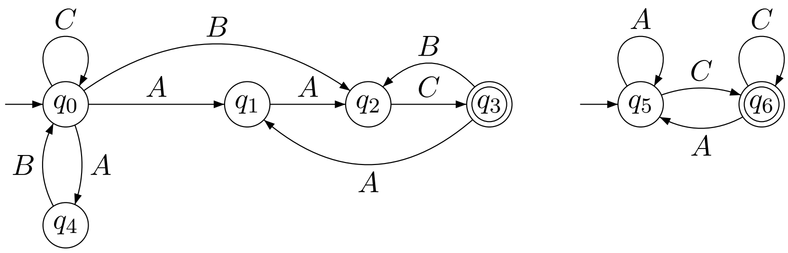
Since $\pi_{\otimes}$ reaches q_3 (a final state of $\mathcal{A}$), $\mathit{trace}(\pi) \in \mathit{BadPref}(P_{safe})$. Hence, $\mathit{Traces}_{fin}(TS) \cap \mathit{BadPref}(P_{safe}) \neq \varnothing$. By Lemma 3.25, this is equivalent to $TS \not\models P_{safe}$.

Problem 2

1. $L_1 = \{\sigma \in \{A, B\}^\omega \mid \sigma \text{ contains } ABA \text{ infinitely often, but } AA \text{ only finitely often}\}$



2. $L_2 = \mathcal{L}\left(((AB + C)^*((AA + B)C)^\omega + (A^*C)^\omega\right)$



Note: We allow more than one initial state! Formally, the automaton outlined above is given by

$$\mathcal{A}_2 = (\{q_0, \ldots, q_6\}, \{A, B, C\}, \delta, \{q_0, q_5\}, \{q_3, q_6\})$$

where δ is defined as shown in the picture.

Problem 3

Proof sketch: Use a product construction and distinguish three phases which have to be repeated in an infinite successful run infinitely often:

1. Wait for the first component to visit a final state;
2. Wait for the second component to a visit final state;
3. Signal that phase 1 and phase 2 have been completed.

Let $\mathcal{A}_i = (Q_i, \Sigma, \delta_i, Q_{0,i}, F_i)$ for $i = 1, 2$. Then, we define $\mathcal{A} = (Q, \Sigma, \delta, Q_0, F)$, where

- $Q = Q_1 \times Q_2 \times \{1, 2, 3\}$
- $\delta \colon Q \times \Sigma \to 2^Q$ such that

$$\begin{aligned}
\delta\left((q_1, q_2, 1), A\right) &= \Big((\delta_1(q_1, A) \setminus F_1) \times \delta_2(q_2, A) \times \{1\}\Big) \\
&\cup \Big((\delta_1(q_1, A) \cap F_1) \times \delta_2(q_2, A) \times \{2\}\Big) \\
\delta\left((q_1, q_2, 2), A\right) &= \Big(\delta_1(q_1, A) \times (\delta_2(q_2, A) \setminus F_2) \times \{2\}\Big) \\
&\cup \Big(\delta_1(q_1, A) \times (\delta_2(q_2, A) \cap F_2) \times \{3\}\Big) \\
\delta\left((q_1, q_2, 3), A\right) &= \delta_1(q_1, A) \times \delta_2(q_2, A) \times \{1\}
\end{aligned}$$

- $Q_0 = Q_{0,1} \times Q_{0,2} \times \{3\}$
- $F = Q_1 \times Q_2 \times \{3\}$

We have to prove that $\mathcal{L}_\omega(\mathcal{A}) = \mathcal{L}_\omega(\mathcal{A}_1) \cap \mathcal{L}_\omega(\mathcal{A}_2)$:

- Let $\sigma = A_1 A_2 A_3 \ldots \in \mathcal{L}_\omega(\mathcal{A})$. Then, there exists an accepting run of $\mathcal{A}$ of the form

$$(p_0, q_0, i_0) \xrightarrow{A_1} (p_1, q_1, i_1) \xrightarrow{A_2} \cdots$$

  such that $i_k = 3$ for infinitely many $k \geq 0$. But then, $p_i \in F_1$ and $q_j \in F_2$ for infinitely many i, j by construction. Hence, the runs $p_0 \xrightarrow{A_1} p_1 \xrightarrow{A_2} p_2 \ldots$ and $q_0 \xrightarrow{A_1} q_1 \xrightarrow{A_2} q_2 \ldots$ are accepting runs for σ in $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. Therefore $\sigma \in \mathcal{L}_\omega(\mathcal{A}_1) \cap \mathcal{L}_\omega(\mathcal{A}_2)$.

- Let $\sigma = A_1 A_2 A_3 \ldots \in \mathcal{L}_\omega(\mathcal{A}_1) \cap \mathcal{L}_\omega(\mathcal{A}_2)$. Then, there exist accepting runs $p_0 \xrightarrow{A_1} p_1 \xrightarrow{A_2} p_2 \ldots$ and $q_0 \xrightarrow{A_1} q_1 \xrightarrow{A_2} q_2 \ldots$ of σ in $\mathcal{A}_1$ and $\mathcal{A}_2$, such that $p_i \in F_1$ and $q_j \in F_2$ for infinitely many i, j. We obtain the induced run of $\mathcal{A}$ on σ as follows:

  $$(p_0, q_0, i_0) \xrightarrow{A_1} (p_1, q_1, i_1) \xrightarrow{A_2} (p_2, q_2, i_2) \cdots$$

  We need to prove that $i_k = 3$ for infinitely many $k \geq 0$.

  Therefore, let $i_k = 3$ for some $k \geq 0$ (this happens at least once, as it happens in every initial state). We prove that there exists a $k' > k$ such that $i_{k'} = 3$:

  As $p_n \in F_1$ infinitely often, there exists a fragment $p_k, p_{k+1}, \ldots, p_{k+l}$ such that $p_{k+l} \in F_1$, $l > 0$ and $p_j \notin F_1$ for $j = k{+}1, \ldots, k{+}l{-}1$. By construction, $i_{k+l} = 2$.

  Analogously, $q_n \in F_2$ for infinitely many n. Thus there exists a fragment $q_{k+l}, q_{k+l+1}, q_{k+l+2}, \ldots, q_{k+l+o}$ with $o > 0$ such that $q_j \notin F_2$ for $j = k{+}l{+}1, \ldots, k{+}l{+}o{-}1$ and $q_{k+l+o} \in F_2$. Then, by construction, $i_{k+l+o} = 3$. To conclude the proof, set $k' = k{+}l{+}o$.