Principles of Model Checking
Solutions to exercise class 1

Transition systems & linear-time properties

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

September, 14, 2012

Problem 1

1. Express the following informally-stated properties as LT-properties:

   - An account with positive balance is opened.

     $$P = \mathcal{L}_\omega((\varnothing + \{ab > 100\})\,(2^{AP})^\omega)$$

   - The balance of an account is negative only finitely many times.

     $$P = \mathcal{L}_\omega((2^{AP})^*\,(\{ab = 0\} + \varnothing + \{ab > 100\})^\omega)$$

   - The balance of an account switches at least once from debit to credit.

     $$P = \mathcal{L}_\omega((2^{AP})^*\,\{ab < 0\}\,(\{ab = 0\} + \varnothing + \{ab > 100\})\,(2^{AP})^\omega)$$

   - Eventually, an account remains with more than €100 credit.

     $$P = \mathcal{L}_\omega((2^{AP})^*\,\{ab > 100\}^\omega)$$

   - false and true.

     $$P_{\mathsf{false}} = \varnothing \quad \text{and} \quad P_{\mathsf{true}} = \mathcal{L}_\omega(\left(2^{AP}\right)^\omega)$$

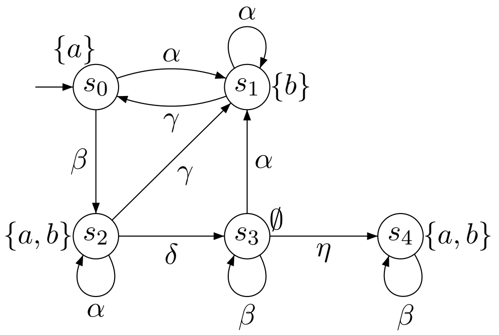
2. Determine for each LT-property whether it is a safety property or a liveness property. Justify your answer!

   - An account with positive balance is opened.
     - This is a safety property, since every trace that is not in P has a finite bad prefix: either $\{ab < 0\}$ or $\{ab = 0\}$.
   - The balance of an account is negative only finitely many times.
     - This is a liveness property, since any finite trace can be extended to satisfy P (for instance, by suffixing $\{ab > 100\}^\omega$).

- The balance of an account switches at least once from debit to credit.
  - This is a liveness property, since any finite trace can be extended to satisfy P (for instance, by suffixing the infinite trace $\{ab < 0\}\{ab > 100\}^\omega$).
- Eventually, an account remains with more than €100 credit.
  - This is a liveness property, since any finite trace can be extended with $\{ab > 100\}^\omega$ to satisfy P.
- false and true.
  - LT_{false} is a safety property. Every trace is erroneous, so all finite prefixes are bad prefixes.
  - LT_{true} is a safety and a liveness property. The fact that it is a safety property is trivially true since there are no bad traces. The fact that it is a liveness property is immediate from the fact that every finite trace can be extended with any infinite trace to satisfy LT_{true}.

Problem 2

We consider the following transition system TS:



Let P be the set of traces of the form $\sigma = A_0A_1A_2\ldots \in \left(2^{AP}\right)^\omega$ such that

$$\overset{\infty}{\exists}\ k.\ A_k = \{a,b\} \quad \wedge \quad \exists n \geq 0.\ \forall k > n.\ \big(a \in A_k \Rightarrow b \in A_{k+1}\big).$$

For the following fairness assumptions $\mathcal{F}_i$ with respect to the transition system TS, we decide whether or not $TS \models_{\mathcal{F}_i} P$.

First of all, notice that $TS \models_{\mathcal{F}_i} P$ if and only if $\mathit{FairTraces}_{\mathcal{F}_i}(TS) \subseteq P$. Because of $\overset{\infty}{\exists}\ k.\ A_k = \{a,b\}$, each trace has to visit at least one of s_2 or s_4 infinitely many times. Additionally, from some point onwards, each a-state must be followed by a state that is annotated with (at least) b.

1. $\mathcal{F}_1 = \Big(\{\{\alpha\}\}, \{\{\beta\}, \{\delta, \gamma\}, \{\eta\}\}, \emptyset \Big)$.

   - It holds that $TS \models_{\mathcal{F}_1} P$. To see why, notice that:
     - Any trace that reaches s_4 is not $\mathcal{F}_1$-fair. After all, for such traces α is executed only finitely many times. This is in contradiction with the unconditional fairness assumption $\{\alpha\}$. Hence, the transition $s_3 \xrightarrow{\eta} s_4$ is never taken.
     - Because of the strong fairness assumption $\{\eta\}$, the η action must be executed infinitely often if it is enabled infinitely often. Since it clearly cannot be executed infinitely often, it is not allowed to be enabled infinitely often. Hence, the state s_3 (in which it is enabled) cannot be visited infinitely often. From now on we only consider what happens after s_3 was visited for the last time.
     - We cannot stay forever in states s_1 or s_2 by only taking their α-transitions, because of the enabled γ transitions to s_0 and s_1, respectively. Due to the strong fairness assumption $\{\delta, \gamma\}$, these γ-transitions must be taken at some point. Hence, every time s_2 is visited, at some point we move to s_1, and every time s_1 is visited, at some point we move to s_0.
     - As β is enabled in s_0, the strong fairness assumption $\{\beta\}$ requires that if s_0 is visited infinitely often, then so is s_2.
     - Hence, all $\mathcal{F}_1$–fair paths visit exactly s_0, s_1 and s_2 infinitely often. It is easy to see that the traces of such paths satisfy the property P. Therefore $\mathit{FairTraces}_{\mathcal{F}_1}(TS) \subseteq P$ and thus $TS \models_{\mathcal{F}_1} P$.

2. $\mathcal{F}_2 = \Big(\{\{\alpha\}\}, \{\{\beta\}, \{\gamma\}\}, \{\{\eta\}\} \Big)$.

   - We find $TS \not\models_{\mathcal{F}_2} P$. To see why, consider the path $\pi = (s_0 s_2 s_3 s_1)^\omega$ with its corresponding trace $\sigma = (\{a\}\{a,b\}\varnothing\{b\})^\omega$. All fairness assumptions are fulfilled: α is executed infinitely often, and so are β and γ. The action η is never continuously enabled, so the weak fairness assumption $\{\eta\}$ does not forbid the path.

     Hence, $\pi \in \mathit{FairPaths}_{\mathcal{F}_2}(TS)$, but $\sigma \notin P$. Therefore, we find $\mathit{FairTraces}_{\mathcal{F}_2}(TS) \not\subseteq P$ and correspondingly $TS \not\models_{\mathcal{F}_2} P$.

Problem 3

Let P and P' be liveness properties over AP. Then

- $P \cup P'$ is guaranteed to be a liveness property too.

  Since P is a liveness property, by definition $\mathit{pref}(P) = \left(2^{AP}\right)^*$. Since $\mathit{pref}(Q) \subseteq \left(2^{AP}\right)^*$ for every LT-property Q, and clearly $\mathit{pref}(P_1 \cup P_2) \supseteq \mathit{pref}(P_1)$ for all LT-properties P_1, P_2, we find $\mathit{pref}(P \cup P') \subseteq \left(2^{AP}\right)^*$ as well as $\mathit{pref}(P \cup P') \supseteq \left(2^{AP}\right)^*$. Therefore, $\mathit{pref}(P \cup P') = \left(2^{AP}\right)^*$ and $P \cup P'$ is a liveness property.

  Note that we did not need the fact the P' is a liveness property.

- $P \cap P'$ is not guaranteed to be a liveness property too.

  Let

  $$P = \mathcal{L}_\omega\left(\left(2^{AP}\right)^* \{a\}^\omega\right) \qquad \text{and} \qquad P' = \mathcal{L}_\omega\left(\left(2^{AP}\right)^* \{b\}^\omega\right)$$

  Clearly, both are liveness properties, since any finite trace can be extended to a valid trace. However, $P \cap P' = \varnothing$, which is not a liveness property as $\mathit{pref}(\varnothing) = \varnothing \neq \left(2^{AP}\right)^*$.

Let P and P' be safety properties over AP. Then

- $P \cup P'$ is guaranteed to be a safety property too.

  Since $\mathit{closure}(P \cup P') = \mathit{closure}(P) \cup \mathit{closure}(P')$ by Lemma 3.36, using Lemma 3.27 we find that $\mathit{closure}(P \cup P') = P \cup P'$. Hence, applying Lemma 3.27 again, we find that $P \cup P'$ is a safety property too.

- $P \cap P'$ is guaranteed to be a safety property too.

  Let $\sigma \in \left(2^{AP}\right)^\omega \setminus (P \cap P')$. Hence, either $\sigma \notin P$ or $\sigma \notin P'$. We assume without loss of generality that $\sigma \notin P$. Since P is a safety property, there exists a finite prefix $\hat{\sigma} \in \mathit{pref}(\sigma)$ such that

  $$P \cap \left\{\sigma' \in \left(2^{AP}\right)^\omega \mid \hat{\sigma} \in \mathit{pref}(\sigma')\right\} = \varnothing.$$

  Since $P \cap P' \subseteq P$, we infer

  $$(P \cap P') \cap \left\{\sigma' \in \left(2^{AP}\right)^\omega \mid \hat{\sigma} \in \mathit{pref}(\sigma')\right\} = \varnothing.$$

  Thus $P \cap P'$ is a safety property too.