Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen
Christian Hensel, Matthias Volk

Introduction to Model Checking (Summer Term 2018)

— Exercise Sheet 4 (due 28th May) —

General Remarks

- The exercises are to be solved in groups of *three* students.
- You may hand in your solutions for the exercises just before the exercise class starts at 12:15 or by dropping them into the "Introduction to Model Checking" box at our chair *before 12:00*. Do *not* hand in your solutions via L2P or via e-mail.

Exercise 1 (6 Points)

Let $\mathrm{AP} = \{a, b\}$ and let

$$E = \left\{\sigma = A_0A_1A_2 \cdots \in \left(2^{AP}\right)^\omega \mid (\exists n \geq 0\,.\,\forall 0 \leq i < n\,.\,a \in A_i \wedge A_n = \{a,b\}) \wedge (\forall j \geq 0\,.\,\exists i \geq j\,.\,b \in A_i)\right\}$$

be an LT property. Provide a decomposition $E = S \cap L$ into a safety property S and a liveness property L. For this, give ω-regular expressions s and l over the alphabet 2^{AP} such that $S = \mathcal{L}_\omega(s)$ and $L = \mathcal{L}_\omega(l)$.

Hint: For a regular expression δ over the alphabet Σ, we let $\mathcal{L}(\delta) \subseteq \Sigma^*$ denote the language of finite words induced δ. An ω-regular expression γ over the alphabet Σ is of the form

$$\gamma = \alpha_1.\beta_1^\omega + \ldots + \alpha_n.\beta_n^\omega$$

where $n \geq 1$, α_i, β_i are regular expressions over Σ such that $\epsilon \notin \mathcal{L}(\beta_i)$ for all $1 \leq i \leq n$. The semantics of an ω-regular expression γ is a language of infinite words defined by

$$\mathcal{L}_\omega(\gamma) = \mathcal{L}(\alpha_1)\mathcal{L}(\beta_1)^\omega \cup \ldots \cup \mathcal{L}(\alpha_n)\mathcal{L}(\beta_n)^\omega$$

where

- for $L \subseteq \Sigma^*$ it is $L^\omega = \{\sigma_1\sigma_2\sigma_3 \ldots \mid \forall i \geq 1\,.\,\sigma_i \in L\}$, and
- for $L_1 \subseteq \Sigma^*, L_2 \subseteq \Sigma^\omega$ it is $L_1L_2 = \{\sigma_1\sigma_2 \mid \sigma_1 \in \mathcal{L}_1 \wedge \sigma_2 \in L_2\} \subseteq \Sigma^\omega$.

Exercise 2★ (1 + 2 + 2 + 3 Points)

Let $\mathrm{TS}_i = (S_i, \mathrm{Act}, \rightarrow_i, S_0^i, \mathrm{AP}_i, L_i)$ be transition systems for $i \in \{1, 2\}$. Note that TS_1 and TS_2 have the same action set.

Prove or disprove the following statements under the assumption $\mathrm{AP}_2 = \emptyset$.

(a) $\mathit{Traces}(\mathrm{TS}_1) \subseteq \mathit{Traces}(\mathrm{TS}_1 \parallel \mathrm{TS}_2)$,

(b) $\mathit{Traces}(\mathrm{TS}_1 \parallel \mathrm{TS}_2) \subseteq \mathit{Traces}(\mathrm{TS}_1)$.

Furthermore, let $\mathcal{F} = (\emptyset, \mathcal{F}_s, \mathcal{F}_w)$ be a fairness assumption.

Prove or disprove the following statements (for arbitrary AP_2).

(c) $Traces(\mathrm{TS}_1) \subseteq Traces(\mathrm{TS}_2) \implies FairTraces_{\mathcal{F}}(\mathrm{TS}_1) \subseteq FairTraces_{\mathcal{F}}(\mathrm{TS}_2)$, and

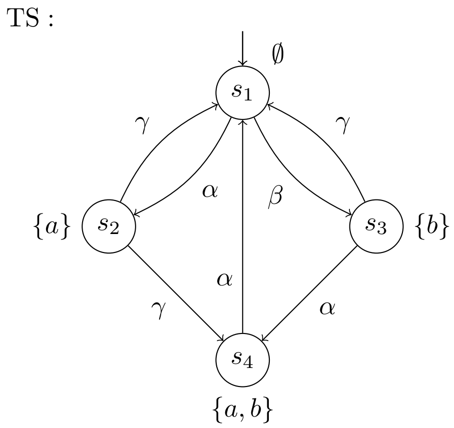
(d) if E is a liveness property and $\mathrm{TS}_2 \models_{\mathcal{F}} E$, then

$$Traces(\mathrm{TS}_1) \subseteq Traces(\mathrm{TS}_2) \implies \mathrm{TS}_1 \models_{\mathcal{F}} E.$$

Exercise 3* (1+3+3 Points)

Consider the transition system TS given below. Let $B_1 = \{\alpha\}$, $B_2 = \{\alpha, \beta\}$ and $B_3 = \{\beta\}$ be sets of actions. Further, let E_a, E_b and E' be the following LT properties:

- E_a = the set of all words $A_0 A_1 A_2 \cdots \in (2^{\{a,b\}})^\omega$ with $A_i \in \{\{a,b\}, \{a\}\}$ for infinitely many i (i.e., infinitely often a).
- E_b = the set of all words $A_0 A_1 A_2 \cdots \in (2^{\{a,b\}})^\omega$ with $A_i \in \{\{a,b\}, \{b\}\}$ for infinitely many i (i.e., infinitely often b).
- E' = the set of all words $A_0 A_1 A_2 \cdots \in (2^{\{a,b\}})^\omega$ for which there does *not* exist an $i \in \mathbb{N}$ s.t. $A_i = \{a\}$, $A_{i+1} = \{a, b\}$ and $A_{i+2} = \emptyset$.



(a) For which LT properties $E \in \{E_a, E_b, E'\}$ does it hold that $\mathrm{TS} \models E$?

(b) For which sets of actions B_i ($i \in \{1, 2, 3\}$) and LT properties $E \in \{E_a, E_b, E'\}$ does it hold that $\mathrm{TS} \models_{\mathcal{F}^i_{strong}} E$? Here, $\mathcal{F}^i_{strong}$ is a strong fairness condition with respect to B_i that does not impose any unconditional or weak fairness conditions (i.e., $\mathcal{F}^i_{strong} = (\emptyset, \{B_i\}, \emptyset)$).

(c) Answer the questions in (b) for weak fairness instead of strong fairness (i.e., $\mathcal{F}^i_{weak} = (\emptyset, \emptyset, \{B_i\})$).

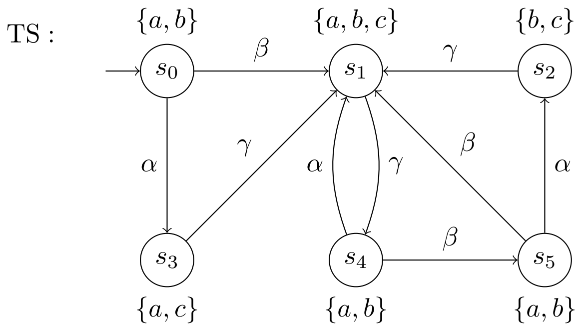
Exercise 4 (2+3 Points)

Consider the transition system TS depicted below and the regular safety property

$$P_{safe} = \begin{array}{c}\text{“always if } a \text{ is valid and } b \wedge \neg c \text{ was valid somewhere before,}\\ \text{then neither } a \text{ nor } b \text{ holds thereafter at least until } c \text{ holds”}\end{array}$$

As an example, it holds:

$$\begin{aligned}
\{b\}\, \emptyset\, \{a,b\}\, \{a,b,c\} &\in pref(P_{safe})\\
\{a,b\}\, \{a,b\}\, \emptyset\, \{b,c\} &\in pref(P_{safe})\\
\{b\}\, \{a,c\}\, \{a\}\, \{a,b,c\} &\in BadPref(P_{safe})\\
\{b\}\, \{a,c\}\, \{a,c\}\, \{a\} &\in BadPref(P_{safe})
\end{aligned}$$



(a) Define an NFA $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) = \mathit{MinBadPref}(P_{safe})$.

(b) Decide whether $\mathrm{TS} \models P_{safe}$ using the $\mathrm{TS} \otimes \mathcal{A}$ construction.
Provide a counterexample if $\mathrm{TS} \not\models P_{safe}$.