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

Introduction to Model Checking (Summer Term 2018)

— Solution 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 $\text{AP} = \{a, b\}$ and let

$$E = \left\{ \sigma = A_0 A_1 A_2 \cdots \in \left(2^{AP}\right)^\omega \mid (\exists n \geq 0 \,.\, \forall 0 \leq i < n \,.\, a \in A_i \wedge A_n = \{a, b\}) \wedge (\forall j \geq 0 \,.\, \exists i \geq j \,.\, b \in A_i) \right\}$$

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 $L_1 L_2 = \{\sigma_1\sigma_2 \mid \sigma_1 \in \mathcal{L}_1 \wedge \sigma_2 \in L_2\} \subseteq \Sigma^\omega$.

Solution:

According to the decomposition theorem from the lecture, every linear time property can be decomposed into a safety and a liveness property in the following way:

$$E = \underbrace{cl(E)}_{S} \cap \underbrace{\left(E \cup \left(\left(2^{AP}\right)^\omega \setminus cl(E)\right)\right)}_{L}$$

The linear time property E can be characterized by the following ω-regular expression:

$$E = \mathcal{L}_\omega\left(\{a\}^*\{a, b\}.\left(\left(2^{AP}\right)^*(\{b\} + \{a, b\})\right)^\omega\right)$$

In our case, this yields the following safety property:

$$\begin{aligned} S &= cl(E) \\ &= \left\{\sigma' \in \left(2^{AP}\right)^\omega \mid \mathit{pref}(\sigma') \subseteq \mathit{pref}(E)\right\} \\ &= \left\{\sigma' \in \left(2^{AP}\right)^\omega \mid \mathit{pref}(\sigma') \subseteq \mathcal{L}\left(\{a\}^*\{a,b\}\left(2^{AP}\right)^* + \{a\}^+\right)\right\} \\ &= \mathcal{L}_\omega\left(\underbrace{\{a\}^*\{a,b\}.\left(2^{AP}\right)^\omega + \{a\}^\omega}_{s}\right) \end{aligned}$$

The liveness property $L = E \cup \left(\left(2^{AP}\right)^\omega \setminus cl(E)\right)$ can be deduced as

$$\begin{aligned} L &= E \cup \left(\left(2^{AP}\right)^\omega \setminus cl(E)\right) \\ &= E \cup \left(\left(2^{AP}\right)^\omega \setminus \mathcal{L}_\omega\left(\{a\}^*\{a,b\}.\left(2^{AP}\right)^\omega + \{a\}^\omega\right)\right) \\ &= E \cup \mathcal{L}_\omega\left(\{a\}^*\left(\emptyset + \{b\}\right)\left(2^{AP}\right)^\omega\right) \\ &= \mathcal{L}_\omega\left(\underbrace{\{a\}^*\{a,b\}.\left(\left(2^{AP}\right)^*\left(\{b\} + \{a,b\}\right)\right)^\omega + \{a\}^*\left(\emptyset + \{b\}\right).\left(2^{AP}\right)^\omega}_{l}\right). \end{aligned}$$

Exercise 2★ (1 + 2 + 2 + 3 Points)

Let $\mathrm{TS}_i = (S_i, \mathrm{Act}, \to_i, S_0^i, \mathrm{AP}_i, L_i)$ 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).

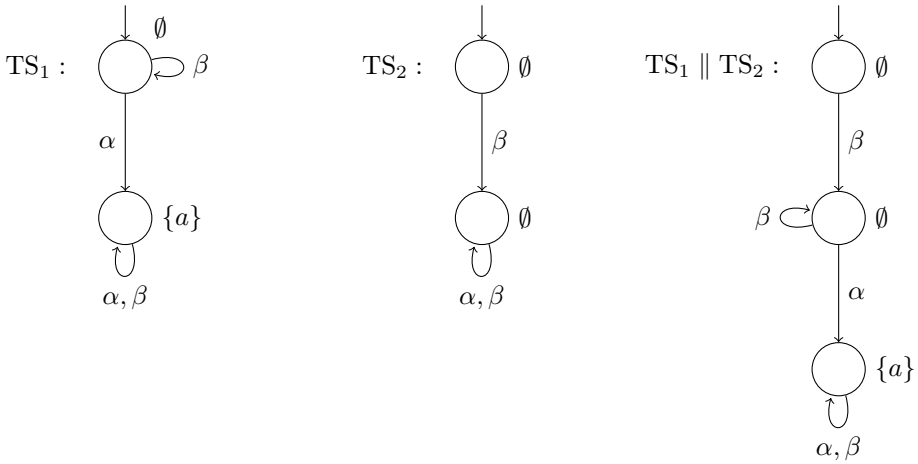
(c) $\mathit{Traces}(\mathrm{TS}_1) \subseteq \mathit{Traces}(\mathrm{TS}_2) \implies \mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_1) \subseteq \mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_2)$, and

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

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

Solution:

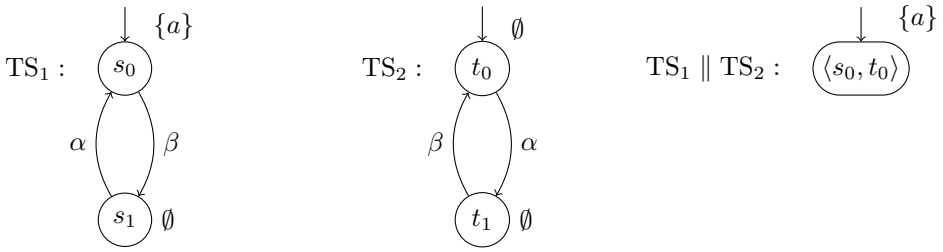
(a) The statement does not hold. Consider the two transition systems TS_1 and TS_2 with $\mathrm{Act} = \{\alpha, \beta\}$ and their composition $\mathrm{TS}_1 \parallel \mathrm{TS}_2$ as below.



We have $\sigma = \emptyset\,\{a\}^\omega \in \mathit{Traces}(\mathrm{TS}_1)$, but $\sigma \notin \mathit{Traces}(\mathrm{TS}_1 \parallel \mathrm{TS}_2)$, so the statement does not hold.

(b) The statement holds *under the assumption that there are no terminal states in* $TS_1 \parallel TS_2$. We first show that in general the statement is violated.

Consider the two transition systems TS_1 and TS_2 as below:



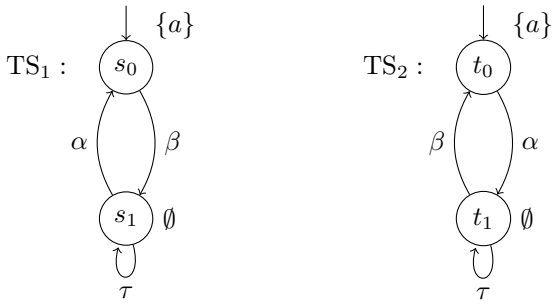
Clearly, $\{a\} \in \mathit{Traces}(\mathrm{TS}_1 \parallel \mathrm{TS}_2)$ as $\langle s_0, t_0\rangle$ is a terminal state. However, $\mathit{Traces}(\mathrm{TS}_1) = \{\{a\}^\omega\} \subseteq \left(2^{\mathrm{AP}}\right)^\omega$ and, in particular, $\{a\} \notin \mathit{Traces}(\mathrm{TS}_1)$.

We now move to the case where $\mathrm{TS}_1 \parallel \mathrm{TS}_2$ does *not* possess terminal states. According to the definition of the parallel composition operator $\parallel$, the composite transition system is given as $\mathrm{TS}_1 \parallel \mathrm{TS}_2 = (S = S_1 \times S_2, \mathrm{Act}, \to, S_0^1 \times S_0^2, \mathrm{AP}_1, L')$ with $L((s_1, s_2)) = L_1(s_1)$. As TS_1 and TS_2 have the same set of actions, $\to$ is the smallest relation satisfying the SOS rules

$$\frac{s_1 \xrightarrow{\alpha}_1 s_1' \quad \wedge \quad s_2 \xrightarrow{\alpha}_2 s_2'}{(s_1, s_2) \xrightarrow{\alpha} (s_1', s_2')} \qquad \text{for all } \alpha \in \mathrm{Act}.$$

Let $\sigma \in \mathit{Traces}(\mathrm{TS}_1 \parallel \mathrm{TS}_2)$. As $\mathrm{TS}_1 \parallel \mathrm{TS}_2$ does not have terminal states, $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega$ is an *infinite* word. Then, there exists an infinite path $\pi = (s_1^0, s_2^0)(s_1^1, s_2^1)\ldots \in \mathit{Paths}(\mathrm{TS}_1 \parallel \mathrm{TS}_2)$ such that $\mathit{trace}(\pi) = L'((s_1^0, s_2^0))L'((s_1^1, s_2^1))\ldots = L(s_1^0)L(s_1^1)\ldots = \sigma$. Since π is a path in $\mathrm{TS}_1 \parallel \mathrm{TS}_2$, it is $(s_1^i, s_2^i) \xrightarrow{\alpha_i} (s_1^{i+1}, s_2^{i+1})$ for all $i \geq 0$. Because of the rules defining $\to$ (above), we have $s_1^i \xrightarrow{\alpha_i}_1 s_1^{i+1}$ for all $i \geq 0$. Consequently, $\pi' = s_1^0 s_1^1 \ldots \in \mathit{Paths}(\mathrm{TS}_1)$ and $\mathit{trace}(\pi') = L(s_1^0)L(s_1^1)\ldots = \sigma$ and therefore $\sigma \in \mathit{Traces}(\mathrm{TS}_1)$.

(c) The statement does not hold. Consider the two transition systems TS_1 and TS_2 over the actions $\mathrm{Act}_1 = \mathrm{Act}_2 = \{\alpha, \beta, \tau\}$ and atomic propositions $\mathrm{AP}_1 = \mathrm{AP}_2 = \{a\}$ as below.



We have $\mathit{Traces}(\mathrm{TS}_1) = \mathit{Traces}(\mathrm{TS}_2)$ and, in particular, $\mathit{Traces}(\mathrm{TS}_1) \subseteq \mathit{Traces}(\mathrm{TS}_2)$ as the traces abstract from actions along transitions. Let $\mathcal{F} = (\emptyset, \emptyset, \{\beta\})$ be the fairness assumption that requires executions that have β continuously enabled from some point on to take β infinitely often. Then $\sigma_{\mathcal{F}} = \{a\}\,\emptyset^\omega \in \mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_1)$ because $\rho = s_0 \xrightarrow{\beta}_3 s_1 \xrightarrow{\tau}_3 s_1 \ldots$ is an $\mathcal{F}$-fair execution in TS_1. The only execution in TS_2 with trace $\sigma_{\mathcal{F}}$ is $\rho' = t_0 \xrightarrow{\alpha}_4 t_1 \xrightarrow{\tau}_4 t_1 \ldots$, which is not $\mathcal{F}$-fair. Therefore $\sigma_{\mathcal{F}} \notin \mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_2)$ and $\mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_1) \not\subseteq \mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_2)$.

(d) The statement does not hold. Reconsider TS_1, TS_2 (with $\mathit{Traces}(\mathrm{TS}_1) \subseteq \mathit{Traces}(\mathrm{TS}_2)$) and the fairness assumption $\mathcal{F}$ from (c). We consider the LT property $E = \{A_0 A_1 \ldots \mid \forall j \geq 0\,.\,\exists i \geq j\,.\,a \in A_i\}$. It is clear that E is a liveness property: take any finite word $\hat{\sigma} \in (2^{\mathrm{AP}})^+$ and extend it to $\hat{\sigma}\,\{a\}^\omega \in E$. It is

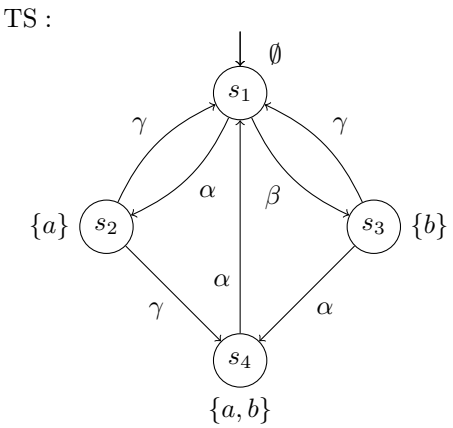
$$\mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_2) = \mathcal{L}_\omega\big((\{a\}^+\,\emptyset^+)^\omega\big) \subseteq E$$

and therefore $\mathrm{TS}_2 \models_{\mathcal{F}} E$. However, ρ (from (c)) is an $\mathcal{F}$-fair execution in TS_1 and has trace $\sigma_{\mathcal{F}} \in \mathit{FairTraces}_{\mathcal{F}}(\mathrm{TS}_1)$ (from (c)). As $\sigma_{\mathcal{F}} \notin E$, we have $\mathrm{TS}_1 \not\models_{\mathcal{F}} E$.

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 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., $\mathcal{F}^i_{weak} = (\emptyset, \emptyset, \{B_i\})$).

Solution:

(a)
- TS $\not\models E_a$. The trace $(\emptyset\,\{b\})^\omega$ is not in E_a.
- TS $\not\models E_b$. The trace $(\emptyset\,\{a\})^\omega$ is not in E_b.
- TS $\not\models E'$. The trace $(\emptyset\,\{a\}\,\{a,b\})^\omega$ is not in E'.

(b) Note that for all possible paths state s_1 is visited infinitely often and thus, actions α and β are enabled infinitely many times on all paths.

- TS $\models_{\mathcal{F}^1_{strong}} E_a$. All paths have to take action α in s_1 infinitely many times. Thus, state s_2 with label $\{a\}$ is visited infinitely often.
- TS $\not\models_{\mathcal{F}^1_{strong}} E_b$. The path $\pi_1 = (s_1 s_2)^\omega$ is a fair path but $trace(\pi_1) \notin E_b$.
- TS $\not\models_{\mathcal{F}^1_{strong}} E'$. The path $\pi_2 = (s_1 s_2 s_4)^\omega$ is a fair path but $trace(\pi_2) \notin E'$.
- TS $\not\models_{\mathcal{F}^2_{strong}} E_a$. The path $\pi_3 = (s_1 s_3)^\omega$ is a fair path but $trace(\pi_3) \notin E_a$.
- TS $\not\models_{\mathcal{F}^2_{strong}} E_b$. The path $\pi_1 = (s_1 s_2)^\omega$ is a fair path but $trace(\pi_1) \notin E_b$.
- TS $\not\models_{\mathcal{F}^2_{strong}} E'$. The path $\pi_2 = (s_1 s_2 s_4)^\omega$ is a fair path but $trace(\pi_2) \notin E'$.
- TS $\not\models_{\mathcal{F}^3_{strong}} E_a$. The path $\pi_3 = (s_1 s_3)^\omega$ is a fair path but $trace(\pi_3) \notin E_a$.
- TS $\models_{\mathcal{F}^3_{strong}} E_b$. All paths have to take action β in s_1 infinitely many times. Thus, state s_3 with label $\{b\}$ is visited infinitely often.
- TS $\not\models_{\mathcal{F}^3_{strong}} E'$. The path $\pi_4 = (s_1 s_3 s_4)^\omega$ is a fair path but $trace(\pi_4) \notin E'$.

(c) Remember the following relationship between strong and weak fairness for transition system TS and LT property P:

$$\text{TS} \models_{\mathcal{F}_{weak}} P \implies \text{TS} \models_{\mathcal{F}_{strong}} P$$

Then it follows:

$$\text{TS} \not\models_{\mathcal{F}_{strong}} P \implies \text{TS} \not\models_{\mathcal{F}_{weak}} P$$

Thus, we can already deduce from the solution to (b):

- TS $\not\models_{\mathcal{F}^1_{weak}} E_b$.
- TS $\not\models_{\mathcal{F}^1_{weak}} E'$.
- TS $\not\models_{\mathcal{F}^2_{weak}} E_a$.
- TS $\not\models_{\mathcal{F}^2_{weak}} E_b$.
- TS $\not\models_{\mathcal{F}^2_{weak}} E'$.
- TS $\not\models_{\mathcal{F}^3_{weak}} E_a$.
- TS $\not\models_{\mathcal{F}^3_{weak}} E'$.

Note that for paths $\pi_3 = (s_1 s_3)^\omega$ and $\pi_4 = (s_1 s_3 s_4)^\omega$ action α is continuously enabled.

- TS $\models_{\mathcal{F}^1_{weak}} E_a$. Paths visiting states s_2 or s_4 infinitely many times satisfy the property E_a. Therefore, the only paths violating the property have the form $\big((s_1 s_2) + (s_1 s_2 s_4) + (s_1 s_3) + (s_1 s_3 s_4)\big)^* (s_1 s_3)^\omega$. However, action α is continuously enabled in $(s_1 s_3)^\omega$ but never taken. Thus, these paths are not fair and are not considered.

- TS $\not\models_{\mathcal{F}^3_{weak}} E_b$. The path $\pi_1 = (s_1 s_2)^\omega$ is a fair path but $trace(\pi_1) \notin E_b$.

Note, for property E' it is also possible to show that E' is a safety property and fairness assumption $\mathcal{F}^i_k$ ($i \in \{1,2,3\}, k \in \{strong, weak\}$) is realizable for TS. Then we can use the fact TS $\not\models E'$ to conclude that TS $\not\models_{\mathcal{F}^i_k} E'$.

Exercise 4 (2+3 Points)

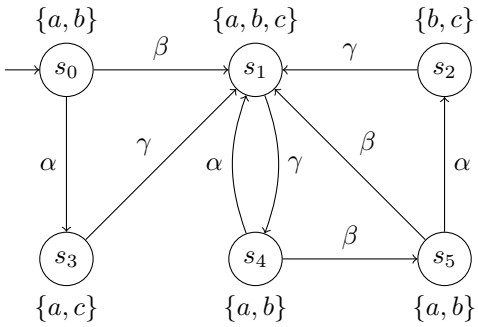
Consider the transition system TS depicted below and the regular safety property

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

As an example, it holds:

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

TS :



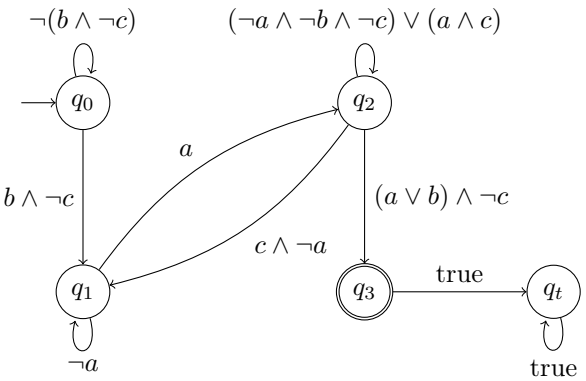
(a) Define an NFA $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) = MinBadPref(P_{safe})$.

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

Solution:

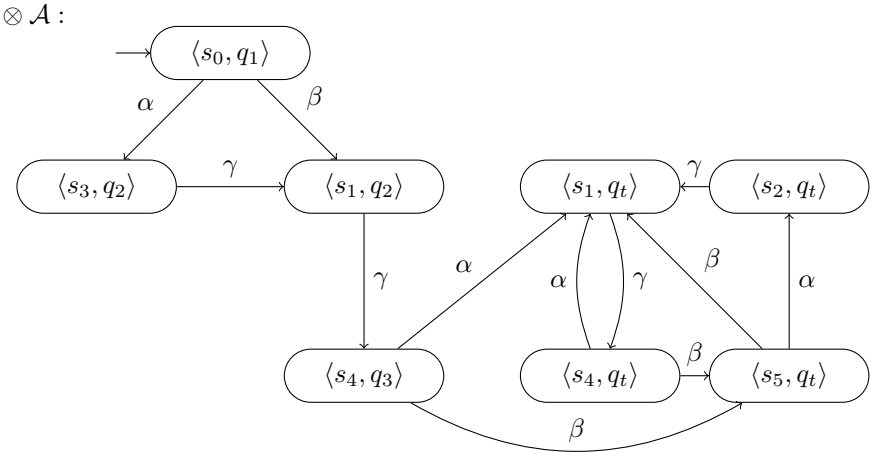
(a) The NFA $\mathcal{A}$ that accepts the set of minimal bad prefixes is depicted below.

$\mathcal{A}$:



(b) First we apply the $TS \otimes \mathcal{A}$ construction which yields:

TS $\otimes$ $\mathcal{A}$:



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

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

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

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

Obviously, $\mathit{trace}(\pi) \in \mathit{BadPref}(P_{safe})$, so we have $\mathit{Traces}_{fin}(\text{TS}) \cap \mathit{BadPref}(P_{safe}) \neq \emptyset$.
Therefore, TS $\not\models P_{safe}$.