

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

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

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

$$\gamma = \alpha_1 \cdot \beta_1^\omega + \dots + \alpha_n \cdot \beta_n^\omega$$

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

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

where

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

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:

$$E = \underbrace{cl(E)}_S \cap \underbrace{\left(E \cup \left((2^{AP})^\omega \setminus cl(E) \right) \right)}_L$$

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

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

In our case, this yields the following safety property:

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

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

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

Exercise 2★

(1 + 2 + 2 + 3 Points)

Let $TS_i = (S_i, \text{Act}, \rightarrow_i, S_0^i, AP_i, L_i)$ 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 $AP_2 = \emptyset$.

- (a) $\text{Traces}(TS_1) \subseteq \text{Traces}(TS_1 \parallel TS_2)$,
- (b) $\text{Traces}(TS_1 \parallel TS_2) \subseteq \text{Traces}(TS_1)$.

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

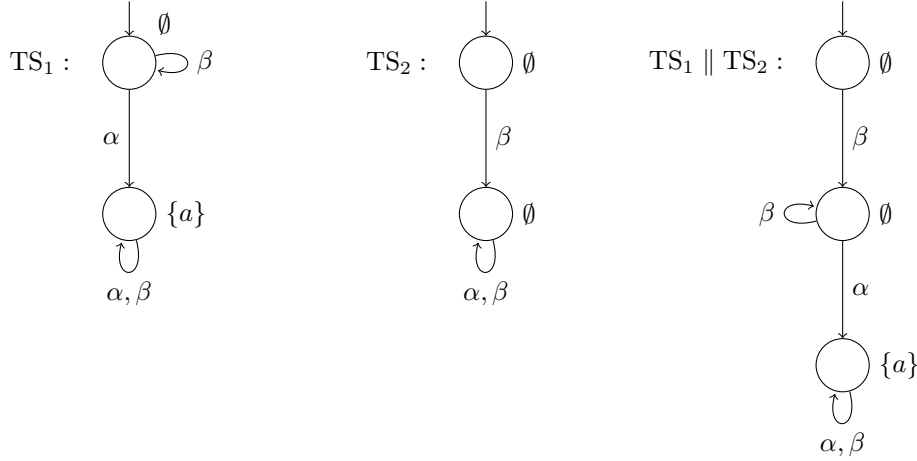
Prove or disprove the following statements (for arbitrary AP_2).

- (c) $\text{Traces}(TS_1) \subseteq \text{Traces}(TS_2) \implies \text{FairTraces}_{\mathcal{F}}(TS_1) \subseteq \text{FairTraces}_{\mathcal{F}}(TS_2)$, and
- (d) if E is a liveness property and $TS_2 \models_{\mathcal{F}} E$, then

$$\text{Traces}(TS_1) \subseteq \text{Traces}(TS_2) \implies TS_1 \models_{\mathcal{F}} E.$$

Solution: _____

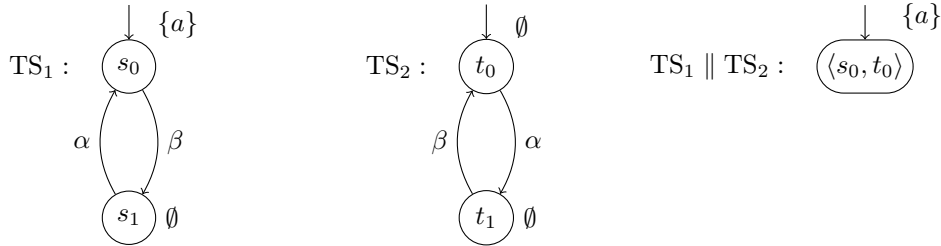
- (a) The statement does not hold. Consider the two transition systems TS_1 and TS_2 with $\text{Act} = \{\alpha, \beta\}$ and their composition $TS_1 \parallel TS_2$ as below.



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

- (b) The statement holds *under the assumption that there are no terminal states in $\text{TS}_1 \parallel \text{TS}_2$* . We first show that in general the statement is violated.

Consider the two transition systems TS_1 and TS_2 as below:



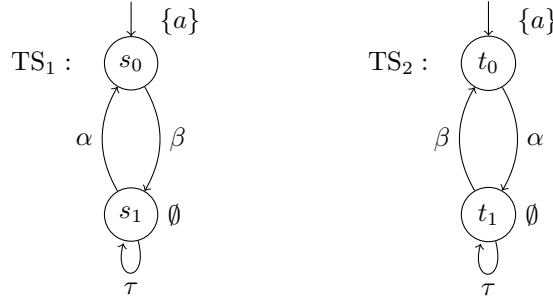
Clearly, $\{a\} \in \text{Traces}(\text{TS}_1 \parallel \text{TS}_2)$ as $\langle s_0, t_0 \rangle$ is a terminal state. However, $\text{Traces}(\text{TS}_1) = \{\{a\}^\omega\} \subseteq (2^{\text{AP}})^\omega$ and, in particular, $\{a\} \notin \text{Traces}(\text{TS}_1)$.

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

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

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

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



We have $Traces(TS_1) = Traces(TS_2)$ and, in particular, $Traces(TS_1) \subseteq Traces(TS_2)$ 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 $\sigma_{\mathcal{F}} = \{a\}\emptyset^\omega \in FairTraces_{\mathcal{F}}(TS_1)$ because $\rho = s_0 \xrightarrow{\beta}_3 s_1 \xrightarrow{\tau}_3 s_1 \dots$ is an $\mathcal{F}$ -fair execution in TS_1 . The only execution in TS_2 with trace $\sigma_{\mathcal{F}}$ is $\rho' = t_0 \xrightarrow{\alpha}_4 t_1 \xrightarrow{\tau}_4 t_1 \dots$, which is not $\mathcal{F}$ -fair. Therefore $\sigma_{\mathcal{F}} \notin FairTraces_{\mathcal{F}}(TS_2)$ and $FairTraces_{\mathcal{F}}(TS_1) \not\subseteq FairTraces_{\mathcal{F}}(TS_2)$.

- (d) The statement does not hold. Reconsider TS_1, TS_2 (with $Traces(TS_1) \subseteq Traces(TS_2)$) and the fairness assumption $\mathcal{F}$ from (c). We consider the LT property $E = \{A_0A_1\dots \mid \forall j \geq 0. \exists i \geq j. a \in A_i\}$. It is clear that E is a liveness property: take any finite word $\hat{\sigma} \in (2^{AP})^+$ and extend it to $\hat{\sigma}\{a\}^\omega \in E$. It is

$$FairTraces_{\mathcal{F}}(TS_2) = \mathcal{L}_\omega(\{a\}^+\emptyset^+)^\omega \subseteq E$$

and therefore $TS_2 \models_{\mathcal{F}} E$. However, ρ (from (c)) is an $\mathcal{F}$ -fair execution in TS_1 and has trace $\sigma_{\mathcal{F}} \in FairTraces_{\mathcal{F}}(TS_1)$ (from (c)). As $\sigma_{\mathcal{F}} \notin E$, we have $TS_1 \not\models_{\mathcal{F}} E$.

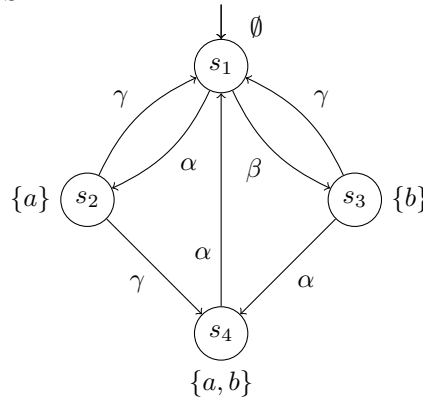
Exercise 3★

(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 $A_0A_1A_2\dots \in (2^{\{a,b\}})^\omega$ with $A_i \in \{\{a,b\}, \{a\}\}$ for infinitely many i (i.e., infinitely often a).
- E_b = the set of all words $A_0A_1A_2\dots \in (2^{\{a,b\}})^\omega$ with $A_i \in \{\{a,b\}, \{b\}\}$ for infinitely many i (i.e., infinitely often b).
- E' = the set of all words $A_0A_1A_2\dots \in (2^{\{a,b\}})^\omega$ for which there does *not* exist an $i \in \mathbb{N}$ s.t. $A_i = \{a\}$, $A_{i+1} = \{a,b\}$ and $A_{i+2} = \emptyset$.

TS :



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

- (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 $TS \models_{\mathcal{F}_{strong}^i} E$? Here, $\mathcal{F}_{strong}^i$ is a strong fairness condition with respect to B_i that does not impose any unconditional or weak fairness conditions (i.e., $\mathcal{F}_{strong}^i = (\emptyset, \{B_i\}, \emptyset)$).
- (c) Answer the questions in (b) for weak fairness instead of strong fairness (i.e., $\mathcal{F}_{weak}^i = (\emptyset, \emptyset, \{B_i\})$).

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

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

Then it follows:

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

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

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

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

- $TS \models_{\mathcal{F}_{weak}^1} E_a$. 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 $((s_1 s_2) + (s_1 s_2 s_4) + (s_1 s_3) + (s_1 s_3 s_4))^* (s_1 s_3)^\omega$. 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.

- $TS \not\models_{\mathcal{F}_{weak}^3} E_b$. 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 $\mathcal{F}_k^i$ ($i \in \{1, 2, 3\}, k \in \{strong, weak\}$) is realizable for TS. Then we can use the fact $TS \not\models E'$ to conclude that $TS \not\models_{\mathcal{F}_k^i} E'$.

Exercise 4

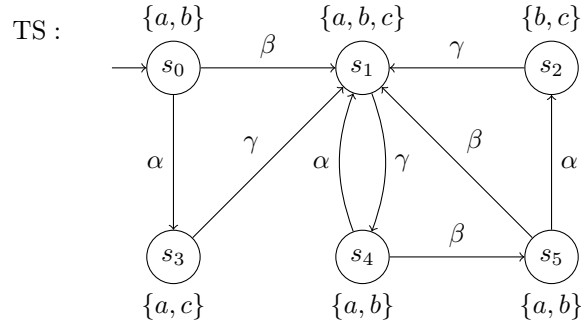
(2+3 Points)

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

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

As an example, it holds:

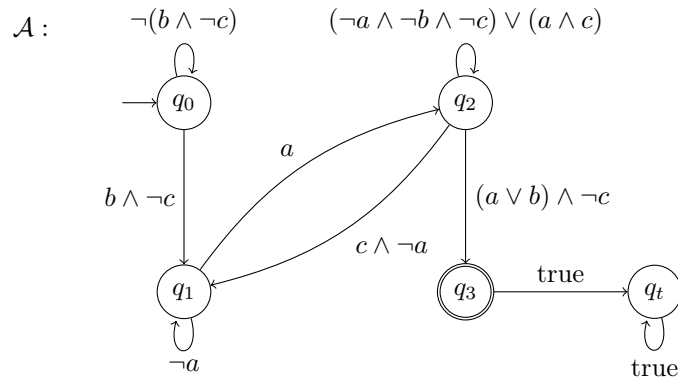
$\{b\} \emptyset \{a, b\} \{a, b, c\} \in \text{pref}(P_{safe})$
 $\{a, b\} \{a, b\} \emptyset \{b, c\} \in \text{pref}(P_{safe})$
 $\{b\} \{a, c\} \{a\} \{a, b, c\} \in \text{BadPref}(P_{safe})$
 $\{b\} \{a, c\} \{a, c\} \{a\} \in \text{BadPref}(P_{safe})$



- Define an NFA $\mathcal{A}$ such that $\mathcal{L}(\mathcal{A}) = \text{MinBadPref}(P_{safe})$.
- Decide whether $TS \models P_{safe}$ using the $TS \otimes \mathcal{A}$ construction.
Provide a counterexample if $TS \not\models P_{safe}$.

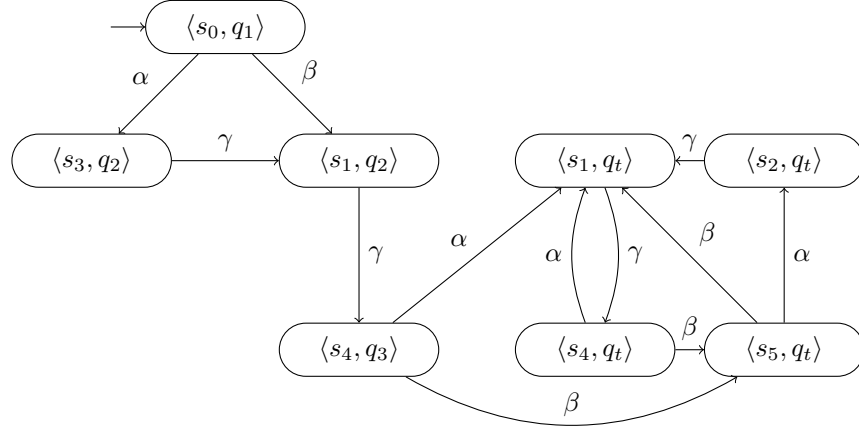
Solution: _____

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



- 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:

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

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