

Exercise 1 (Safety):

(3 points)

Consider the set AP of atomic propositions defined by $AP = \{x = 0, x > 1\}$ and consider a nonterminating sequential computer program P that manipulates the variable x .

- a) Formulate the following informally stated properties as LT properties:
 - a) initially x differs from zero
 - b) initially x is equal to zero, but at some point x exceeds one
 - c) x exceeds one only finitely many times
 - d) x exceeds one infinitely often
 - e) the value of x alternates between zero and one
- b) Determine which of the provided LT properties are safety properties? Which are liveness properties? Justify your answers by a formal argument.

Solution: _____

- a) (a) initially, x differs from zero: $(\emptyset + \{x > 1\})(2^{AP})^\omega$
 (b) initially, x is equal to zero, but at some point x exceeds one: $\{x = 0\}(2^{AP})^*\{x > 1\}(2^{AP})^\omega$.
 (c) x exceeds one only finitely often: $(2^{AP})^*(\{x = 0\} + \emptyset)^\omega$.
 (d) x exceeds one infinitely often: $((2^{AP})^*\{x > 1\})^\omega$.
 (e) the value of x alternates between zero and one: $(\{x = 0\}\emptyset)^\omega + (\emptyset\{x = 0\})^\omega$
- b) Let us check which of the above LT properties are safety properties.
 - (a) initially, x differs from zero: $P_1 = \mathcal{L}_\omega((\emptyset + \{x > 1\}) \cdot (2^{AP})^\omega)$. P_1 is a safety property with $\text{MinBadPref}(P_1) = \{\{x = 0\}\}$
 - (b) initially, x is equal to zero, but at some point, x exceeds one:

$$P_2 = \mathcal{L}_\omega(\{x = 0\} \cdot (2^{AP})^* \cdot \{x > 1\} \cdot (2^{AP})^\omega).$$

It follows that $\text{closure}(P_2) = \mathcal{L}_\omega(\{x = 0\} \cdot (2^{AP})^\omega)$. Therefore $\text{closure}(P_2) \neq P_2$ and P_2 is not a safety property.

- (c) x exceeds one only finitely many times: $P_3 = \mathcal{L}_\omega((2^{AP})^* \cdot (\{x = 0\} + \emptyset)^\omega)$. We have that $\text{closure}(P_3) = (2^{AP})^\omega$ and $\text{closure}(P_3) \neq P_3$. Therefore P_3 is not a safety property.
- (d) x should exceed one infinitely often. This is not a safety property.
- (e) the value of x alternates between zero and one: $P_4 = \mathcal{L}_\omega((\{x = 0\}.\emptyset)^\omega + (\emptyset.\{x = 0\})^\omega)$:
 P_4 is a safety property with:

$$\text{MinBadPref}(P_4) = \mathcal{L}((2^{AP})^* \cdot \{x > 1\} + (2^{AP})^* \cdot \emptyset.\emptyset + (2^{AP})^* \cdot \{x = 0\} \cdot \{x = 0\})$$

The first summand refers to the situation in which x exceeds 1, the second summand to the situation in which x equals 1 at successive positions, and finally the last summand does the same for x being zero.

The only safety-property that is also a liveness property is P_{true} . Thus, (a) and (e) are no liveness properties.

- (b) Consider a word $w = x > 0 \dots$; for every suffix w' , ww' is not in the language.
- (c, d) Can be rewritten into $(2^{AP})^*$ concatenated by the language.

Exercise 2 (Finite Trace Equivalence):

(2 points)

Recall the definition of AP-deterministic transition systems (cf. Series 1, Exercise 1). Let TS and TS' be transition systems with the same set of atomic propositions AP. Prove the following relationship between trace inclusion and finite trace inclusion:

- a) For AP-deterministic TS and TS':

$$\text{Traces}(\text{TS}) = \text{Traces}(\text{TS}') \text{ if and only if } \text{Traces}_{\text{fin}}(\text{TS}) = \text{Traces}_{\text{fin}}(\text{TS}').$$

- b) Give concrete examples of TS and TS' where at least one of the transition systems is not AP-deterministic, and

$$\text{Traces}(\text{TS}) \not\subseteq \text{Traces}(\text{TS}') \text{ and } \text{Traces}_{\text{fin}}(\text{TS}) = \text{Traces}_{\text{fin}}(\text{TS}').$$

Solution: _____

- a) First we show the easier direction " $\Rightarrow$ ". Assume $\text{Traces}(\text{TS}) = \text{Traces}(\text{TS}')$.

- a) Fix a trace $\pi = A_1 \dots A_n \in \text{Traces}_{\text{fin}}(\text{TS})$. We now show $\pi \in \text{Traces}_{\text{fin}}(\text{TS}')$.

Observe that π is a prefix of some $\pi' \in \text{Traces}(\text{TS})$ since $\text{Traces}(\text{TS})$ contains all traces of maximal (finite and infinite) paths. By assumption $\pi' \in \text{Traces}(\text{TS}')$ and then the same prefix π also belongs to $\text{Traces}_{\text{fin}}(\text{TS}')$. Note that this is independent of AP-determinism.

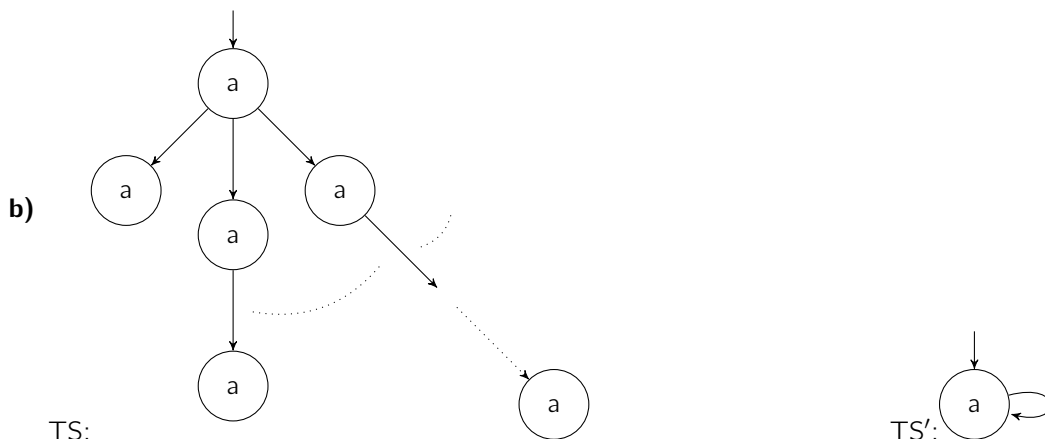
- b) Symmetrically, for a trace $\pi = A_1 \dots A_n \in \text{Traces}_{\text{fin}}(\text{TS}')$ it can be shown that $\pi \in \text{Traces}_{\text{fin}}(\text{TS})$.

Now we prove the other direction " $\Leftarrow$ ". Assume $\text{Traces}_{\text{fin}}(\text{TS}) = \text{Traces}_{\text{fin}}(\text{TS}')$.

- a) Fix an infinite¹ trace $\pi = A_1 A_2 \dots \in \text{Traces}(\text{TS})$. We now show $\pi \in \text{Traces}(\text{TS}')$.

Due to AP-determinism we know that every finite prefix of π has a unique underlying path. This means if we have a finite prefix $\pi' = A_1 \dots A_n$, $\pi' \in \text{Traces}_{\text{fin}}(\text{TS})$ and by assumption $\pi' \in \text{Traces}_{\text{fin}}(\text{TS}')$. We can extend it to $\pi' A_{n+1}$ along a unique path. This continues for all $n \in \mathbb{N}$ and therefore also the infinite trace π is in $\text{Traces}(\text{TS}')$.

- b) is again symmetric.



$$\text{Traces}(\text{TS}) = \{a^k \mid k \in \mathbb{N}\} \not\subseteq \{a^\omega\} = \text{Traces}(\text{TS}')$$

$$\text{however } \text{Traces}_{\text{fin}}(\text{TS}) = \{a^k \mid k \in \mathbb{N}\} = \text{Traces}_{\text{fin}}(\text{TS}').$$

¹ $\text{Traces}(\text{TS})$ also contains maximal finite paths, but if you pick a finite path here, there is nothing to left to prove.

Exercise 3 (Closure Properties):

(3 points)

Let Σ be a finite alphabet. A finite word x is a *prefix* of a word y (finite or infinite) is denoted as $x \prec y$. The linear time closure operator $\text{closure}: \mathcal{P}(\Sigma^\omega) \rightarrow \mathcal{P}(\Sigma^\omega)$ is defined as:

$$\text{closure}(T) = \{ t \in \Sigma^\omega \mid \forall x \prec t \exists t' \in T : x \prec t' \}.$$

Prove the following equivalences:

- a) $\text{closure}(\emptyset) = \emptyset$
- b) $A \subseteq B$ implies $\text{closure}(A) \subseteq \text{closure}(B)$
- c) $T \subseteq \text{closure}(T)$
- d) $\text{closure}(T) = \text{closure}(\text{closure}(T))$

Solution: _____

- a) $\text{closure}(\emptyset) = \emptyset$.

Proof: Assume there exists t such that $t \in \text{closure}(\emptyset)$.

$$\implies \forall x \prec t, \exists t' \in \emptyset : x \prec t'$$

$$\implies \exists t' \in \emptyset$$

$$\implies \text{false}$$

Hence, $t \notin \text{closure}(\emptyset)$.

- b) $A \subseteq B \implies \text{closure}(A) \subseteq \text{closure}(B)$.

Proof:

$$\begin{aligned} \text{closure}(A) &= \{ t \mid \forall x \prec t, \exists t' \in A : x \prec t' \} \\ &\subseteq \{ t \mid \forall x \prec t, \exists t' \in B : x \prec t' \} \\ &= \text{closure}(B) \end{aligned}$$

- c) $T \subseteq \text{closure}(T)$.

Proof: W.l.o.g. $T \neq \emptyset$

$$\begin{aligned} T &= \{ t \mid \exists t' \in T : t = t' \} \\ &= \{ t \mid \forall x \prec t \exists t' : t' \in T \text{ and } t = t' \text{ and } x \prec t' \} \\ &\subseteq \{ t \mid \forall x \prec t \exists t' : t' \in T \text{ and } x \prec t' \} \\ &= \text{closure}(T) \end{aligned}$$

- d) $\text{closure}(\text{closure}(T)) = \text{closure}(T)$.

Proof: It suffices to show $\text{closure}(\text{closure}(T)) \subseteq \text{closure}(T)$. The rest follows from b), c).

$$\begin{aligned} \text{closure}(\text{closure}(T)) &= \{ t \mid \forall x : (x \prec t) \rightarrow \exists t' : (x \prec t') \wedge (t' \in \text{closure}(T)) \} \\ &= \{ t \mid \forall x : (x \prec t) \rightarrow \exists t' : (x \prec t') \wedge (\forall y : (y \prec t') \rightarrow \exists t'' : (t'' \in T) \wedge y \prec t'') \} \\ &\subseteq \{ t \mid \forall x : (x \prec t) \rightarrow \exists t' : (x \prec t') \wedge ((x \prec t') \rightarrow \exists t'' : (t'' \in T) \wedge x \prec t'') \} \\ &= \{ t \mid \forall x : (x \prec t) \rightarrow (\exists t'' : (t'' \in T) \wedge x \prec t'') \} \\ &= \text{closure}(T) \end{aligned}$$

Exercise 4 (Fairness):

(2 points)

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

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

Consider the following fairness assumptions with respect to the transition system TS outlined on the right:

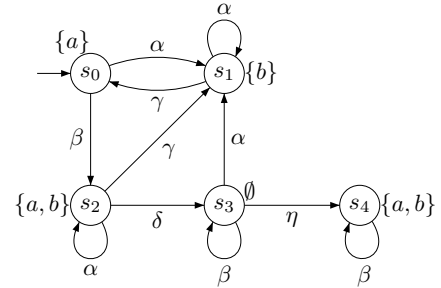
1. $\mathcal{F}_1 = (\{\{\alpha\}\}, \{\{\beta\}, \{\delta, \gamma\}, \{\eta\}\}, \emptyset)$.

Decide whether $TS \models_{\mathcal{F}_1} P$.

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

Decide whether $TS \models_{\mathcal{F}_2} P$.

Justify your answers!



Solution:

We consider each of the fairness assumptions $\mathcal{F}_i$ for $i \in \{1, 2\}$:

We have $TS \models_{\mathcal{F}_i} P$ iff $\text{FairTraces}_{\mathcal{F}_i}(TS) \subseteq P$. Because of $\exists^\infty k. A_k = \{a, b\}$, 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. $TS \models_{\mathcal{F}_1} P$:

- Any trace that reaches s_4 is not $\mathcal{F}_1$ -fair as α is executed only finitely many times. This is in contradiction to $\mathcal{F}_{1, \text{uncond}} = \{\{\alpha\}\}$.
- Therefore $s_3 \xrightarrow{\eta} s_4$ is never taken.
- Because of $\{\eta\} \in \mathcal{F}_{1, \text{strong}}$ and because η actions cannot be executed infinitely often (in fact, only once from s_3 to s_4), the state s_3 must not be visited infinitely often.
- We cannot stay in states s_1 or s_2 by only taking transitions $s_1 \xrightarrow{\alpha} s_1$ and $s_2 \xrightarrow{\alpha} s_2$ because of the enabled γ transitions to s_0 or s_1 , respectively.
- As β is enabled in s_0 , all $\mathcal{F}_1$ -fair paths visit exactly s_0, s_1 and s_2 infinitely often.

Therefore $\text{FairTraces}_{\mathcal{F}_1}(TS) \subseteq P$ and $TS \models_{\mathcal{F}_1} P$.

2. $TS \not\models_{\mathcal{F}_2} P$:

Consider the path $\pi = (s_0s_2s_3s_1)^\omega$ with its corresponding trace $\sigma = (\{a\}\{a, b\}\emptyset\{b\})^\omega$.

We have $\pi \in \text{FairPaths}_{\mathcal{F}_2}(TS)$, but $\sigma \notin P$.

$\Rightarrow \text{FairTraces}_{\mathcal{F}_2}(TS) \not\subseteq P$.