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

Introduction to Model Checking (Summer Term 2018)

— Solution 3 (due 14th May) —

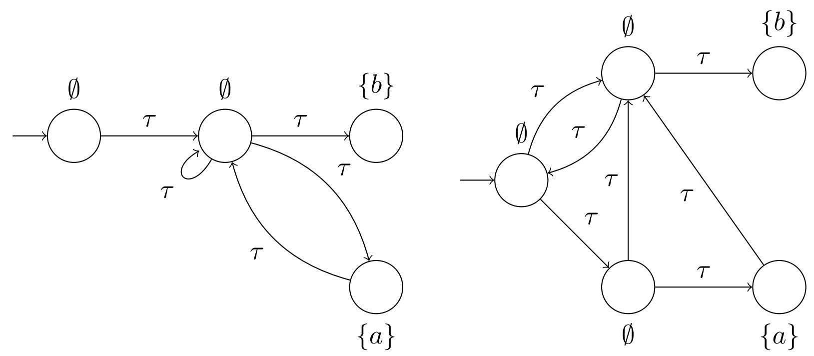
General Remarks

- 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 (1+1 Points)

Consider the following transition systems. Note that the transition systems might contain terminal states.

TS_1 : TS_2 :



(a) Give the traces of TS_1, i.e., $\mathit{Traces}(\mathrm{TS}_1)$.

(b) Are TS_1 and TS_2 trace equivalent?

Solution:

(a) $\mathit{Traces}(\mathrm{TS}_1) = \{\emptyset\emptyset(\emptyset + \{a\}\,\emptyset)^*\,\{b\} + \emptyset\emptyset(\emptyset + \{a\}\,\emptyset)^\omega\}$

(b) TS_1 and TS_2 are not trace equivalent. Consider the trace $\pi = \emptyset\emptyset\emptyset\,\{a\}\,\emptyset\,\{b\}$. It is $\pi \in \mathit{Traces}(\mathrm{TS}_1)$ but $\pi \notin \mathit{Traces}(\mathrm{TS}_2)$.

Exercise 2★ (4+4 Points)

In the following we show that LT properties are not solely a theoretical concept but have a wide range of practical applications. As proof, we apply the concept of LT properties to movie/TV series quotes.

(a) We assume each following quote informally describes some property. Formulate these properties as LT properties over the given set AP of atomic propositions:

(i) "**Winter is coming.**"
AP = $\{winter\}$.
winter will eventually by reached.

(ii) "**Everything is awesome.**"
AP = $\{awesome\}$.
awesome always holds.

(iii) "**I'll be back.**"
AP = $\{here\}$.
I am currently *here* but at some point I will not be *here*. However, I will be *here* again at a later time.

(iv) "**You either die a hero, or you live long enough to see yourself become the villain.**"
AP = $\{live, hero\}$.
In the beginning, you *live* and are a *hero*. You either cease to *live* and die, still being a *hero*, or you *live* but become the villain, i.e., you are not a *hero* anymore.

(v) "**By night one way, by day another**
Thus shall be the norm
Till you receive true love's kiss
then, take love's true form."
AP = $\{day, form_1, form_2, true\_form, kiss\}$.
You start by having $form_1$ at night, i.e., not *day*. You alternate between $form_1$ at night and $form_2$ by *day*. This alternation goes on till at some point you receive true love's *kiss* and from there on have love's *true_form*.

(vi) "**A Lannister always pays his debts.**"
AP = $\{in\_debt\}$.
Whenever a Lannister is *in_debt*, he will be *in_debt* as long as he has not payed back his debt. If he has payed back his debt, he is no longer *in_debt*. A Lannister can be *in_debt* arbitrarily (but finitely) many times.

(vii) "**Anything is possible [if you just believe].**"
AP = $\{ap_1, \ldots, ap_n\}$.
We do not consider the second part here and just concentrate on the fact, that everything is possible.

(viii) "**It's gonna be legen... wait for it... dary!**"
AP = $\{legen, wait\_for\_it, dary\}$.
In the beginning it is *legen*, then we have to *wait_for_it* for some time, and then it is *dary* at some point.

(b) Determine for all LT properties of (a) whether they are

(i) safety properties *and/or*

(ii) liveness properties.

Justify your answers.

Solution:

(a) We give the LT properties in the following as ω-regular expressions[1] (cf. exercise 1 of sheet 4).

(i) "Winter is coming."

$$P_1 = \emptyset^* \{winter\} (2^{\mathrm{AP}})^\omega$$

(ii) "Everything is awesome."

$$P_2 = \{awesome\}^\omega$$

[1]Note that the LT property P described by an ω-regular expression r is technically given as $P = \mathcal{L}_\omega(r)$.

(iii) "I'll be back."

$$P_3 = \{here\}^+ \, \emptyset^+ \, \{here\}^+ \, (2^{\mathrm{AP}})^\omega$$

(iv) "You either die a hero, or you live long enough to see yourself become the villain."

$$P_4 = \{live, hero\}^+ \, \{hero\} \, (2^{\mathrm{AP}})^\omega + \{live, hero\}^+ \, \{live\} \, (2^{\mathrm{AP}})^\omega$$

(v) "By night one way, by day another
Thus shall be the norm
Till you receive true love's kiss
then, take love's true form."

$$P_5 = \big((\{form_1\} \, \{day, form_2\})^+ + \{form_1\} \, (\{day, form_2\} \, \{form_1\})^*\big) \, \{kiss, true\_form\} \\ (\{true\_form\} \, \{true\_form, day\})^\omega$$

(vi) "A Lannister always pays his debts."

$$P_6 = \emptyset^* (\{in\_debt\}^+ \, \emptyset^+)^* \emptyset^\omega$$

(vii) "Anything is possible [if you just believe]"

$$P_7 = (2^{\mathrm{AP}})^\omega$$

(viii) "It's gonna be legen... wait for it... dary!"

$$P_8 = \{legen\} \, \{wait\_for\_it\}^+ \, \{dary\} \, (2^{\mathrm{AP}})^\omega$$

(b) First we consider which LT properties are safety properties. In case an LT property P is not a safety property we give a word w which is not in P as counterexample. Then we show, that w does not have a finite prefix w' which is a bad prefix, i.e. all prefixes w' can be extended to words $w'w''$ which are in P.

(i) P_1 is not a safety property. The word $w = \emptyset^\omega$ is not in P_1 but each prefix $w' = \emptyset^+$ of w can be extended to $w' \, \{winter\}^+ \, (2^{\mathrm{AP}})^\omega$ which is in P_1.

(ii) P_2 is a safety property, because P_2 is an invariant.

(iii) P_3 is not a safety property. The word $w = \{here\}^+ \, \emptyset^\omega$ is not in P_3 but each prefix $w' = \{here\}^+ \, \emptyset^*$ of w can be extended to $w' \, \{here\}^+ \, (2^{\mathrm{AP}})^\omega$ which is in P_3.

(iv) P_4 is not a safety property. The word $w = \{live, hero\}^\omega$ is not in P_4 but each prefix $w' = \{live, hero\}^+$ of w can be extended to $w' \, \{hero\}^+ \, (2^{\mathrm{AP}})^\omega$ which is in P_4.

(v) P_5 is not a safety property. The word $w = (\{form_1\} \, \{day, form_2\})^\omega$ is not in P_5 but each prefix $w' = (\{form_1\} \, \{day, form_2\})^+$ of w can be extended to $w' \, \{kiss, true\_form\} \, \{true\_form\}^\omega$ which is in P_5.

(vi) P_6 is not a safety property. The word $w = \emptyset^* \, \{in\_debt\}^\omega$ is not in P_6 but each prefix $w' = \emptyset^* \, \{in\_debt\}^+$ of w can be extended to $w'\emptyset^\omega$ which is in P_6.

(vii) P_7 is a safety property (see Lemma 3.35).

(viii) P_8 is not a safety property. The word $w = \{legen\} \, \{wait\_for\_it\}^\omega$ is not in P_8 but each prefix $w' = \{legen\} \, \{wait\_for\_it\}^+$ of w can be extended to $w' \, \{dary\} \, (2^{\mathrm{AP}})^\omega$ which is in P_8.

Second we consider which LT properties are liveness properties. In case an LT property P is not a liveness property we give a finite word w as counterexample and show that w cannot be extended to a word ww' which is in P.

(i) P_1 is a liveness property. Each prefix $w = \emptyset^* \, \{winter\} \, (2^{\mathrm{AP}})^*$ can be extended to $w(2^{\mathrm{AP}})^\omega$ in P_1. Each prefix $w' = \emptyset^+$ can be extended to $w' \, \{winter\} \, (2^{\mathrm{AP}})^\omega$ in P_1.

(ii) P_2 is not a liveness property. The prefix $w = \emptyset$ cannot be extended to a word in P_2.

(iii) P_3 is not a liveness property. The prefix $w = \emptyset$ cannot be extended to a word in P_3.

(iv) P_4 is not a liveness property. The prefix $w = \emptyset$ cannot be extended to a word in P_4.

(v) P_5 is not a liveness property. The prefix $w = \emptyset$ cannot be extended to a word in P_5.

(vi) P_6 is a liveness property. Each prefix $w = \emptyset^*(\{in\_debt\}^+\,\emptyset^*)^+$ can be extended to $w\emptyset^\omega$ in P_6. Each prefix $w' = \emptyset^+$ can be extended to $w'\emptyset^\omega$ in P_6.

(vii) P_7 is a liveness property (see Lemma 3.35).

(viii) P_8 is not a liveness property. The prefix $w = \emptyset$ cannot be extended to a word in P_8.

Exercise 3 (3+3 Points)

(a) Let P and P' be liveness properties over AP. Prove or disprove the following claims:

(i) $P \cup P'$ is a liveness property,

(ii) $P \cap P'$ is a liveness property.

(b) Answer the same questions for P and P' being safety properties.

Hint: you can use the distributivity of union over closure for LT properties P, P':

$$cl(P \cup P') = cl(P) \cup cl(P')$$

Solution:

Assume P and P' are liveness properties.

- $P \cup P'$ is a liveness property. This can be seen as follows. $\mathit{pref}(P) = \mathit{pref}(P') = \left(2^{\mathrm{AP}}\right)^+$. Moreover:

$$\mathit{pref}(P \cup P') = \bigcup_{\sigma \in P \cup P'} \mathit{pref}(\sigma) = \bigcup_{\sigma \in P} \mathit{pref}(\sigma) \cup \bigcup_{\sigma' \in P'} \mathit{pref}(\sigma') = \mathit{pref}(P) \cup \mathit{pref}(P')$$

  Thus $\mathit{pref}(P \cup P') = \left(2^{\mathrm{AP}}\right)^+$ and $P \cup P'$ is a liveness property.

- $P \cap P'$ is not a liveness property. A counterexample can be given as follows. Let $\mathrm{AP} = \{a, b\}$ and define

$$\begin{aligned} P &= \mathcal{L}_\omega\left(\left(2^{\mathrm{AP}}\right)^* a^\omega\right) \\ P' &= \mathcal{L}_\omega\left(\left(2^{\mathrm{AP}}\right)^* b^\omega\right). \end{aligned}$$

  Then $P \cap P' = \emptyset$; thus $P \cap P'$ is not a liveness property.

Now let P and P' be safety properties.

- $P \cup P'$ is a safety property. From the lecture we know that $cl(P \cup P') = cl(P) \cup cl(P')$. Given that P and P' are safety properties, we have

$$cl(P \cup P') = cl(P) \cup cl(P') = P \cup P'$$

  Thus $P \cup P'$ is a safety property.

- $P \cap P'$ is a safety property. Let $\sigma \in \left(2^{\mathrm{AP}}\right)^\omega \setminus (P \cap P')$. Either $\sigma \notin P$ or $\sigma \notin P'$; assume w.l.o.g. $\sigma \notin P$. Since P is a safety property, there exists $\hat{\sigma} \in \mathit{pref}(\sigma)$ such that

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

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

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

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

Exercise 4 (4 Points)

Let P be an LT property. Prove: $\mathit{pref}(\mathit{cl}(P)) = \mathit{pref}(P)$.

Solution:

We have to show that $\mathit{pref}(\mathit{cl}(P)) = \mathit{pref}(P)$ for any LT-property P.

"$\subseteq$":

$$\begin{aligned}
\text{Let } \hat{\sigma} \in \mathit{pref}(\mathit{cl}(P)) &\implies \exists \sigma \in \left(2^{\mathrm{AP}}\right)^{\omega} \text{ with } \sigma \in \mathit{cl}(P) \text{ and } \hat{\sigma} \in \mathit{pref}(\sigma) \\
&\implies \mathit{pref}(\sigma) \subseteq \mathit{pref}(P) \\
&\implies \hat{\sigma} \in \mathit{pref}(P).
\end{aligned}$$

$\supseteq$:

$$\begin{aligned}
\text{Let } \hat{\sigma} \in \mathit{pref}(P) &\implies \exists \sigma \in P \text{ with } \hat{\sigma} \in \mathit{pref}(\sigma) \\
&\implies \text{since } \sigma \in P \text{ we have } \mathit{pref}(\sigma) \subseteq \mathit{pref}(P) \\
&\implies \sigma \in \mathit{cl}(P) \\
&\implies \hat{\sigma} \in \mathit{pref}(\mathit{cl}(P)).
\end{aligned}$$