Prof. Dr. Ir. Dr. h. c. Joost-Pieter Katoen

Christian Hensel, Matthias Volk

Introduction to Model Checking (Summer Term 2018)

— Solution 6 (due 11th June) —

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+2+3+4 Points)

Consider the transition system TS_{Sem} for mutual exclusion with a semaphore.

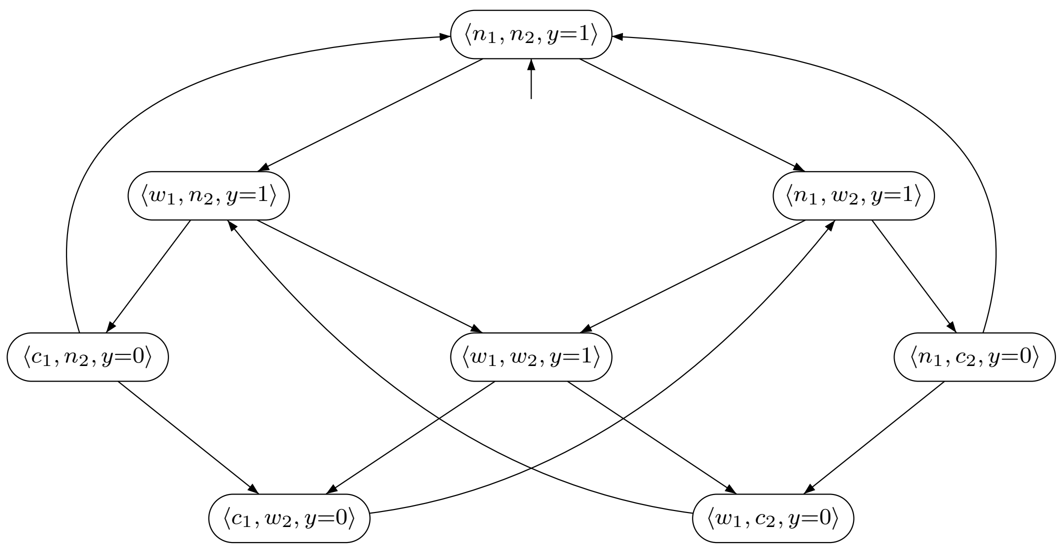


Figure 6.1: Mutual exclusion with semaphore (transition system representation).

Let P_{live} be the following ω-regular property over $\mathrm{AP} = \{wait_1, crit_1\}$:

"whenever process 1 is waiting for the critical section,
it will eventually (potentially at the very same time) be in its critical section."

Check whether $\mathrm{TS}_{Sem} \models P_{live}$ with the following steps:

(a) Introduce the necessary labels in TS_{Sem}.

(b) Depict an NBA $\overline{\mathcal{A}}$ for the complement property $\overline{P_{live}} = \left(2^{\mathrm{AP}}\right)^\omega \setminus P_{live}$.
Hint: There is an NBA $\overline{\mathcal{A}}$ for $\overline{P_{live}}$ with 3 states.

(c) Depict the reachable fragment of the product $TS_{Sem} \otimes \overline{\mathcal{A}}$.
Hint: There is an NBA for $\overline{\mathcal{A}}$ with 3 states that is a solution to task (b) and will lead to a product transition system with 19 states.

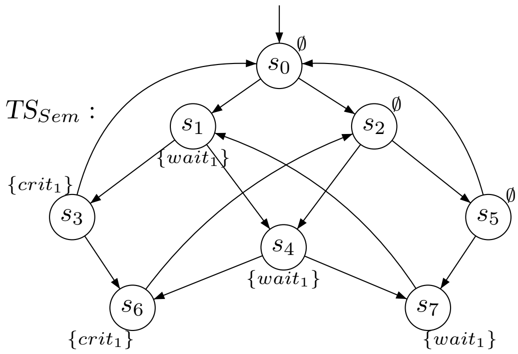
(d) Apply the nested depth-first search (lecture 11, slides 150 and 159) to $TS_{Sem} \otimes \overline{\mathcal{A}}$ for the persistence property "eventually forever $\neg F$", where F is the acceptance set of $\overline{\mathcal{A}}$. To illustrate the steps:

- before each *Pop* operation give:
  - for the first DFS the contents of stack π and set U, and
  - for the second DFS the contents of stack ξ and set V.
- indicate whenever *cycle_check*() is called.

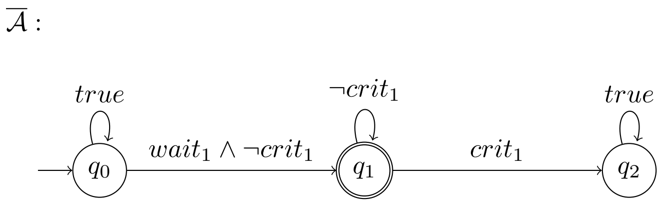
Does $TS_{Sem} \models P_{live}$ hold? In case the property is refuted, give the counterexample returned by the algorithm.

Solution:

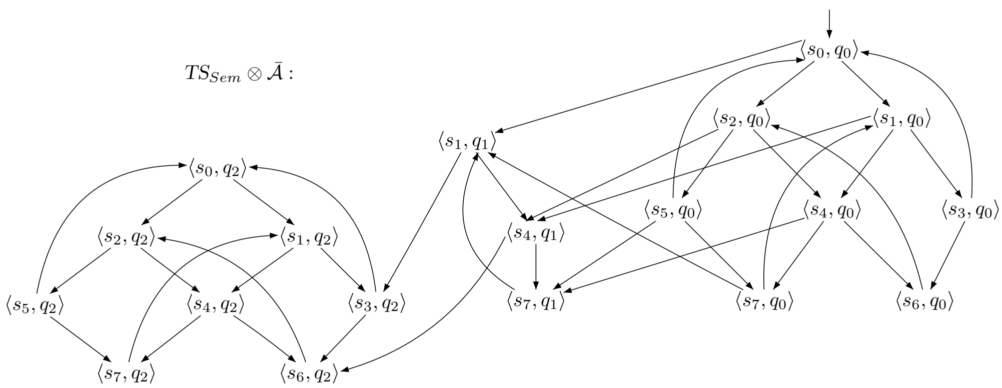
(a) The transition system TS_{Sem} can be outlined as follows:



(b) The NBA $\overline{\mathcal{A}}$ for $\overline{P_{live}} = \left(2^{\mathrm{AP}}\right)^{\omega} \setminus P_{live}$ is:



(c) Based on TS_{Sem} and $\overline{\mathcal{A}}$, we construct the product transition system $TS_{Sem} \otimes \overline{\mathcal{A}}$:



(d) To prove $\mathrm{TS}_{Sem} \not\models P_{live}$, we check the persistence property P_{pers} = "eventually forever Φ" (where $F = \{q_1\}$ and $\Phi = \neg F$) for the transition system $\mathrm{TS}_{Sem} \otimes \overline{\mathcal{A}}$. Using the nested depth-first search algorithm, we search for a reachable cycle in $\mathrm{TS}_{Sem} \otimes \overline{\mathcal{A}}$ containing at least one $\neg\Phi$-state (i.e., a state from F).

We denote the stack content from left to right and the top element is on the left. The algorithm yields the following:

- Initial state (1st DFS): $\langle s_0, q_0\rangle$

$$\begin{aligned} \pi &= \langle s_0, q_0\rangle \\ U &= \{\langle s_0, q_0\rangle\} \\ \xi &= \varepsilon \\ V &= \{\} \end{aligned}$$

- 1st descent (1st DFS):

$$\begin{aligned} \pi &= \langle s_0, q_2\rangle\langle s_3, q_2\rangle\langle s_1, q_2\rangle\langle s_7, q_2\rangle\langle s_4, q_2\rangle\langle s_2, q_2\rangle\langle s_6, q_2\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\ U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_4, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\ \xi &= \varepsilon \\ V &= \{\} \end{aligned}$$

$\langle s_0, q_2\rangle, \langle s_3, q_2\rangle, \langle s_1, q_2\rangle, \langle s_7, q_2\rangle, \langle s_4, q_2\rangle$ are popped from the stack as they have no successor states that are not visited yet and their state component is not a final state of $\overline{\mathcal{A}}$. This yields:

$$\begin{aligned} \pi &= \langle s_2, q_2\rangle\langle s_6, q_2\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\ U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_4, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\ \xi &= \varepsilon \\ V &= \{\} \end{aligned}$$

- 2nd descent (1st DFS):

$$\begin{aligned} \pi &= \langle s_5, q_2\rangle\langle s_2, q_2\rangle\langle s_6, q_2\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\ U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_4, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_5, q_2\rangle, \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\ \xi &= \varepsilon \\ V &= \{\} \end{aligned}$$

Again, all successor states of $\langle s_5, q_2\rangle$ are already visited ($\in U$), therefore $\langle s_5, q_2\rangle, \langle s_2, q_2\rangle$ and $\langle s_6, q_2\rangle$ are popped. This results in:

$$\begin{aligned} \pi &= \langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\ U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_4, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_5, q_2\rangle, \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\ \xi &= \varepsilon \\ V &= \{\} \end{aligned}$$

- 3rd descent (1st DFS): The successor state $\langle s_7, q_1\rangle$ of $\langle s_4, q_1\rangle$ is not visited yet:

$$\begin{aligned} \pi &= \langle s_1, q_1\rangle\langle s_7, q_1\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\ U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_1, q_1\rangle, \langle s_4, q_1\rangle, \langle s_7, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_5, q_2\rangle, \\ &\quad \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\ \xi &= \varepsilon \\ V &= \{\} \end{aligned}$$

Now, all successor states of $\langle s_1, q_1\rangle$ are already visited. However, since $\langle s_1, q_1\rangle \not\models \Phi$ ($q_1 \in F$), we start a nested depth-first search from here looking for a backward edge to $\langle s_1, q_1\rangle$ and pop $\langle s_1, q_1\rangle$ from π.

- **cycle_check**($\langle s_1, q_1\rangle$): Initial configuration (1st DFS):

$$\begin{aligned}
\pi &= \langle s_7, q_1\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\
U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_1, q_1\rangle, \langle s_4, q_1\rangle, \langle s_7, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_5, q_2\rangle, \\
&\quad \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\
\xi &= \varepsilon \\
V &= \{\}
\end{aligned}$$

- 1st descent (2nd DFS):

$$\begin{aligned}
\pi &= \langle s_7, q_1\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\
U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_1, q_1\rangle, \langle s_4, q_1\rangle, \langle s_7, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_5, q_2\rangle, \\
&\quad \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\
\xi &= \langle s_7, q_1\rangle\langle s_4, q_1\rangle\langle s_1, q_1\rangle \\
V &= \{\langle s_1, q_1\rangle, \langle s_4, q_1\rangle, \langle s_7, q_1\rangle\}
\end{aligned}$$

$Post(\langle s_7, q_1\rangle) = \{\langle s_1, q_1\rangle\}$ and therefore we found a backward edge to $\langle s_1, q_1\rangle$.

$$\begin{aligned}
\pi &= \langle s_7, q_1\rangle\langle s_4, q_1\rangle\langle s_2, q_0\rangle\langle s_0, q_0\rangle \\
U &= \{\langle s_0, q_0\rangle, \langle s_2, q_0\rangle, \langle s_1, q_1\rangle, \langle s_4, q_1\rangle, \langle s_7, q_1\rangle, \langle s_0, q_2\rangle, \langle s_1, q_2\rangle, \langle s_2, q_2\rangle, \langle s_3, q_2\rangle, \langle s_4, q_2\rangle, \langle s_5, q_2\rangle, \\
&\quad \langle s_6, q_2\rangle, \langle s_7, q_2\rangle\} \\
\xi &= \langle s_1, q_1\rangle\langle s_7, q_1\rangle\langle s_4, q_1\rangle\langle s_1, q_1\rangle \\
V &= \{\langle s_1, q_1\rangle, \langle s_4, q_1\rangle, \langle s_7, q_1\rangle\}
\end{aligned}$$

The generated counterexample now is:

$$Reverse(\xi \cdot \pi) = \langle s_0, q_0\rangle\langle s_2, q_0\rangle\langle s_4, q_1\rangle\langle s_7, q_1\rangle\langle s_1, q_1\rangle\langle s_4, q_1\rangle\langle s_7, q_1\rangle\langle s_1, q_1\rangle$$

Note that different state successors could be chosen during the DFS leading to different counterexamples. For example the following is also a valid counterexample:

$$\langle s_0, q_0\rangle\langle s_1, q_1\rangle\langle s_4, q_1\rangle\langle s_7, q_1\rangle\langle s_1, q_1\rangle\langle s_4, q_1\rangle\langle s_7, q_1\rangle$$

Exercise 2* (4 Points)

Recall the following LT properties from exercise sheet 3.

(i) "**Winter is coming.**"
$P_1 = \emptyset^* \{winter\} (2^{\mathrm{AP}})^\omega$

(ii) "**Everything is awesome.**"
$P_2 = \{awesome\}^\omega$

(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.**"

$$\begin{aligned}
P_5 = &\big((\{form_1\}\{day, form_2\})^+ + \{form_1\}(\{day, form_2\}\{form_1\})^*\big)\{kiss, true_form\} \\
&(\{true_form\}\{true_form, day\})^\omega
\end{aligned}$$

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

Express each property P_i as an LTL formula φ_i.

Solution:

(i) "**Winter is coming.**"
$\varphi_1 = \Diamond\, winter$

(ii) "**Everything is awesome.**"
$\varphi_2 = \Box\, awesome$

(iii) "**I'll be back.**"
$\varphi_3 = here \wedge \big(here \,\mathsf{U}\, (\neg here \wedge (\neg here \,\mathsf{U}\, here))\big)$ or
$\varphi_3' = here \wedge \bigcirc \big(\Diamond\, (\neg here \wedge \bigcirc \Diamond\, here)\big)$

(iv) "**You either die a hero, or you live long enough to see yourself become the villain.**"
$\varphi_4 = (live \wedge hero) \wedge \big((live \wedge hero) \,\mathsf{U}\, ((\neg live \wedge hero) \vee (live \wedge \neg hero))\big)$

(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."
Let $NF = form_1 \wedge \neg day$, $DF = form_2 \wedge day$, $NT = true\_form \wedge \neg day$, $DT = true\_form \wedge day$.
Further let $Alter_1 = \big((NF \wedge \bigcirc DF) \vee (DF \wedge \bigcirc NF)\big) \wedge \neg kiss \wedge \neg true\_form$ and
$Alter_2 = \big((NT \wedge \bigcirc DT) \vee (DT \wedge \bigcirc NT)\big) \wedge \neg form_1 \wedge \neg form_2$.

$$\varphi_7 = NF \wedge NotKiss \wedge \Bigg((Alter_1) \,\mathsf{U}\, \Big(\bigcirc \Big(kiss \wedge true\_form \wedge \neg form_1 \wedge \neg form_2 \wedge \neg day \wedge \bigcirc \big(NT \wedge \Box\, (Alter_2)\big)\Big)\Big)\Bigg)$$

(vi) "**A Lannister always pays his debts.**"
$\varphi_6 = \Diamond \Box \neg in\_debt$

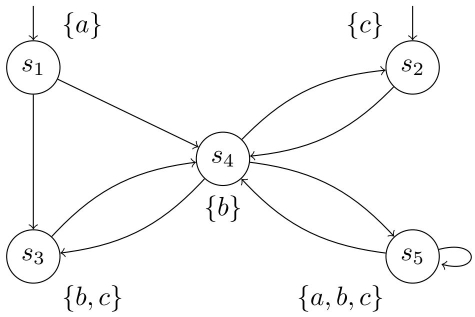
(vii) "**Anything is possible [if you just believe]**"
$\varphi_7 = true$

(viii) "**It's gonna be legen... wait for it... dary!**"
$\varphi_8 = (legen \wedge \neg wait\_for\_it \wedge \neg dary) \wedge \bigcirc \Big((wait\_for\_it \wedge \neg legen \wedge \neg dary) \wedge \big((wait\_for\_it \wedge \neg legen \wedge \neg dary) \,\mathsf{U}\, (dary \wedge \neg legen \wedge \neg wait\_for\_it)\big)\Big)$

Exercise 3★ (6 Points)

Consider the following transition system TS where we omit the transition labels, because they are all τ.

TS :



For each of the LTL formulae φ_i below, decide whether TS $\models \varphi_i$. Justify your answer and, in particular, provide a path $\pi_i \in \mathit{Paths}(\text{TS})$ such that $\pi_i \not\models \varphi_i$ in case you find TS $\not\models \varphi_i$.

- $\varphi_1 = \Diamond \Box c$,
- $\varphi_2 = \Box \Diamond c$,
- $\varphi_3 = \bigcirc \neg c \rightarrow \bigcirc \bigcirc c$,
- $\varphi_4 = \Box a$,
- $\varphi_5 = a \mathsf{U} \Box (b \vee c)$,
- $\varphi_6 = (\bigcirc \bigcirc b) \mathsf{U} (b \vee c)$,
- $\varphi_7 = c \mathsf{R} b$,

where the *release operator* $\varphi \mathsf{R} \psi$ for two LTL formulae φ, ψ is defined by $\varphi \mathsf{R} \psi \equiv \neg(\neg\varphi \mathsf{U} \neg\psi)$.

Solution:

- TS $\not\models \varphi_1$ since the path $\pi_1 = (s_2 s_4)^\omega$ has trace $\sigma_1 = (\{c\}\,\{b\})^\omega$ and $\sigma_1 \not\models \varphi_1$,
- TS $\models \varphi_2$. All paths in TS visit either s_4 or s_5 infinitely often and all their successors satisfy c.
- TS $\models \varphi_3$. If a trace in TS has $\bigcirc \neg c$ at some position i, the corresponding path must be in s_1, s_2, s_3 or s_5 at position i and in s_4 at position $i+1$. As all successors of s_4 are labeled with a set including c, we have c at position $i+2$.
- TS $\not\models \varphi_4$ since along the path $\pi_4 = \pi_1$ with $\sigma_4 = \sigma_1$ the atomic proposition a does not hold at the first position.
- TS $\models \varphi_5$. Once a path reaches s_2, s_3, s_4 or s_5, the right-hand side $\Box (b \vee c)$ of the until formula is satisfied. In particular, all paths starting in s_2 have traces satisfying φ_5. The traces of paths starting in s_1 start with an $\{a\}$ satisfying the left-hand side of the until formula and have $\Box b \vee x$ in all their successors.
- TS $\not\models \varphi_6$. Consider the path $\pi_6 = s_1 (s_4 s_2)^\omega$ with trace $\sigma_6 = \{a\}\,(\{b\}\,\{c\})^\omega$. Then $\sigma_6 \not\models b \vee c$. The until formula therefore requires $\bigcirc \bigcirc b$, but $\sigma_6 \not\models \bigcirc \bigcirc b$.
- TS $\not\models \varphi_7$ since the path $\pi_7 = s_1 (s_4 s_3)^\omega$ has trace $\sigma_7 = \{a\}\,(\{b\}\,\{b, c\})^\omega$ and $\sigma_7 \not\models c \mathsf{R} b$, because neither b nor c hold at the first position.