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

Introduction to Model Checking (Summer Term 2018)

— Exercise Sheet 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.

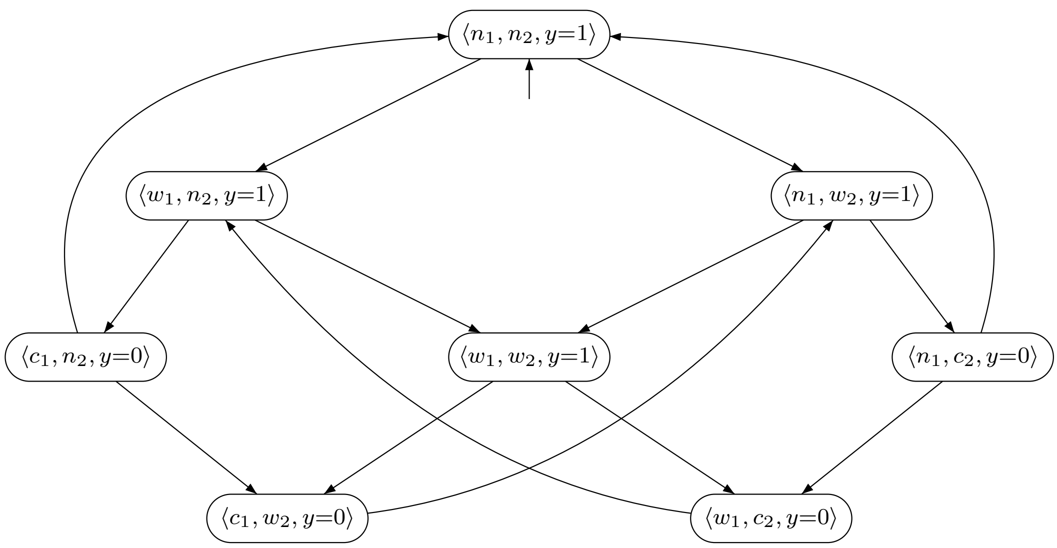


Figure 6.1: Mutual exclusion with semaphore (transition system representation).

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

"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 $TS_{Sem} \models P_{live}$ with the following steps:

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

(b) Depict an NBA $\overline{\mathcal{A}}$ for the complement property $\overline{P_{live}} = \left(2^{AP}\right)^{\omega} \setminus P_{live}$.
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.

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.**"

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

(vi) "**A Lannister always pays his debts.**"
$P_6 = \emptyset^* (\{in\_debt\}^+ \emptyset^+)^* \emptyset^\omega$

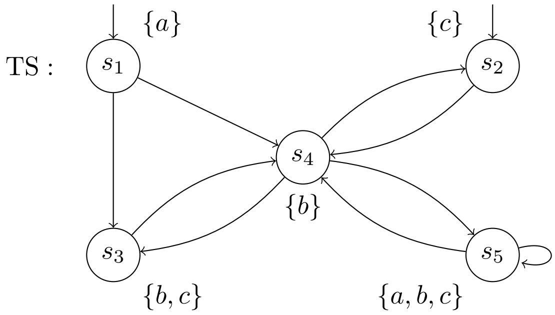
(vii) "**Anything is possible [if you just believe]**"
$P_7 = (2^{\mathrm{AP}})^\omega$

(viii) "**It's gonna be legen... wait for it... dary!**"
$P_8 = \{legen\} \{wait\_for\_it\}^+ \{dary\} (2^{\mathrm{AP}})^\omega$

Express each property P_i as an LTL formula φ_i.

Exercise 3★ (6 Points)

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



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

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

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