Prof. Dr. Andreas Podelski
Elisabeth Henkel
Dominik Klumpp

Hand in until November 29th, 2023
15:59 via ILIAS
Discussion: December 4th/5th, 2023

Tutorial for Cyber-Physical Systems - Discrete Models
Exercise Sheet 6

Accuracy is very important when talking about properties of a system. Therefore, we will now fix the meaning of symbols for which different interpretations have been encountered in the previous submissions: The symbol $\mathbb{N}$ denotes the set $\{0, 1, 2, \ldots\}$ of (non-negative) natural numbers. We use $\mathbb{N}_{>i}$, where i can be any natural number, to denote the set $\{i+1, i+2, i+3, \ldots\}$, e.g., by $\mathbb{N}_{>0}$, we denote the set $\{1, 2, 3, \ldots\}$ of positive natural numbers.

Exercise 1: Linear-Time Properties — 5 Points

The goal of this exercise is to find properties for given transition systems.

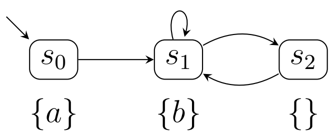
Assume $AP = \{a, b\}$. For each of the transition system T_i, complete the following tasks:

(a) Give a property (different from "True") using set comprehension that is satisfied by T_i. Do not use any property more than once.

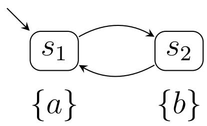
(b) Give a property (different from "False") using set comprehension that is not satisfied by T_i. Do not use any property more than once.

Example: The property "always a" can be formalized using set comprehension as $\{A_0A_1A_2 \ldots | \forall i \in \mathbb{N} \,.\, a \in A_i\}$.

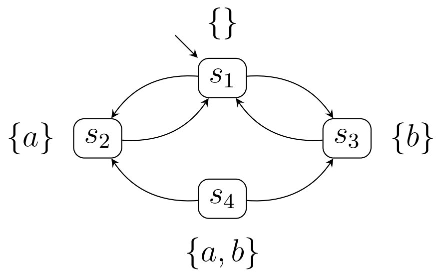
(T_1)



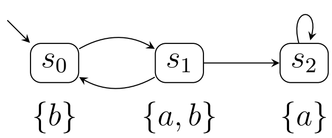
(T_2)



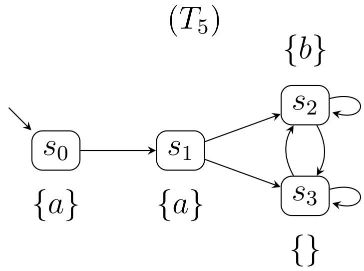
(T_3)



(T_4)



(T_5)



Exercise 2: Starvation Freedom 5 Points

Below you can see two different definitions of the starvation freedom property for the mutual exclusion problem. We consider the set of atomic propositions $AP = \{\mathsf{wait}_1, \mathsf{wait}_2, \mathsf{crit}_1, \mathsf{crit}_2\}$. The properties are defined as

$$LIVE := \begin{cases} \text{set of all infinite traces } A_0A_1A_2\ldots \text{ s.t.} \\ (\overset{\infty}{\exists} i \in \mathbb{N}\,.\,\mathsf{wait}_1 \in A_i) \to \overset{\infty}{\exists} i \in \mathbb{N}\,.\,\mathsf{crit}_1 \in A_i \\ (\overset{\infty}{\exists} i \in \mathbb{N}\,.\,\mathsf{wait}_2 \in A_i) \to \overset{\infty}{\exists} i \in \mathbb{N}\,.\,\mathsf{crit}_2 \in A_i \end{cases}$$

$$LIVE' := \begin{cases} \text{set of all infinite traces } A_0A_1A_2\ldots \text{ s.t.} \\ \forall i \in \mathbb{N}\,.\,(\mathsf{wait}_1 \in A_i \to \exists j \in \mathbb{N}\,.\,j \geq i \wedge \mathsf{crit}_1 \in A_j) \\ \forall i \in \mathbb{N}\,.\,(\mathsf{wait}_2 \in A_i \to \exists j \in \mathbb{N}\,.\,j \geq i \wedge \mathsf{crit}_2 \in A_j) \end{cases}$$

(a) Show that the property $LIVE'$ is at least as strong as the property $LIVE$, i.e., prove that $LIVE' \subseteq LIVE$.

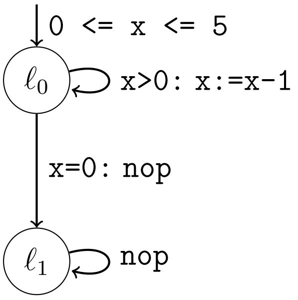
(b) Show that $LIVE'$ is a *strictly stronger* property than $LIVE$: Give an infinite trace $\pi = A_0A_1A_2\ldots$, and prove that $\pi \in LIVE$ but $\pi \notin LIVE'$.

(c) Does such a trace π with $\pi \in LIVE$ but $\pi \notin LIVE'$ exist in the transition systems for mutual exclusion discussed in the lecture (with semaphore resp. with Peterson algorithm)? Why/why not?

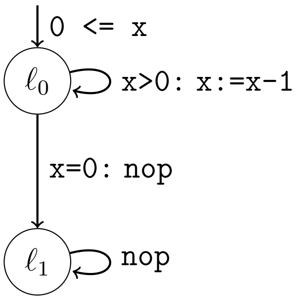
(d) Does there exist a trace π with $\pi \in LIVE'$ but $\pi \notin LIVE$ in the transition systems for mutual exclusion discussed in the lecture (with semaphore resp. with Peterson algorithm)? Why/why not?

Exercise 3: Trace Inclusion 9 Points

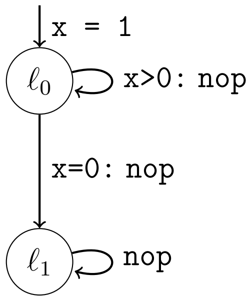
Consider the program graphs $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_{3a}$, and $\mathcal{P}_{3b}$ as well as the transition system $\mathcal{T}_4$.



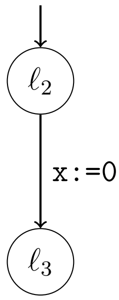
$\mathcal{P}_1$



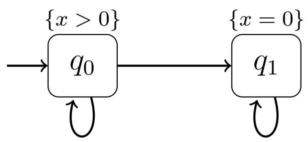
$\mathcal{P}_2$



$\mathcal{P}_{3a}$



$\mathcal{P}_{3b}$



$\mathcal{T}_4$

The domain of the variable x in all 3 program graphs is the set of integers $\mathbb{Z}$. The effect of the assignment action is as expected, and $\mathit{Effect}(\texttt{nop}, \eta) = \eta$.

(a) Draw the (reachable part of the) transition systems $\mathcal{T}_{\mathcal{P}_1}$, $\mathcal{T}_{\mathcal{P}_2}$ and $\mathcal{T}_{\mathcal{P}_{3a} ||| \mathcal{P}_{3b}}$.

As atomic propositions of the transition system, use the guards of the actions in the program graph, i.e. $AP = \{x > 0, x = 0\}$.

(b) For each of the 12 possible pairs $(\mathcal{T}, \mathcal{T}')$ that one can form with $\mathcal{T}$ and $\mathcal{T}'$ in $\{\mathcal{T}_{\mathcal{P}_1}, \mathcal{T}_{\mathcal{P}_2}, \mathcal{T}_{\mathcal{P}_{3a} ||| \mathcal{P}_{3b}}, \mathcal{T}_4\}$, consider the trace inclusion $\mathit{Traces}(\mathcal{T}) \subseteq \mathit{Traces}(\mathcal{T}')$. If it holds, argue why this is the case. If it does not hold, give a trace $\pi = A_0 A_1 A_2 \ldots$ such that $\pi \in \mathit{Traces}(\mathcal{T})$ but $\pi \notin \mathit{Traces}(\mathcal{T}')$.

(c) Give a property E (i.e., a set of traces) such that $\mathcal{T}_{\mathcal{P}_1} \models E$ and $\mathcal{T}_{\mathcal{P}_2} \models E$ but $\mathcal{T}_{\mathcal{P}_{3a} ||| \mathcal{P}_{3b}} \not\models E$ and $\mathcal{T}_4 \not\models E$. Explain why each of the four hold; i.e., argue why $\mathcal{T}_{\mathcal{P}_1}$ and $\mathcal{T}_{\mathcal{P}_2}$ satisfy the property E, and give traces of $\mathcal{T}_{\mathcal{P}_{3a} ||| \mathcal{P}_{3b}}$ and $\mathcal{T}_4$ that violate the property E.