Prof. Dr. Andreas Podelski
Dominik Klumpp

Hand in until December 18th, 2019
15:59 via the post boxes
Discussion: January 13th, 2020

Tutorial for Cyber-Physical Systems - Discrete Models

Exercise Sheet 9

Exercise 1: Starvation Freedom 4 Points

In the lecture we discussed 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

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

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

where $\exists^\infty$ means *"there exist infinitely many"*.

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

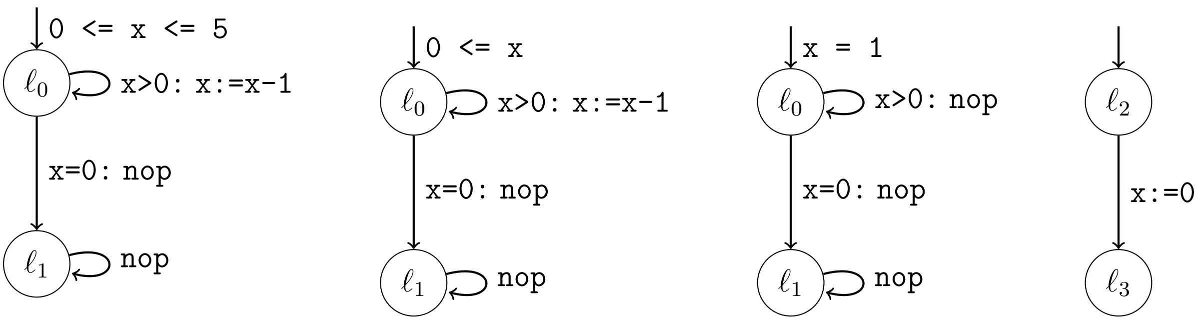
(b) Show that $LIVE'$ is a *strictly stronger* property than $LIVE$: Give an infinite trace $\pi = A_0A_1A_2\dots$, and prove that $\pi \in LIVE$ but $\pi \notin LIVE'$.

(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?

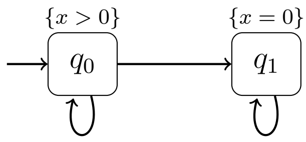
(d) Does there exist a trace π with $\pi \in LIVE'$ but $\pi \notin LIVE$ in the transition systems for mutual exclusion discussed in the lecture (with semaphore resp. with Peterson algorithm)? Why/why not?

Exercise 2: 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 pair $\mathcal{T}, \mathcal{T}' \in \{\mathcal{T}_{\mathcal{P}_1}, \mathcal{T}_{\mathcal{P}_2} \mathcal{T}_{\mathcal{P}_{3a} ||| \mathcal{P}_{3b}}, \mathcal{T}_4\}$, 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 $\mathcal{T}_4 \not\models E$. Give traces of $\mathcal{T}_{\mathcal{P}_{3a} ||| \mathcal{P}_{3b}}$ and $\mathcal{T}_4$ that violate the property, and argue why $\mathcal{T}_{\mathcal{P}_1}$ and $\mathcal{T}_{\mathcal{P}_2}$ satisfy the property.