Prof. Dr. Andreas Podelski
Dominik Klumpp

Hand in until February 10th, 2020
15:59 via the post boxes
Discussion: February 12th, 2020

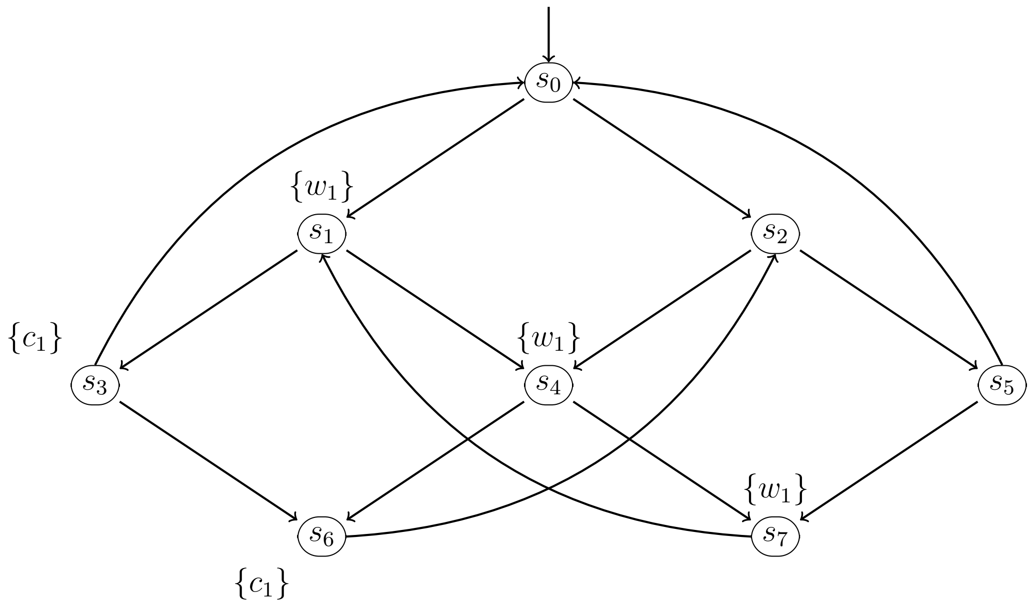
Tutorial for Cyber-Physical Systems - Discrete Models
Exercise Sheet 15

⚠ This exercise sheet must be submitted by Monday, not Wednesday! ⚠

The goal of this exercise sheet is to demonstrate how a computer can check whether a cyber-physical system (modeled as transition system) satisfies an omega-regular correctness property. All the steps in the exercise below can be performed automatically.

Exercise 1: Checking ω-regular properties 8 Points

Consider the transition system $\mathcal{T}_{sem}$ for mutual exclusion with a semaphore below.



Let $AP = \{w_1, c_1\}$ and let $\Sigma = 2^{AP}$. Let P_{live} be the following ω-regular property:

> "Whenever process 1 is in its waiting location (w_1), it will eventually enter its critical section (c_1)."

Perform the following steps to check if $\mathcal{T}_{sem}$ satisfies this property.

(a) Give an ω-regular expression for P_{live}.

(b) Convert the transition system $\mathcal{T}_{sem}$ to a nondeterministic Büchi automaton (NBA), i.e., draw an NBA $\mathcal{A}_{\mathcal{T}_{sem}}$ such that $Traces(\mathcal{T}_{sem}) = \mathcal{L}_\omega(\mathcal{A}_{\mathcal{T}_{sem}})$. All states in this NBA should be accepting.

(c) Draw an NBA $\mathcal{A}_{\overline{P}_{live}}$ for the complement property $\overline{P}_{live} = \Sigma^\omega \setminus P_{live}$.

You may give the NBA in symbolic notation (edges labeled with propositional formulas) or in standard notation (edges labeled by letters in Σ). However, for the next exercise below, it will be useful to have the standard notation.

(d) Construct the reachable fragment of the parallel composition (or *"product automaton"*) $\mathcal{A}_{\mathcal{T}_{sem}} \parallel_\Sigma \mathcal{A}_{\overline{P}_{live}}$. As in the previous exercise sheet, the synchronization labels (for handshaking) are here the letters in Σ.

(e) Check $\mathcal{A}_{\mathcal{T}_{sem}} \parallel_\Sigma \mathcal{A}_{\overline{P}_{live}}$ for lassos: Determine if there exists a state $\langle q, p\rangle$ such that

(i) $\langle q, p\rangle$ is reachable from an initial state,

(ii) q is an accepting state of $\mathcal{A}_{\mathcal{T}_{sem}}$ and p is an accepting state of $\mathcal{A}_{\overline{P}_{live}}$,

(iii) and from $\langle q, p\rangle$, the same state $\langle q, p\rangle$ can be reached again (with at least one transition in between).

If no lasso exists, then $\mathcal{T}_{sem} \models P_{live}$.

If such a lasso exists, then give the lasso trace and the corresponding execution of $\mathcal{T}_{sem}$. The trace is then a counterexample: It is a trace of $\mathcal{T}_{sem}$ that does not satisfy the property P_{live}. Therefore $\mathcal{T}_{sem} \not\models P_{live}$.