Prof. Dr. Andreas Podelski
Dominik Klumpp

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

Tutorial for Cyber-Physical Systems - Discrete Models
Exercise Sheet 4

In this exercise sheet, we will work with transition systems and the different methods of synchronization and communication between their components.

Exercise 1: Railroad Crossing — 6 Points

The goal of this exercise is to demonstrate how synchronous communication (handshaking) can be used to control the possible behaviours of a transition system.

In the lecture we discussed a model of a railroad crossing involving a train, a controller and a gate. We saw that the transition system $\mathit{Train} \parallel \mathit{Controller} \parallel \mathit{Gate}$ for this model can reach a configuration where the train is on the crossing (state *in*) but the gate has not been lowered (state *up*). This is of course undesirable, the train should only be on the crossing when the gate is lowered.

(a) Identify the design flaw that causes this problem.

Hint: Consider for instance the case where the gate is stuck and cannot be lowered.

(b) How can this design flaw be fixed? Give the transition systems Train', $\mathit{Controller}'$ and Gate' for the repaired components.

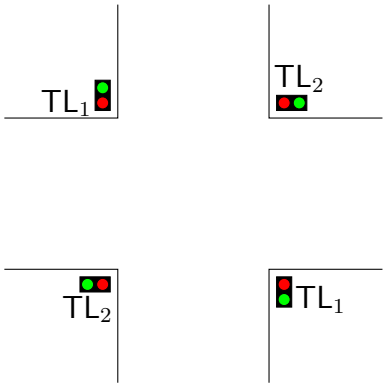
Hint: You can introduce additional states as well as new actions, which can be used to synchronize components and reduce nondeterminism. It is not necessary to change the gate.

(c) Draw the transition system for the new model, i.e., the parallel composition of the three components $\mathit{Train}' \parallel \mathit{Controller}' \parallel \mathit{Gate}'$.

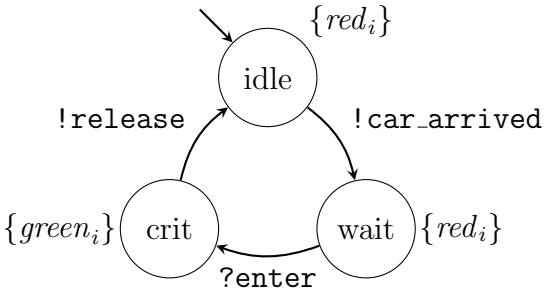
Exercise 2: Crossroads Traffic Lights — 5 Points

The goal of this exercise is to practice using an arbiter for synchronization, and to understand the limitations of this approach.

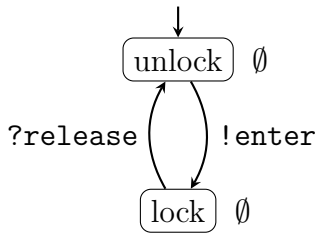
Consider the crossing of two roads with four traffic lights as depicted on the right. The two traffic lights labelled with TL_1 always show the same color, and likewise the two traffic lights labelled with TL_2 always show the same color. The traffic-lights are demand-driven and only switch to green when they have detected the presence of a car.



We model this system with two transition systems, TS_1 and TS_2, for the traffic lights, one for each direction of the crossing. To avoid car crashes, these transition systems are connected via an arbiter that ensures only one traffic light can be green at a time.



TS_i



Arbiter

(a) Draw the parallel composition $(TS_1 ||| TS_2) \parallel \mathit{Arbiter}$ of the three transition systems. The traffic lights do not synchronize with each other, but they both synchronize with the arbiter. A configuration of the composed system is labeled with all atomic propositions that hold in any of its local states.

(b) Use the transition system to answer the following questions.

- Is the system safe, i.e., can the traffic lights for both streets be green at the same time? Why / why not?
- What other property would we expect from a traffic light? Why does it not hold here?