Prof. Dr. Andreas Podelski
Dominik Klumpp

Hand in until January 29th, 2020
15:59 via the post boxes
Discussion: February 3rd, 2020

Tutorial for Cyber-Physical Systems - Discrete Models

Exercise Sheet 13

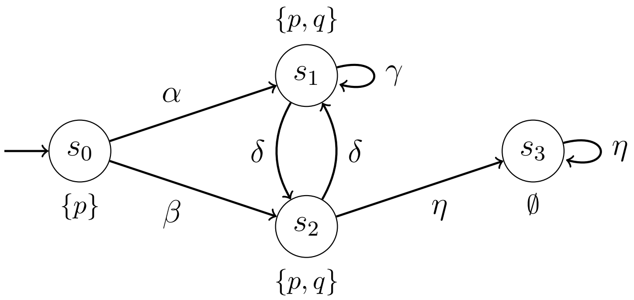
The goal of this exercise sheet is to understand fairness. Modeling the behavior of a cyber-physical system as a transition system is fine when one is interested in safety properties. However, it is not always sufficient when one is interested in liveness properties. Remember that a counterexample to a liveness property must be represented by an infinite path, but not every infinite path is realistic. We use fairness to single out realistic paths. In other words, our model is given by a transition system together with a fairness assumption.

Exercise 1*: Evaluation — 1 Bonus Point

Complete the lecture evaluation.

Exercise 2: Fairness — 10 Points

Consider the following transition system:



and the following questions:

(Q1) Is $s_0 \xrightarrow{\beta} s_2 \xrightarrow{\eta} s_3 (\xrightarrow{\eta} s_3)^\omega$ a fair execution?

(Q2) Is $s_0 \xrightarrow{\alpha} s_1 (\xrightarrow{\gamma} s_1)^\omega$ a fair execution?

(Q3) Is $s_0 \xrightarrow{\alpha} s_1 \xrightarrow{\delta} s_2 (\xrightarrow{\delta} s_1 \xrightarrow{\delta} s_2)^\omega$ a fair execution?

(Q4) Is $\{p\}\,\{p, q\}^\omega$ a fair trace?

Answer the questions $(Q1) - (Q4)$ for each of the fairness assumptions below. Justify your answers.

(a) unconditional fairness for $\{\alpha\}$

(b) weak fairness for $\{\delta\}$

(c) weak fairness for $\{\delta\}$ and strong fairness for $\{\eta\}$

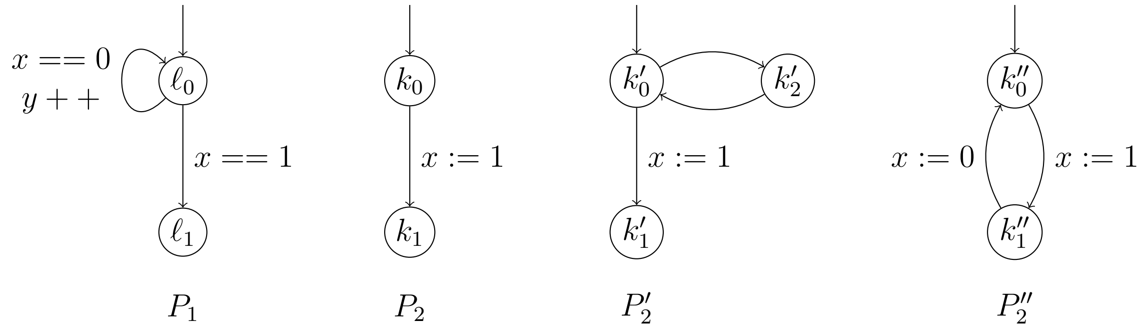
(d) strong fairness for $\{\gamma\}$

(e) weak fairness for $\{\gamma, \eta\}$

Exercise 3: Fairness Assumptions 6 Points

The goal of this task is to learn how to model a realistic system by choosing suitable fairness assumptions.

Consider the following program graphs.



Let $AP = \{exit\}$ and the atomic proposition *exit* holds if P_1 is in location ℓ_1. Consider the following parallel systems:

(a) $P_1 ||| P_2$ (b) $P_1 ||| P_2'$ (c) $P_1 ||| P_2''$

Assume that initially the variables x and y are equal to 0 in each system. As we usually consider infinite runs, assume that the terminal state ℓ_1 has an implicit self-loop (and termination of the program is modeled using the atomic proposition *exit*).

For each of the parallel systems given in (a)–(c), perform the following tasks.

(i) Draw an outline of the reachable part of the transition system for the interleaving.

(ii) We write *set* for $x := 1$. Give the weakest fairness assumption on the set $A = \{set\}$ (if there exists such a fairness assumption) such that the parallel system terminates, i.e., the system satisfies the liveness property "eventually *exit*" under this fairness assumption.