Prof. Dr. Andreas Podelski
Tanja Schindler

Hand in until January 30th, 2019
15:59 via the post boxes
Discussion: February 4th/5th, 2019

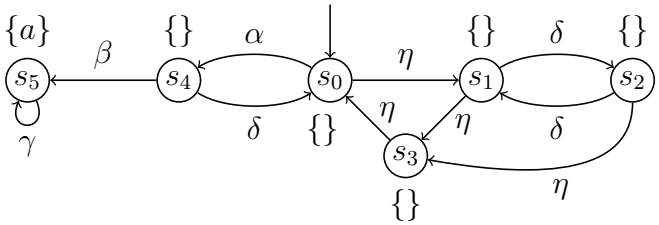
Tutorial for Cyber-Physical Systems - Discrete Models
Exercise Sheet 12

The goal of this exercise sheet is to understand fairness. To model the behavior of a transition system (i.e., a graph) is fine when one is interested in safety properties but it is not 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 graph plus a fairness assumption.

Exercise 1: Fairness, Traces, and Satisfaction under Fairness Assumptions

The goal of this task is to train your ability to identify fair and unfair traces of a given transition system, in order to reason about properties of a system under given fairness assumptions.

Consider the following transition system:



For the fairness assumptions given in (a)–(h), perform the following tasks.

(i) For each of the fairness assumptions below, give an execution that fulfills the fairness assumption (a fair trace) and an execution that violates the fairness assumption (an unfair trace).

(ii) A system satisfies a property P under a given fairness assumption, if all fair traces satisfy property P.
Under which of the following fairness assumptions does the system satisfy the property "eventually a"? Justify your answer.

(a) unconditional fairness for $A = \{\gamma\}$

(b) unconditional fairness for $A_1 = \{\alpha\}$ and for $A_2 = \{\gamma\}$

(c) unconditional fairness for $A = \{\alpha, \gamma\}$

(d) strong fairness for $A = \{\beta\}$

(e) strong fairness for $A_1 = \{\alpha\}$ and for $A_2 = \{\beta\}$

(f) strong fairness for $A_1 = \{\alpha\}$ and for $A_2 = \{\beta\}$ and for $A_3 = \{\eta\}$

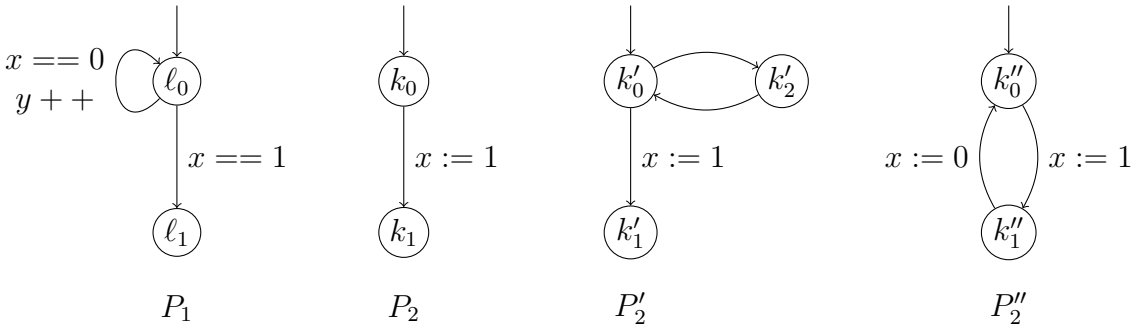
(g) weak fairness for $A = \{\eta\}$

(h) weak fairness for $A_1 = \{\alpha\}$ and for $A_2 = \{\beta\}$ and for $A_3 = \{\eta\}$

Exercise 2: Fairness Assumptions

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 each terminal state 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.

Exercise 3: Logical Implication

The goal of this exercise is to train your understanding of logical implication. This is important to understand strong and weak fairness assumptions which are formulated as implications.

Under which conditions on B and B' is the following implication valid?

$$(A \to B) \to (A \to B')$$