Prof. Dr. Andreas Podelski
Dominik Klumpp
Frank Schüssele

Hand in until February 14th, 2021
23:59 via ILIAS
Discussion: February 17th, 2021

Tutorial for Cyber-Physical Systems - Discrete Models

Exercise Sheet 12

This is a bonus sheet to cover the content of the last two lectures. It will be discussed in a voluntary tutorial on Wednesday, February 17th at 16:00, which will be recorded and uploaded afterwards.

Exercise 1*: LT Properties — 8 Bonus Points

The goal of this task is to learn to identify the different types of LT properties.

Consider the following LT properties with $AP = \{a, b\}$. State for each of the properties which of them are invariants, which are safety properties, which are liveness properties, and which are neither. Justify your answer!

(i) Always (at any point of time) a or b holds.

(ii) Either a holds exactly once, or b never holds.

(iii) If a holds, then b will never hold in the next step.

(iv) Every time a holds there will be eventually a point of time where b holds.

(v) The atomic propositions a and b never hold at the same time.

(vi) If a holds infinitely often, then b holds infinitely often.

(vii) There are only finitely many points of time where a holds.

(viii) True

Exercise 2*: Safety-Liveness Decomposition — 5 Bonus Points

The goal of this exercise is to understand the relation between any LT property and safety and liveness properties, by applying the decomposition theorem.

According to the decomposition theorem, any LT property P can be decomposed into a safety property P_{safe} and a liveness property P_{live}, such that the property P is equal to their intersection, i.e.,

$$P = P_{safe} \cap P_{live} \quad .$$

Apply the construction in the proof of the decomposition theorem to find the decomposition for the following properties with $AP = \{a, b\}$. In particular, for each property, give its closure. Use set notation to express P_{safe} and P_{live}.

(i) Every a is immediately followed by b.

(ii) The atomic proposition a holds infinitely often.

(iii) At exactly 3 points of time, a holds.

(iv) a holds initially and infinitely often.

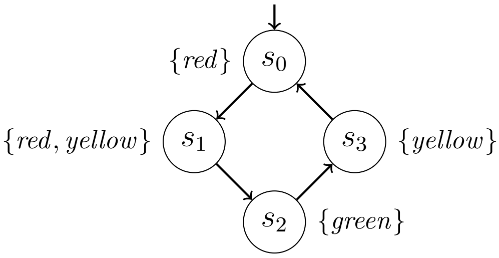
(v) True

Hint: Some tasks may require very little work.

Exercise 3*: Traffic Light 6 Bonus Points

In this exercise, we arrive at the goal towards which we have worked the whole semester: For a cyber-physical system (given as a transition system) and desired correctness properties, we are able to determine if the system satisfies these properties.

The following transition system T models the behaviour of a traffic light.



(a) Consider the following properties:

(P_1) *"It is always the case that if the red light is on, then the green light will be off in the next step."* (Safety)

(P_2) *"The red light is on infinitely often."* (Liveness)

- Draw a NFA $\mathcal{A}_{P_1}$ such that it accepts exactly the bad prefixes of P_1
- Draw a NBA $\mathcal{A}_{P_2}$ that accepts the complement of P_2

Draw the automata in symbolic notation, i.e., with propositional formulas as edge labels.

(b) Draw the product transition systems $T \otimes \mathcal{A}_{P_1}$ and $T \otimes \mathcal{A}_{P_2}$
You do not necessarily need the definition below, you can also try to understand the examples from the lecture.

Definition: Given a transition system $T = (S, Act, \rightarrow, I, AP, L)$ without terminal states and an automaton $A = (Q, 2^{AP}, \delta, Q_0, F)$.
Then we define $T \otimes A := (S \times Q, Act, \rightarrow', I', AP', L')$ with:

- $I' := \{\langle s_0, q\rangle \mid s_0 \in I \wedge \exists q_0 \in Q_0.\ q_0 \xrightarrow{L(s_0)} q\}$
- $AP' := Q$
- $L'(\langle s, q\rangle) := \{q\}$

- $\to'$ is the smallest relation defined by:

$$\frac{s \overset{\alpha}{\to} s' \wedge q \xrightarrow{L(s')} q'}{\langle s, q\rangle \overset{\alpha}{\to}{}' \langle s', q'\rangle}$$

(c) Check whether $T \models P_1$ and $T \models P_2$ hold using invariant checking of $T \otimes \mathcal{A}_{P_1}$ and persistence checking of $T \otimes \mathcal{A}_{P_2}$. If they do not hold, give a counterexample.