Prof. Dr. Andreas Podelski
Dominik Klumpp

Hand in until January 15th, 2020
15:59 via the post boxes
Discussion: January 20th, 2020

Tutorial for Cyber-Physical Systems - Discrete Models

Exercise Sheet 11

Exercise 1: Safety-Liveness Decomposition — 6 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.,

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

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 $(\{A_0 A_1 A_2 \ldots \mid \forall k \exists j \ldots\})$ 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.

Hint: Some tasks may require very little work.

Exercise 2: Good and Bad Prefixes — 6 Points

Assume that $\Sigma = 2^{AP}$ for a given set of atomic propositions. For each of the following pairs of sets (of finite words), determine whether the equality always holds. Consider the inclusions in both directions separately. If an inclusion holds, argue why this is the case. If it does not hold, give an example of a property E and a trace that demonstrates that the inclusion does not hold.

(a) $\mathit{pref}(E) \stackrel{?}{=} \Sigma^* \setminus \mathit{BadPref}_E$

(b) $\mathit{pref}(\Sigma^\omega \setminus E) \stackrel{?}{=} \Sigma^* \setminus \mathit{pref}(E)$

(c) $\mathit{BadPref}_E \stackrel{?}{=} \mathit{pref}(\Sigma^\omega \setminus E)$

Exercise 3: Safety and Liveness — 5 Points

The goal of this exercise is to understand why safety and liveness are not mutually exclusive, and to see how edge cases are often the key to mathematical theorems.

Assume a set of atomic propositions $AP = \{a, b\}$, and assume that $\Sigma = 2^{AP}$. Perhaps contrary to intuition, there exist LT properties over AP that are both a safety and a liveness property. In the lecture, two candidates for such a property were discussed: $P_1 = \Sigma^\omega$ (or *"true"*) and $P_2 = \emptyset$ (or *"false"*). We will analyse these candidates here.

(a) Show that P_1 is a safety property, by giving the set of bad prefixes $BadPref_{P_1}$.

(b) Show that P_1 is a liveness property, by showing how an arbitrary prefix $A_0 A_1 \ldots A_n$ can be continued to an infinite trace $A_0 A_1 A_2 \ldots \in P_1$.

(c) Let E be an LT property that is both a safety property and a liveness property. Show that $E = P_1$.

Hint: The alternative characterizations of safety and liveness property using the prefix closure cl might be helpful.

(d) Is P_2 a safety property? If so, give the set of bad prefixes $BadPref_{P_2}$. If not, argue why this is the case.

(e) Is P_2 a liveness property? If so, show how to continue an arbitrary prefix $A_0 A_1 \ldots A_n$ to an infinite trace $A_0 A_1 A_2 \ldots \in P_2$. If not, give a bad prefix and argue why it cannot be continued.