Prof. Dr. Andreas Podelski
Dominik Klumpp
Elisabeth Henkel

Hand in until December 14th, 2022
23:59 via ILIAS
Discussion: December 19th/20th, 2022

Tutorial for Cyber-Physical Systems - Discrete Models
Exercise Sheet 8

Exercise 1: Prefixes and Closure I 4 Points

The goal of this task is to get a better understanding of the relation between the set of finite prefixes of a property and the closure (which is defined using the prefixes).

Let P be any LT property. Prove the following claims:

(a) $P \subseteq cl(P)$

(b) $pref(cl(P)) = pref(P)$

(c) $cl(cl(P)) = cl(P)$

Note: You can use claim (a) in the proof of claim (b), and you can use claims (a) and (b) in the proof of claim (c).

Exercise 2: Prefixes and Closure II 6 Points

The goal of this task is to get a better understanding of prefixes and closures by applying them to given properties.

Consider following properties over the set $AP = \{a, b\}$ of atomic propositions.

(P_1) a holds exactly once.

(P_2) Whenever a holds, b holds in the next step.

(P_3) a holds only finitely many times.

(P_4) a holds initially and infinitely often.

For each property P_i complete the following tasks:

(a) Formalize P_i as a set of traces using set comprehension.

(b) Give the set of prefixes using set comprehension, i.e. $pref(P_i)$.

(c) Provide its closure using set comprehension, i.e. $cl(P_i)$.

Exercise 3: Safety & Liveness Properties 12 Points

The goal of this task is to learn how to recognize invariants, safety and liveness properties, and to learn how one can show that a property belongs to one of these three classes.

Consider following properties over the set $AP = \{a, b\}$ of atomic propositions.

- $P_1 = \{A_0A_1A_2 \ldots \mid \neg\exists i.\ a \in A_i\}$
  (a never holds)
- $P_2 = \{A_0A_1A_2 \ldots \mid \forall i.\ (a \in A_i \to \exists j.\ (i \leq j \wedge b \in A_j))\}$
  (every a should eventually be followed by b)
- $P_3 = \{A_0A_1A_2 \ldots \mid \forall i.\ (b \in A_i \to a \in A_i)\}$
  (every time b holds, a also holds)
- $P_4 = \{A_0A_1A_2 \ldots \mid \forall i.\ (b \in A_i \to \forall j.\ (i \neq j \to b \notin A_j))\}$
  (b holds at most once)

For each property P_i complete the following tasks:

(a) Determine if P_i is an invariant. In that case, provide the invariant condition. Otherwise give a set of atomic propositions A and two traces σ_1, σ_2 such that σ_1 satisfies P_i, σ_2 does not satisfy P_i, and A appears in both traces.

Example: The property *"in the first step, a holds"* is not an invariant. We can choose $\sigma_1 = \{a\}^\omega$ and $\sigma_2 = \emptyset\,\{a\}^\omega$, both of which contain the set $A = \{a\}$.

(b) Determine if P_i is a safety property. In that case, give the set of all bad prefixes. Otherwise give a counterexample, i.e. a trace $\sigma \in (2^{AP})^\omega \setminus P_i$ such that σ does not have a bad prefix.

Example: The property *"always a"* is a safety property, and its bad prefixes are

$$BadPref_{\text{always } a} = \{A_0A_1 \ldots A_n \mid \exists i \in \{0, \ldots, n\}\,.\, a \notin A_i\}$$

(c) Determine if P_i is a liveness property. In that case, show how any prefix $A_0A_1 \ldots A_n$ can be extended to an infinite trace that satisfies P_i. Otherwise give one bad prefix of the property.

Example: The property *"a holds infinitely often"* is a liveness property, and any finite trace prefix $A_0A_1 \ldots A_n$ can be extended to an infinite trace σ that satisfies the property by setting $\sigma = A_0A_1 \ldots A_n\ \{a\}^\omega$.