Prof. Dr. Andreas Podelski
Dominik Klumpp
Frank Schüssele

Hand in until December 15th, 2021
23:59 via ILIAS
Discussion: December 20th/21st, 2021

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 (a) in the proof of (b), and you can use (a) and (b) in the proof of (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 Properties 6 Points

The goal of this task is to learn how to recognize safety properties and invariants.

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

- $P_1 = \{A_0 A_1 A_2 \ldots \mid \neg\exists i.\ a \in A_i\}$
  (a never holds)

- $P_2 = \{A_0A_1A_2\ldots \mid \forall i.\ (a \in A_i \rightarrow \exists j.\ (i \leq j \wedge b \in A_j))\}$
  (every a should eventually be followed by b)
- $P_3 = \{A_0A_1A_2\ldots \mid \forall i.\ (b \in A_i \rightarrow a \in A_i)\}$
  (every time b holds, a also holds)
- $P_4 = \{A_0A_1A_2\ldots \mid \forall i.\ (b \in A_i \rightarrow \forall j.\ (i \neq j \rightarrow b \notin A_j))\}$
  (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.

(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.
For example, the bad prefixes of "always a" can be given as

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