Prof. Dr. Andreas Podelski
Elisabeth Henkel
Dominik Klumpp

Hand in until December 13th, 2023
15:59 via ILIAS
Discussion: December 18th/19th, 2023

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.

In the lecture, you have seen how to determine whether or not properties are safety or liveness properties, and how to show that a property is an invariant. To show that an LT property is not an invariant, we use the following proposition. (Proving this proposition will be a task on one of the upcoming exercise sheets.)

Proposition: *Let $E \subseteq (2^{AP})^\omega$ be an LT property. E is not an invariant if and only if there exists a trace $\sigma = A_0 A_1 \ldots$ such that $\sigma \notin E$, but for every $i \in \mathbb{N}$, the set A_i also occurs in some trace $\pi_i \in E$.*

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

- $P_1 = \{A_0 A_1 A_2 \ldots \mid \neg\exists i \in \mathbb{N}.\ a \in A_i\}$
  (a never holds)
- $P_2 = \{A_0 A_1 A_2 \ldots \mid \forall i \in \mathbb{N}.\ (a \in A_i \rightarrow \exists j \in \mathbb{N}.\ (i \leq j \wedge b \in A_j))\}$
  (every a should eventually be followed by b)
- $P_3 = \{A_0 A_1 A_2 \ldots \mid \forall i \in \mathbb{N}.\ (b \in A_i \rightarrow a \in A_i)\}$
  (every time b holds, a also holds)
- $P_4 = \{A_0 A_1 A_2 \ldots \mid \forall i \in \mathbb{N}.\ (b \in A_i \rightarrow \forall j \in \mathbb{N}.\ (i \neq j \rightarrow b \notin A_j))\}$
  (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. Otherwise give a trace $\sigma = A_0 A_1 \ldots$ such that $\sigma \notin P_i$, but for every $i \in \mathbb{N}$, the set A_i also occurs in some trace $\pi_i \in P_i$.

Example: The property *"in the first step, a holds"* is not an invariant.

We choose $\sigma = (\{\}\{b\})^\omega \notin P_{\text{initially a}}$. The set $\{\}$ also occurs in the trace $\{a\}\{\}^\omega \in P_{\text{initially a}}$, and similarly $\{b\}$ also occurs in $\{a\}\{b\}^\omega \in P_{\text{initially a}}$.

(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

$$BadPref_{\text{always a}} = \{A_0 A_1 \ldots A_n \mid \exists i \in \{0, \ldots, n\}\,.\, a \notin A_i\}$$

(c) Determine if P_i is a liveness property. In that case, show how any prefix $A_0 A_1 \ldots A_n$ 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 $A_0 A_1 \ldots A_n$ can be extended to an infinite trace σ that satisfies the property by setting $\sigma = A_0 A_1 \ldots A_n\ \{a\}^\omega$.