Prof. Dr. Andreas Podelski
Tanja Schindler

Hand in until January 16, 2019
15:59 via the post boxes
Discussion: January 21/22, 2019

Tutorial for Cyber-Physical Systems - Discrete Models
Exercise Sheet 10

The goal of this sheet is to become familiar with safety properties and with the concepts that are important for safety properties, i.e., with prefixes and the closure.

Exercise 1: LT Properties for a Program

The goal of this task is to learn how to recognize safety properties in the context of a program (for atomic propositions that are defined for a given program).

Let the set AP of atomic propositions be given by $AP = \{x = 0, x > 1\}$.
Consider a nonterminating sequential program P that manipulates the variable x.
Formalize the following properties as LT properties, using set notation,
i.e., $\{A_0 A_1 A_2 \ldots \mid \langle \textit{condition on indices } i, \textit{ or } i \textit{ and } j, \textit{ etc.} \rangle\}$.

(a) false

(b) initially x is equal to 0

(c) initially x differs from 0

(d) intially x is equal to 0, but at some point x exceeds 1

(e) x exceeds 1 only finitely many times

(f) x exceeds 1 infinitely often

(g) the value of x alternates between 0 and 2

(h) true

Determine which of the properties are safety properties. Justify your answers.

Exercise 2: Traces and Closure

The goal of this task is understand the concepts of safety and closure by manipulating the corresponding definitions.

Let TS be a transition system. Show that the set $\mathit{closure}(\mathit{Traces}(TS))$ is a safety property.
As an asidee, $TS \models \mathit{closure}(\mathit{Traces}(TS))$. There is a simple reason why this holds, namely?

Exercise 3: Prefixes and Closure of a Property

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 an LT property. Prove the following claim:

$$\mathit{pref}(\mathit{closure}(P)) = \mathit{pref}(P)$$

Exercise 4: Safety Properties

The goal of this task is to learn how to recognize safety properties (for atomic propositions that are left abstract).

Consider the set $AP = \{a, b\}$ of atomic propositions. Formulize the following properties as LT properties. Determine which of the properties is an invariant, a safety property, or neither.

(a) a should never occur

(b) a should occur exactly once

(c) a and b alternate infinitely often

(d) a should eventually be followed by b.

Exercise 5: Real Numbers as Traces, Closure for Sets of Real Numbers

The goal of this task is to understand the notion of a safety property as a closed set (i.e., a set that is equal to its closure), via an analogy to closed intervals.

We define real numbers as a variant of decimal numbers, namely decimal numbers with infinitely many digits after the comma (possibly 0). A decimal number is one with finitely many digits after the comma (possibly 0). In other words, a real number is an infinite sequence of digits (and one occurrence of a comma), and a decimal number is a finite sequence of digits (and at most one occurrence of a comma). In this view, a (finite) prefix of a real number is thus a decimal number.

Let S be a set of real numbers. Define

$$\mathit{closure}_1(S) = \{x \mid \text{for every } n \text{ there exists } y \in S \text{ such that } |x - y| < (1/10)^n\}$$

and

$$\mathit{closure}_2(S) = \{x \mid \text{every prefix of } x \text{ is the prefix of some element } y \in S\} \ .$$

Thus, in the notation of the lecture, $\mathit{closure}_2(S) = \{x \mid \mathit{pref}(x) \subseteq \mathit{pref}(S)\}$.

We also define

$$\mathit{closure}_3(S) = \{x \mid \text{for every } n \text{ there exists } y \in S \text{ such that distance}(x, y) < 1/n\}$$

where distance$(x, y) = 1/n$ where n is the first position where the digits of x and y differ.

Show that the closure of the open interval $(0, 1) = \{x \mid 0 < x < 1\}$ is the closed interval $[0, 1] = \{x \mid 0 \leq x \leq 1\}$ for all three notions of closure.