Prof. Dr. Andreas Podelski
Dr. Matthias Heizmann
Christian Schilling

Preference deadline: July 17, 2017
Discussion: July 19, 2017

Tutorial for Program Verification
Exercise Sheet 11

Exercise 1: Regular traces 1 Point

Consider the program whose set of control flow traces is given by the following regular expression.

$$\boxed{\texttt{assume(x is prime))}}\ (\boxed{\texttt{x--}})^*\ \boxed{\texttt{assume(x = 0)}}$$

(a) Consider the pre-/postcondition pair $(true, true)$.

  (i) Is the set of correct control flow traces a regular language?

  (ii) Is the set of feasible correct control flow traces a regular language?

  (iii) Is the set of infeasible correct control flow traces a regular language?

(b) Consider the pre-/postcondition pair $(true, false)$. Answer the same questions as above.

Exercise 2: Transitive closure 1 Point

Let R be a binary relation over a set Σ. Consider the following two relations.

- Let R_{tcl1} be the smallest set such that the following properties hold.
  (a) $R \subseteq R_{tcl1}$ and
  (b) for all $s, s', s'' \in \Sigma$ if $(s, s') \in R_{tcl1}$ and $(s', s'') \in R_{tcl1}$ then $(s, s'') \in R_{tcl1}$
- Let R_{tcl2} be the smallest set such that the following properties hold.
  (a) $R \subseteq R_{tcl2}$ and
  (b) for all $s, s', s'' \in \Sigma$ if $(s, s') \in R_{tcl2}$ and $(s', s'') \in R$ then $(s, s'') \in R_{tcl2}$

Prove that the equality $R_{tcl1} = R_{tcl2}$ holds.

Exercise 3: Transitive closure, abstract version 1 Point

We consider the same setting as in Exercise 2.

(a) Lift the definitions of R_{tcl1} and R_{tcl2} to an abstract domain (call the new relations $R^{\#}_{tcl1}$ and $R^{\#}_{tcl2}$, respectively).

(b) Does $R^{\#}_{tcl1} = R^{\#}_{tcl2}$ still hold?

Exercise 4: Transition invariants 1 Point

Consider the program $P = (\Sigma, \mathcal{T}, \rho)$, where

- $\Sigma = \mathbb{Z} \times \mathbb{Z}$,
- $\mathcal{T} = \{\tau_1, \tau_2, \tau_3, \tau_4\}$,
- $\rho_{\tau_1} \equiv x \geq 0 \wedge y \geq 0 \wedge y \leq x \wedge y' = y - 1$,
- $\rho_{\tau_2} \equiv x \geq 0 \wedge y \geq 0 \wedge y \leq x \wedge x' = y - 1$,
- $\rho_{\tau_3} \equiv x \geq 0 \wedge y \geq 0 \wedge x < y \wedge y' = x - 1$, and
- $\rho_{\tau_4} \equiv x \geq 0 \wedge y \geq 0 \wedge x < y \wedge x' = x - 1$.

(a) Find a ranking function f for the program P. Prove that f is a ranking function.

(b) Use transition predicate abstraction to prove that the program is terminating.

- Find a suitable set of transition predicates *Preds*.
- Compute the corresponding set of abstract transitions $P^{\#} = \{T_1, \ldots, T_n\}$.
- Argue that each abstract transition T_i is well-founded.

(c) Find a disjunctive well-founded transition invariant $T_1 \cup T_2$ such that

- T_1 and T_2 are well-founded relations and
- both T_1 and T_2 are formulas that contain only primed and unprimed variables, logical connectives, and (function/relation/constant) symbols from the set $\{>, +, -, 1, 0\}$.