Prof. Dr. Andreas Podelski
Matthias Heizmann

11.1.2012
Submission: 17.1.2012
at the beginning of the lecture

Tutorials for Program Verification
Exercise sheet 10

In the lecture we mentioned two different ways to define the transitive closure of a binary relation. In the following exercise you prove that both definitions are equivalent.

Exercise 1: Transitive Closure 3 bonus points

Let R be a binary relation over a set Σ.
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_{rcl2} be the smallest set such that the following properties hold.

(a) $R \subseteq R_{rcl2}$ and

(b) for all $s, s', s'' \in \Sigma$ if $(s, s') \in R_{rcl2}$ and $(s', s'') \in R$ then $(s, s'') \in R_{rcl2}$

Prove that the equality $R_{tcl1} = R_{rcl2}$ holds.

Exercise 2: Transition Invariants 2+2+1 bonus points

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

- $\Sigma = \mathbb{Z} \times \mathbb{Z}$,
- $\mathcal{T} = \{\tau_1, \tau_2, \tau_3, \tau_4\}$,
- ρ_{τ_1} is $x \geq 0 \wedge y \geq 0 \wedge y \leq x \wedge y' = y - 1$,
- ρ_{τ_2} is $x \geq 0 \wedge y \geq 0 \wedge y \leq x \wedge x' = y - 1$,
- ρ_{τ_3} is $x \geq 0 \wedge y \geq 0 \wedge x < y \wedge y' = x - 1$,
- and ρ_{τ_4} is $x \geq 0 \wedge y \geq 0 \wedge x < y \wedge x' = x - 1$.

(a) State a ranking function for the program P.

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

- State a set of transition predicates $\mathcal{P}$ such that the set of abstract transitions $P^{\#}$ contains only well-founded realations.

- Compute the set of abstract transitions $P^{\#} = \{T_1, \ldots, T_n\}$.
- Illustrate that each abstract transition T_i is well founded (no detailed proof necessary).

(c) State a disjunctively well-founded transition invariant $T_1 \cup T_2$ that

- is the union of two well-founded relations
- and both, T_1 and T_2 are formulas that contain only variables, logical connectives and symbols of the set $\{>, +, -, 1, 0\}$.