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

WITH SOLUTIONS

Exercise 1: Regular traces — 1 Point

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?

Solution

(a) The only change (underlined) is that the relations are defined over an abstract domain of transition predicates.

- Let $R^{\#}_{tcl1}$ be the smallest set <u>in $D^{\#}$</u> such that the following properties hold.
  (i) $\underline{\alpha}(R) \subseteq R^{\#}_{tcl1}$ and
  (ii) for all $s, s', s'' \in \Sigma$ if $(s, s') \in R^{\#}_{tcl1}$ and $(s', s'') \in R^{\#}_{tcl1}$ then $\underline{\alpha}((s, s'')) \in R^{\#}_{tcl1}$
- Let $R^{\#}_{tcl2}$ be the smallest set <u>in $D^{\#}$</u> such that the following properties hold.
  (i) $\underline{\alpha}(R) \subseteq R^{\#}_{tcl2}$ and
  (ii) for all $s, s', s'' \in \Sigma$ if $(s, s') \in R^{\#}_{tcl2}$ and $(s', s'') \in R$ then $\underline{\alpha}((s, s'')) \in R^{\#}_{tcl2}$

In least fixed point/abstract interpretation notation we could write:

$$R^{\#}_{tcl1} = \mu X \in D^{\#}.\ X \sqsupseteq \alpha(R) \sqcup \alpha(X \circ^{\#} X)$$
$$R^{\#}_{tcl2} = \mu Y \in D^{\#}.\ Y \sqsupseteq \alpha(R) \sqcup \alpha(R \circ \gamma(Y))$$

(The abstract operators and γ are not important in our setting because our abstraction is in the same domain (sets of transitions).)

(b) In general equality does not hold. The following counterexample may be easier to understand by writing pairs of states instead of formulas.

Let $R := \{\rho\}$ with $\rho :\equiv x = 1 \wedge x' = 1$. The predicates are:

$$\mathit{Preds} := \{(x = 1 \wedge x' = 1) \vee (x = 1 \wedge x' = 2) \vee (x = 2 \wedge x' = 1), x = 2 \wedge x' = 2\}.$$

First we compute $\alpha(R) \equiv \{(x = 1 \wedge x' = 1) \vee (x = 1 \wedge x' = 2) \vee (x = 2 \wedge x' = 1)\}$.

We execute the first step for the fixed point equations and get

$$\alpha(R) \cup \alpha(\alpha(R) \circ \alpha(R)) \equiv \alpha(R) \cup \{x = 2 \wedge x' = 2\}$$
$$\alpha(R) \cup \alpha(R \circ \alpha(R)) \equiv \alpha(R).$$

Thus we reached a fixed point in the second case while in the first case we have at least one additional element. Hence $R^{\#}_{tcl1} \supseteq \alpha(R) \cup \{x = 2 \wedge x' = 2\} \supsetneq \alpha(R) \equiv R^{\#}_{tcl2}$.