Prof. Dr. Andreas Podelski
Matthias Heizmann

14.12.2011
Submission: 20.12.2011
at the beginning of the lecture

Tutorials for Program Verification
Exercise sheet 8

Exercise 1: Relational Composition 1 points

Give the formula that denotes the relational composition $\rho_1 \circ \rho_2$ of the two relations denoted by the formulas ρ_1 and ρ_2, formulas in the variables $V \cup V'$, where V' contains the primed versions of the variables in V.

Exercise 2: Properties of $post^\#$ 3 points

Give a counterexample for those of the following propositions which are wrong.

(a) $post^\#(\phi, \rho_1 \circ \rho_2) \subseteq post^\#(post^\#(\phi, \rho_1), \rho_2)$

(b) $post^\#(\phi, \rho_1 \circ \rho_2) \supseteq post^\#(post^\#(\phi, \rho_1), \rho_2)$

(c) $post^\#(\phi, \rho_1 \vee \rho_2) \subseteq post^\#(\phi, \rho_1) \vee post^\#(\phi, \rho_2)$

(d) $post^\#(\phi, \rho_1 \vee \rho_2) \supseteq post^\#(\phi, \rho_1) \vee post^\#(\phi, \rho_2)$

(e) $post^\#(\phi_1 \vee \phi_2, \rho) \subseteq post^\#(\phi_1, \rho_1) \vee post^\#(\phi_2, \rho)$

(f) $post^\#(\phi_1 \vee \phi_2, \rho) \supseteq post^\#(\phi_1, \rho_1) \vee post^\#(\phi_2, \rho)$

Exercise 3: Execution of AbstReach Informally and Formally 11 points

Consider the following program.

```
   int x, y, z, w;
   void foo()
   {
1:     do {
2:         z = 0;
3:         x = y;
4:         if (w == 17){
5:             x++;
6:             z = 1;
           }
7:     } while(x!=y)
8:     assert (z != 1);
   }
```

(a) Informal! Is the program safe? Give an informal argument.

(b) Informal! Give three predicates (in addition to the predicates on the program counter) such that the corresponding abstraction is suffient to prove safety. Give the corresponding abstract reachability graph (in an informal presentation where the edges are labeled by line numbers).

(c) Informal! Give the abstract reachability graph that corresponds to the abstraction for the set of predicates $Pred_0$ which contains only the predicates on the program counter. Take the shortest counterexample path. Add one predicate p_1 to eliminate this first counterexample.

(d) Informal! Give the abstract reachability graph that corresponds to the abstraction for the set of predicates $Pred_1 := Pred_0 \cup \{p_1\}$. Take again the shortest counterexample path. Add two predicates, p_2 and p_3, to eliminate this counterexample. (Did you get the three predicates from (b)?)

(e) Translate the program into the formal presentation based on logical formulas.

(f) Give the sequence of relations which is the formal presentation of the counterexample from (c).

(g) Apply the algorithm FeasiblePath. It is sufficient to give (some simplified version of) the formula called φ in the slides (i.e., don't prove the inconsistency of φ and don't give intermediate formulas).

(h) Apply AbstractReach for $Pred_1$.

(i) Give the sequence of relations which is the formal presentation of the counterexample from (d).

(j) Apply the algorithm FeasiblePath. It is sufficient to give (some simplified version of) the formula called φ in the slides (i.e., don't prove the inconsistency of φ and don't give intermediate formulas).

(k) Apply AbstractReach for $Pred_2 := Pred_2 \cup \{p_2, p_3\}$.