Prof. Dr. Andreas Podelski
Christian Schilling

Tutorial for Cyber-Physical Systems - Hybrid Models
Exercise Sheet 6

Exercise 1: Relational composition
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 in the variables $V \cup V'$, where V' contains the primed versions of the variables in V.

Exercise 2: Properties of $post^\#$
Give a counterexample for those of the following propositions which are wrong.

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

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

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

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

(e) $post^\#(\varphi_1 \vee \varphi_2, \rho) \subseteq post^\#(\varphi_1, \rho) \vee post^\#(\varphi_2, \rho)$

(f) $post^\#(\varphi_1 \vee \varphi_2, \rho) \supseteq post^\#(\varphi_1, \rho) \vee post^\#(\varphi_2, \rho)$

Exercise 3: Predicate abstraction
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) Is the program safe? Give an informal argument.

(b) Give three predicates (in addition to the predicates on the program counter) such that the corresponding predicate abstraction is sufficient to prove safety.

(c) Give the abstract reachability graph corresponding to your chosen predicates (in an informal presentation where the edges are labeled by line numbers). An example of an *abstract reachability graph* is given in Fig. 3 in "Predicate Abstraction for Program Verification". It is defined in the same line as the region transition system for timed automata.