Software-Modellierung und Verifikation
Informatik 2
Prof. J.-P. Katoen
RWTH Aachen

Priv.-Doz. T. Noll noll@cs.rwth-aachen.de
J. Heinen heinen@cs.rwth-aachen.de
Ch. Jansen christina.jansen@cs.rwth-aachen.de

10. Exercise sheet *Static Program Analysis 2011*

Due Mon, 11. July 2011, *before* the exercise course begins.

Exercise 10.1: **(3 points)**

Consider the following predicates q_1 and q_2. Calculate $q_1 \sqcup q_2$ and $q_1 \sqcap q_2$.

(a) $q_1 := \neg p_1 \wedge \neg p_2 \wedge \neg p_3$, $q_2 := p_1 \wedge \neg p_3$

(b) $q_1 := \neg p_1 \wedge \neg p_2$, $q_2 := p_1 \wedge p_2$

(c) $q_1 := \neg p_3$, $q_2 := p_1 \wedge \neg p_3$

Exercise 10.2: **(1+1+2+4+3 points)**

Consider the following program fragment c calculating the factorial of x.

```
$[a := x]^1$;
$[y := 1]^2$;
while $[\neg(a == 1)]^3$ do $[y := y \cdot a]^4; [a := a - 1]^5$;
if $([1 \leq x \wedge x \leq 2]^6)]^2$ then if $([y == x]^7)$ then $[\textsf{skip}]^8$ else $[\textsf{skip}]^9$ else $[\textsf{skip}]^{10}$;
```

We want to show, that label 9 is not reachable.

(a) Give the abstract transition system of c for the set of predicates $P = \emptyset$.

(b) Provide a spurious counterexample for your initial abstraction from (a).

(c) Compute the strongest postconditions P' for your counterexample from (b).

(d) Execute one abstraction refinement step with the help of your counterexample from (b).

(e) Is this refinement step sufficing to show that label 9 is not reachable? If not, why? Is the desired property provable using predicate abstraction as considered in the lecture?

Exercise 10.3: **(3 points)**

Consider the following variation of the (if1) execution relation for predicate abstraction:

$$(\text{if1})\ \frac{\exists \sigma : \sigma \models b \wedge q}{< \textsf{if } b \textsf{ then } c_1 \textsf{ else } c_2, q > \rightarrow < c_1, \overline{q \wedge b} >}$$

Does this (if1) executation relation provide an optimisation of predicate abstraction as considered in the lecture? If, provide an example derivation where this execution relation exhibits less nondeterminism than the one presented in the lecture. If not, show why!