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

Priv.-Doz. T. Noll noll@cs.rwth-aachen.de
C. Jansen christina.jansen@cs.rwth-aachen.de

7. Exercise sheet *Semantics and Verification of Software SoSe2010*

Due to Monday, 7th June 2010, *before* the exercise course begins.

Exercise 7.1: **(2 points)**

Prove by structural induction on expressions $a \in \mathbf{LExp}$ and $n \in \mathbb{N}$ that

$$\mathfrak{L}[\![a]\!]I[i \to n]\sigma = \mathfrak{L}[\![a[i \to n]]\!]I\sigma.$$

Exercise 7.2: **(1+2 points)**

Let $c \in \mathbf{Cmd}$ be given by

$$z := 0; \textsf{while } y \leq x \textsf{ do } (z := z + 1; x := x - y).$$

(a) Give a partial correctness property for c which formalizes the following observation: if the execution of c is started in a state $\sigma \in \Sigma$ with $\sigma(x) \geq 0$ und $\sigma(y) > 0$, and if it terminates in a state $\sigma' \in \Sigma$, then $\sigma'(z) = \sigma(x)$ **div** $\sigma(y)$ and $\sigma'(x) = \sigma(x)$ **mod** $\sigma(y)$.

(b) Establish the validity of this correctness property using the proof system from the lecture.

Exercise 7.3: **(0.5+2.5 points)**

We extend the set of boolean assertions $Assn$ by a further rule $A ::= \exists i.A \in Assn$.

(a) Give semantics for the new assertion by expressing it by means of already given assertions or extend the axiomatic functional accordingly.

(b) Using your semantics from a), show that the following proposition holds:

$$\sigma \models^I \exists i.A \Leftrightarrow \sigma \models^I A[i \to z] \text{ for some } z \in \mathbb{Z}$$

Exercise 7.4: **(1+2 points)**

Provide postconditions for these code fragments and show their partial correctness.

(a)
```
{m ≥ 0}
  x := 0; odd := 1; sum := 1;
  while sum ≤ m do {
    x := x + 1; odd := odd + 2; sum := sum + odd; }
{Postcondition}
```

(b)
```
{m > 0, n ≥ 0}
  a := m; b := n; k := 1;
  while b > 0 do {
    if b = 2 · (b/2) then {
      a := a · a; b := b/2; }
    else { b := b − 1; k := k · a; } }
{Postcondition}
```