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

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

Due to Monday, 28th June 2010, *before* the exercise course begins.

Exercise 9.1: **(3 points)**

To conclude the section about axiomatic semantics, answer the following questions.

(a) What is the idea of axiomatic semantics? Which conclusions about program behaviour can be drawn using them?

(b) Describe the concept of assertions and partial correctness properties.

(c) What do you know about soundness and compleneness of axiomatic semantics?

(d) Briefly sketch the steps needed to prove total correctness of a program fragment. Which statements about termination of a program fragment can be proven by means of partial correctness properties?

Exercise 9.2: **(2+2 points)**

Prove that the following program terminates for each of the termination expressions:

(a) $E_1 = \langle m, n \rangle$ with the lexicographic ordering on $\mathbb{N} \times \mathbb{N}$

(b) $E_2 = 2m + n$ with the „greater than“ordering on $\mathbb{N}$

$\{a \geq 0 \wedge b \geq 0 \wedge (a \neq 0 \vee b \neq 0)\}$
$m := a; n := b$
while $m > 0$ do
  if $m \leq n$ then $n := n - m$
  else $x := m; m := n; n := x;$
  end if
end while
$\{n$ is greatest common divisor of a and $b\}$

Reminder (showing termination):

- Find a set W with a strict well-founded ordering $>$.
- Find a termination expression E with the following properties:
  - Whenever control passes through the beginning of the iterative loop, the value of E is in W.
  - E takes a smaller value with respect to $>$ each time the top of the iterative loop is passed.

Exercise 9.3: **(2 points)**

Assume we allow the usage of recursive function calls in our extended while language from Ex. 8.4. For these functions termination cannot be handled by total correctness rules. But if a suitable property can be identified on which an induction proof is possible, termination of recursive procedures can be shown inductively.

Consider the following procedure, which counts the digits in a number m.

```
procedure count is{
 begin
    if m < 10 then
       ans := 1;
    else
       count(m/10);
       ans := ans + 1;
    end if
 end
```

Give an induction proof for the following lemma stating that the procedure terminates for any nonnegative integer m.

Lemma 1 *If $m > 0$, the procedure count halts.*

Exercise 9.4: **(2 points)**

Consider the axiomatic equivalence of two statements defined in 14.3 in the lecture. Based on this definition show that the following proposition holds:

Proposition 1 $c_1 \approx c_2 \Leftrightarrow \forall A, B \in Assn.(\models \{A\}\, c_1\, \{\Downarrow B\} \Leftrightarrow \models \{A\}\, c_2\, \{\Downarrow B\})$.