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

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

Due to Monday, 12th July 2010, *before* the exercise course begins.

Exercise 11.1: **(2+3 points)**

Consider the following program c, which iteratively counts the digits in a natural number $z \in \mathbb{N}$.

```
w := 1; s := 10;
while (z + 1 > s) do
    w := w + 1;
    s := s * 10;
end while
```

(a) Translate the following program into abstract machine code by using the translation function given in lecture 16.

(b) Provide a computation of a run on the abstract machine for the input value $z = 10$ by means of the transition relation given in definition 16.2 of the lecture.

Exercise 11.2: **(1+1 points)**

Extend the WHILE language of the lecture with the construct **repeat** c **until** b and specify the corresponding translation function.

When modeling the **repeat** c **until** b via the similar construct c; **while** $\neg b$ **do** c; containing a while-loop in a straightforward way, the body c will be translated twice. Can you think of a way to avoid this double translation of c?

Exercise 11.3: **(4 points)**

Provide the second/missing proof step for theorem 17.4 of the lecture, i.e. show that the following lemma holds:

Lemma 1 (17.6) *For every $c \in Cmd$, $\sigma, \sigma' \in \Sigma$ and $e \in Stk$, $\langle \mathfrak{T}_c[\![c]\!], \epsilon, \sigma\rangle \rhd^* \langle \epsilon, e, \sigma'\rangle$ implies $\langle c, \sigma\rangle \to \sigma'$ and $e = \epsilon$.*

You may use all theorems and lemmata presented in the lecture (except from theorem 17.4 and lemma 17.6 of course). Additionally you may find the following lemma useful.

Lemma 2 (Decomposition Lemma) *If $\langle d_1 : d_2, e, s\rangle \rhd^k \langle \epsilon, e'', \sigma''\rangle$, then there exists a configuration $\langle \epsilon, e', \sigma'\rangle$ and natural numbers k_1, k_2 with $k_1 + k_2 = k$ such that $\langle d_1, e, \sigma\rangle \rhd^{k_1} \langle \epsilon, e', \sigma'\rangle$ and $\langle d_2, e', \sigma'\rangle \rhd^{k_2} \langle \epsilon, e'', \sigma''\rangle$.*