Technische Universität München
Fakultät für Informatik
Dr. Peter Lammich
Simon Wimmer

WS 2018/19
05. 02. 2019

Semantics of Programming Languages

Exercise Sheet 15

Exercise 15.1 Program Verification

(Pen & Paper)
The following exercises are typical exam problems. You are supposed to solve them on a sheet of paper, without using Isabelle/HOL.

We want to analyze a program that checks whether an array's content (viewed as a word) is of the form $0^n 1^n$ for some $n \geq 0$. The following is the *IMP2* implementation of the program:

```
i = 0;
j = h - 1;
while (i < j && a[i] == 0 && a[j] == 1)
{
  i=i+1;
  j=j-1
}
```

The parameter h specifies the number of elements in array a. We assume $h \geq 0$ initially.
Questions:

1. Propose a suitable post-condition that states correctness of the program.
2. Give a valid loop invariant that is strong enough to prove the above specification.
3. Give a valid variant for the loop to prove termination.
4. What does the verification condition at the end of the loop look like? (It is of the form $I \wedge \neg\ b \longrightarrow Q$, where I is your invariant, b is the loop condition, and Q is your post-condition.)
5. Prove the verification condition $I \wedge \neg\ b \longrightarrow Q$ informally.

Hint: You may use the notation $a[i{:}j]$ as a shorthand for *lran a i j*.

Exercise 15.2 Hoare-Logic

(Pen & Paper)
The following exercises are typical exam problems. You are supposed to solve them on a sheet of paper, without using Isabelle/HOL.

We replace the assignment in IMP by a command *REL R* that performs an arbitrary state transition according to relation $R :: (state \times\ state)\ set$.
In the big-step semantics, we remove the *assign*-rule, and add the following rule:

Rel: $(s,s') \in R \implies (REL\ R,s) \Rightarrow s'$

1. Is the semantics deterministic, i.e., does the following hold (proof or counterexample):

   $(c,s) \Rightarrow t \implies (c,s) \Rightarrow t' \implies t{=}t'$

2. What does the weakest precondition $wp\ (REL\ R)\ Q$ look like?
3. Prove soundness and completeness of $wp\ (REL\ R)\ Q$

Hints

- Question 2: Recall the definition of the weakest precondition:

  $wp\ c\ Q\ =\ (\lambda s.\ \forall t.\ (c,s) \Rightarrow t \longrightarrow Q\ t)$