J. Hoenicke
A. Nutz

11.05.2017
Please hand in your solution until
18.05.2017, via email to
nutz@informatik.uni-freiburg.de.

Tutorials for "Formal methods for Java"
Exercise sheet 3

Exercise 1: Specification in JML

Consider the following Java method:

```
static int f(int n) {
  int s = 0;
  int i = 0;

  while (i++ < n) {
    s = s + 2 * i - 1;
  }

  return s;
}
```

Write some code that calls the method `f` and prints its results conveniently. Write a precise specification with pre- and postcondition for method `f`. Assume as precondition that `n` is non-negative.

Exercise 2: Operational semantics of loops

By induction over k show the following statement for all $k \geq 0$:

$$\forall heap. \forall lcl.\, lcl(i)^2 = lcl(s) \wedge lcl(n) - lcl(i) = k \implies$$

$$(Norm, heap, lcl) \xrightarrow{\texttt{while (i++<n) \{s=s+2*i-1;\}}} (Norm, heap, lcl \oplus \{i \mapsto lcl(n) + 1, s \mapsto lcl(n)^2\})$$

For simplicity you may ignore that in the operational semantics all arithmetic operations are done modulo 2^{32}.

Exercise 3: Proving correctness

Using the result of exercise 2, give a proof that method `f` fulfills the specification you gave in exercise 1, i.e., show for all $(Norm, heap, lcl)$ that if $lcl(n)$ fulfills the precondition, and $(Norm, heap, lcl) \xrightarrow{body} (Ret, heap', lcl')$, where *body* is the body of `f`, then lcl'(`\result`) and $lcl(n)$ fulfill the postcondition (as specified in lecture 5).
You can use the statement in exercise 2, even if you did not manage to prove it.