



J. Hoenicke
J. Christ

29.01.2013

Hand in solutions via email to
`christj@informatik.uni-freiburg.de`
until 05.01.2013 (only Java sources, KeY
proofs, and PDFs accepted).
Paper submissions possible after the lecture.

Tutorials for “Formal methods for Java” Exercise sheet 12

Exercise 1: Dynamic Logic

For each of the following dynamic logic formulae find an equivalent formula without modalities.

- (a) $\langle \mathbf{while}(x \neq 0)\{x = x - 1;\} \rangle \mathbf{false}$
- (b) $[\mathbf{while}(x \neq 0)\{x = x - 1;\}] \mathbf{false}$
- (c) $\langle \mathbf{while}(x \neq 0)\{x = x - 1;\} \rangle x = 0$
- (d) $[\mathbf{while}(x \neq 0)\{x = x - 1;\}] x = 0$
- (e) $[\mathbf{if}(y = \mathbf{false})\{x = x + 1;\} \mathbf{else}\{x = x - 1;\}] x = 5$
- (f) $[\mathbf{if}(y == 0)\{x = x + 1;\} \mathbf{else}\{x = x - 1;\}] x = 5$

Exercise 2: Integer square roots

Consider the following Java class:

```
class IntSqrt {
    /*@ requires n > 0;
       @ ensures \result * \result <= n
       @      && (\result + 1) * (\result + 1) > n
       @*/
    static int sqrt(int n){
        int result = 0;
        int s = 1;
        while (s <= n) {
            result = result + 1;
            s = s + 2 * result + 1;
        }
        return result;
    }
}
```

Use the KeY prover to prove correctness of method `IntSqrt.sqrt`. Find an invariant/variant proof that proves total correctness. Hand in either the KeY proof file, or a Java source file where the loop is annotated accordingly.

Note that the webstart version contains some GUI bugs when using KeY with Java 7. A working version can be downloaded from http://www.key-project.org/download/releases/key165rc/KeY-1.6.5_cf8990d4ec6fef2d0a49662adb3ec509e023a0c3.tgz. A webstart for this version is available from <http://www.key-project.org/download/releases/key165rc/webstart/KeY.jnlp>.