ALBERT-LUDWIGS-
UNIVERSITÄT FREIBURG

J. Hoenicke
J. Christ

14.12.2011
Hand in solutions via email to
`christj@informatik.uni-freiburg.de`
until 21.12.2011 (only Java sources, KeY proofs, and PDFs accepted).
Paper submissions possible after the lecture.

Tutorials for "Formal methods for Java"
Exercise sheet 8

Exercise 1: Replace Known
Consider the following additional rules from the KeY system:

$$\text{Rule } \textit{replace-known-left}: \quad \frac{\Gamma[\mathit{true}/\phi], \phi \Longrightarrow \Delta[\mathit{true}/\phi]}{\Gamma, \phi \Longrightarrow \Delta}$$

$$\text{Rule } \textit{replace-known-right}: \quad \frac{\Gamma[\mathit{false}/\psi] \Longrightarrow \Delta[\mathit{false}/\psi], \psi}{\Gamma \Longrightarrow \Delta, \psi}$$

Show that the close rule can be simulated by these rules, and the other rules of sequent calculus.

Exercise 2: Insertion Sort
On the webpage of the lecture you find a version of Insertion Sort that is fully annotated. Set the proof search strategy of KeY to

- Goal Chooser: "Default"
- Logical splitting: "Off"
- Loop treatment: "Invariant"
- Method treatment: "Expand"
- Quantifier treatment: "None"

This proof search strategy does not succeed to automatically prove total correctness even though the annotations are sufficient. Instead, this strategy leads to five goals.

(a) Explain the goals, i.e., what is to be proven in each case. Since KeY is deterministic at this part you may enumerate the remaining goals.

(b) Use your knowledge from the previous exercise to prove the remaining goals.

Exercise 3: Bonus: Insertion Sort

In the previous exercise we forced to array to be non-empty by adding the pre-condition `arr.length > 0`. If we remove this pre-condition the proof gets slightly more complicated.

(a) Identify the problems that might occur with empty arrays.

(b) How can we elegantly fix these problems with KeY without modifying the code. Of course, we remove the pre-condition `arr.length > 0`.