Formal Methods for Java

Lecture 18: Key and Procedures

Jochen Hoenicke

Software Engineering
Albert-Ludwigs-University Freiburg

December 23, 2011

KeY and Procedures

In KeY, the default rule is to inline the procedures.
Advantages:

- No function contract needed.
- No separate proof for correctness of function needed.

But it has several disadvantages:

- Proof gets larger (especially important if proof is interactive).
- Proof has to be repeated for every function call.
- No recursive procedures possible.

The rule Use Operation Contract

The rule "Use Operation Contract" allows compositional proofs.
It opens three subgoals:

- Pre: Show that pre-condition holds (this includes class invariants).
- Post: Show that with the post-condition, the remaining program is correct.
- Exceptional Post: Show that if called method throws an exception, the remaining program is correct.

Note: Use Operation Contract cannot be used for the method you are just proving.

Proving recursive functions

Unfortunately, KeY has no direct support for recursive functions.

An induction proof can work. Ingredients:

- A precondition *pre*,
- A postcondition *post*,
- A ranking function *rank*.

Show by induction over r:

```
\forall int x. (pre & rank < r) -> \< result = methodcall(x); \> post
```