Software Component Technology Group

Master Project

Integration of a new VCGen in ESC/Java2

Claudia Brauchli
Supervisor: Hermann Lehner
Prof. Dr. Peter Müller

5. April 2007

Introduction One of MOBIUS project goals is to develop a proof transforming compiler for Java source code to bytecode. In order to do that, we want to create proofs on the source code level which can then be transformed to the bytecode level. The goal of this work is to integrate a new VCGen into ESC/Java2 which produces verification conditions in such a way that the proof transformation is as simple as possible.

Goal of this master's project is to extend the ESC/Java2 tool by providing new lookup functions for JML level 0 annotations. JML level 0 defines a subset of JML specifications including pre-, postconditions, class invariants, and local annotations. These lookup functions yield first order logic representations of local assertions for given program points as well as method level specifications for given methods. Parameter for these lookup functions are pointers into the Java-AST. Using a visitor pattern, the functions can extract the desired information from the Java-AST. The functions will cover at least JML level 0.

The main parts of this project are:

1. Define the transformation of JML level 0 to first order logic
2. Implement four lookup functions to get information about the pre-, post-, and exceptional postconditions of a method and about the local assertions inside a method
3. Design and implement Java + JML subset checker, which can be turned on and off by command line switches
4. Design and implement static analysis that checks which objects can be changed within a method (for invariant checking)
5. Support history constraints

Possible extensions are:

- Verifying some simple example programs in Coq
- Support ownership structure to check invariants