ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Semester Project

Generating Proof Obligations from JML Specifications

The Software Component Technology Group (SCT) and the Softwaretechnik group at TU Kaiserslautern work on the development of Jive, which is an interactive program prover that allows programmers to prove that their Java Card implementation behaves as specified.
Instead of formulating the behavior of methods in a natural language (e.g. "*if you give me a non-zero integer, I will compute its inverse*"), the programmer uses a formal specification language, which is far more accurate and, in particular, machine-checkable.

A previous version of Jive supported specifications written directly in first-order logic. This solution left the gap between the specification language and the underlying logic of Jive relatively small. On the other hand, writing specifications in first-order logic is not intuitive for programmers, unless they invest time and effort to learn the required mathematical background.

Currently there is an ongoing project to change the specification language of Jive to JML (Java Modeling Language) which allows one to specify programs via pre- and postconditions of methods and type invariants using a Java-like syntax. This enables Java-programmers to learn the specification language significantly faster.

This switch to JML increases though the gap between the specification language and the underlying logic of Jive. A great part of bridging this gap, and the main focus of this Semester Project, is the re-implementation of the Proof Obligation Generator module, which generates Hoare-triples out of JML method specifications and invariants.

Another part of the project is to give the semantics of some JML constructs that have not yet been studied by the SCT group.