Master Project

September 15th 2005 - March 15th 2006

Ronny Zakhejm

Ownership-based Program Verification in Jive

The Jive verification tool does not yet exploit the advantages a program equipped with ownership annotations offers. The goal of this master project is to enable Jive using the information provided by the universe type system, a task consisting of several parts, both conceptual and practical.

The first part is to integrate the latest JML compiler into Jive, which will enable the Jive tool to parse the current JML syntax including full support for the universe type system. Furthermore the JML compiler must be adapted to do admissibility checks for invariants and model fields according to the ownership proof technique.

The ownership information must be represented by means of a mapping from universe types into the program logic of Jive. The goal of this task is to find an appropriate mapping in order to be able to adapt the proof obligation generation mechanism of the tool.

As a second part, the semantics of modifies clauses should be analysed in order to be able to state proof obligations. This analysis considers the implication of the universe type system, as well as the following issues: information hiding, the extended state problem, modularity and correct abstraction.

The merit of these enhancements should be demonstrated by a couple of examples. As an optional part these examples could be extended to bigger case studies.

Depending on how fast progress is made, history constraints, which are often cited but yet neglected features of JML, should be considered as well.

Project supervised by

Prof. Peter Mueller, Adam Darvas
darvasa@inf.ethz.ch
RZ F2 / F3
ETH Zurich