

Semester Project

Welldefinedness and expressiveness of JML specifications

The Software Component Technology Group together with the Softwaretechnik group at TU Kaiserslautern work on the development of Jive, which enables its users to interactively prove the correctness of Java Card programs.

The specification language of Jive is JML (Java Modeling Language) which is specifically tailored to Java, in order to enable programmers to easily learn it. JML extends the side-effect free expression syntax of Java, thus also allows method calls to occur in specifications. Such methods have to be so-called pure, meaning that they cannot have any side-effect on previously allocated objects. The use of pure methods make specifications more compact and expressive, but their translation to logic also introduces difficulties.

Previous work on the formalization of method calls leads to unsoundness in case the specifications of certain pure methods form a cycle, i.e. they refer to each other mutually.

The aim of this project is to look at existing classes specified by JML and find out

- whether such cycles are typical in specifications,
- whether such cycles can be eliminated by rewriting specifications,
- how we can handle cycles in a consistent way if they cannot be eliminated by rewriting.

The project will look at two significantly different type of classes: one from the model library of JML and one from a real application.