Verification of a Java compiler in Isabelle

Martin Strecker
Technische Universität München, Instititut für Informatik
`http://www.in.tum.de/~streckem`

November 23, 2001

In this talk, we will report on our efforts of proving the correctness of a compiler from Java source code to Java bytecode in the Isabelle system. To the best of our knowledge, this is the first fully formal proof of compiler correctness for a realistic object-oriented language.

The compiler, given as a directly executable function, takes expressions of the source language and produces a list of bytecode instructions. The correctness statement has the form of the traditional "commuting diagram" argument: Evaluation of a source program has the same effect as evaluation of the corresponding bytecode. Some additional preconditions require the source program to be well-typed and the program to start in a "well-defined" state.

To make these notions precise, the talk will first survey the formalization of the source and bytecode level, in particular the type system and operational semantics, and sketch the type correctness proof. We will then state the compiler correctness theorem and outline its proof, which proceeds by induction of the evaluation relation and offers few surprizes. Consequently, object-orientation does not enforce a completely new proof style. Even though, it suggests a particular style of semantics definition. The talk will discuss the impact on the preconditions of the compiler correctness theorem and its proof.