Mechanical Program Verification

Juergen F. H. Winkler
Friedrich Schiller University
Jena, Germany

Mechanical program verification (MPV) is the verification of a program relative to a given specification by an algorithm or program, which is called a mechanical program prover (MPP). The basis of MPV are a formal semantics of the specification language and a formal semantics of the programming language, and a calculus for proving mathematical theorems mechanically.

The basic goal of the work presented in the course is the mechanical verification of programs or program fragments of real programming languages intended to be executed by real a computer.

The course gives a short historical overview of program correctness and of approaches to formal semantics of programming languages. One type of formal semantics is the wp-calculus, which leads to an assertion-oriented style of formal specification. The Frege Program Prover (FPP) is a MPP which is based on the wp-calculus and supports a small subset of Ada.

The work on FPP led to the observation that some verification schemes based on the wp-calculus are incomplete and unsafe. But, safety is essential for MPV. Therefore, a new relation-oriented base for the definition of the semantics of programs and specifications will be presented. Based on this semantics safe verification schemata will be proposed.

2006.Jun.09