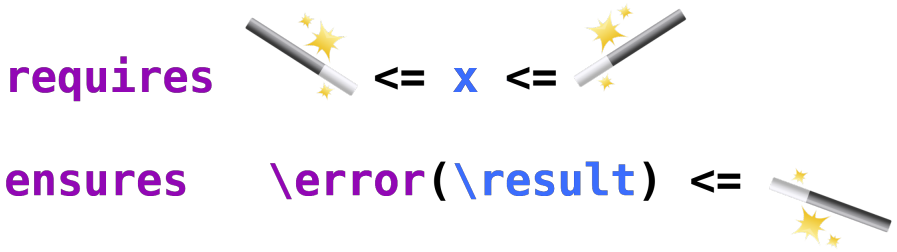
Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Praxis der Forschung

Specification Inference for Floating Point Programs



Background. When computers operate on real numbers, they approximate them using floating point values for which fast computing hardware exists, but which also have a limited precision. The rounding effects that occur may endanger the correctness of computation results in many areas like controllers for critical devices or important scientific computations. The error from repeated rounding effects on floating point values is pretty unpredictable – here formal verification may come to the rescue and provide dependable information on rounding effects.

Problem Description. Analysing a full program for inadvertent rounding effects is often impossible for complexity reasons. One can do what computer scientists usually do: divide and conquer. We break the analysis problem down into several analyses on a function-by-function basis.
Unfortunately, every intermediate function needs a specification then. Writing these specifications can be a lot of work. It would be best if they could be inferred automatically. This is especially true for floating point programs, since the contracts are likely to contain some magic numbers regarding error boundaries.

Goal. The goal of this PdF project is to come up with an inference technique that allows the inference of specifications for Java methods that work on floating point numbers.
This includes the theoretical foundation of this technique and its prototypical realisation in the two verification tools “KeY” and “Daisy”.

Context. This project is in the context of a collaboration on floating point program verification that we have with the Max Planck Institute for Software Systems, Kaiserslautern and Chalmers University of Technology in Gothenburg.

Requirements. Basic understanding of first order logic, program verification as taught, e.g., in the course *Formale Systeme*.

If you are interested, contact Mattias Ulbrich <ulbrich@kit.edu>.