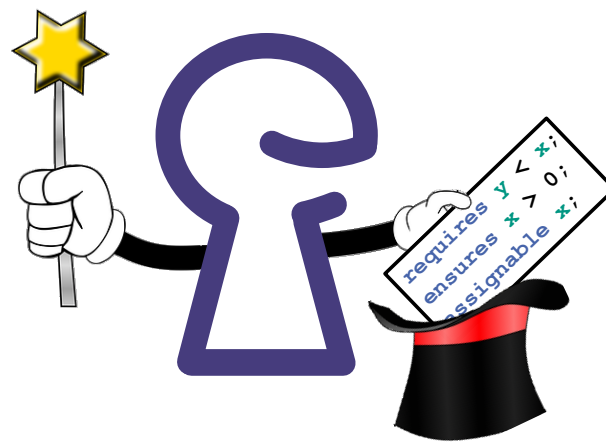Praxis der Forschung

Extracting Specifications for KeY

Background. The KeY verifier is a powerful tool developed in our group with which Java programs can be proved correct. With KeY, one can formally establish that Java method satisfies its formal specifications.

Problem Description. KeY requires that every method is specified with a sufficiently strong specification because it works method-modular. It can be very tedious to specify all internal methods with sufficiently strong contracts. In many (but not in all!) cases, the method contracts are easily obtained from the code or from a given partial specification.
To extend the reach of KeY as a verification tool that can be applied in practice, it is important that a user needs not come up with manually all specifications. Only relevant parts should be specified. The rest can be inferred.

Goals.
The goal of this PdF project is to review existing specification extraction methods and to bring a selection of them into the KeY approach. The resulting experimental extension of KeY should be able to extract simple contracts / contract clauses from a given partial specification and the code.

Kontakt

Mattias Ulbrich   ulbrich@kit.edu   Office: 50.34, R229