

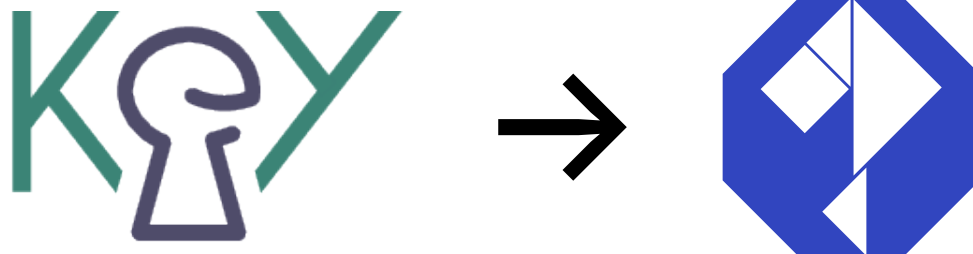
Master's Thesis

Compiling KeY Sequents to Why3

Background.

Deductive program verification deals with formal proofs of program properties. *KeY* (<https://www.key-project.org/>) is a tool for proving the conformity of Java programs to a formal specification. *KeY* translates programs into sequents, whose validity ensures that certain properties hold for a program. Sequents are proved using built-in rules in a sequent calculus or external tools (e.g. the Z3 solver) by translating the sequents into first-order formulas.

The use of a large set of external tools for the verification are convenient, since each solver behaves differently for different problems. Moreover, the more solver succeed, the more we are confident in the result. However, *KeY* currently supports only a small set of external provers. Other deductive verification tools such as *Why3* (<http://why3.lri.fr/>) have a much larger gallery of external solvers and can be used for more general problems.



Your Task.

Your task is to create a bridge between *KeY* and *Why3* to take advantage of *Why3*'s large gallery of external provers. The first step is to analyse *KeY*'s sequents and implement an associated parser. The next step is to implement a compiler from *KeY* sequents to *WhyML* (the language used by *Why3*).

Your profile.

Ideally, you have a basic background in *formal systems* (e.g., from respective lectures of the KIT curricula). Knowledge in functional programming is helpful.

Kontakt

Lionel Blatter

lionel.blatter@kit.edu

Office: 50.34, R227