

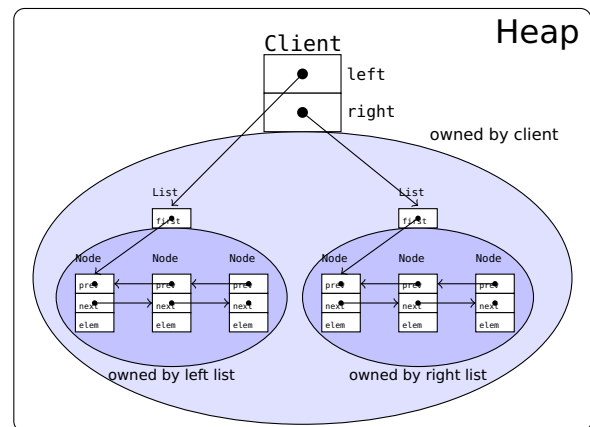
Bachelor's Thesis

Universe Types for KeY

Background: Universe Types.

Ownership type systems are a technique to enforce a hierarchical topology of the objects in programming. In recent years, this technique got a revival driven by the popularity of Rust.

More sophisticated ownership type systems, such as Universe types, can furthermore be used to ensure encapsulation by restricting certain references to only be used for read access.



Background: KeY. KeY is a formal verification tool for Java, using symbolic execution and deductive reasoning in a dynamic logic with sequent calculus rules. KeY can be used for verifying that a Java program adheres to a formal specification written in the Java Modeling Language (JML).

Your Task. The goal is to develop a technique and a workflow to exploit ownership types in the KeY system. The idea is to integrate an existing type checker built with the checker framework.

Theoretical part:

- Adapt calculus rules of KeY

Practical part:

- Make the existing ownership checker usable
- Implement the adapted rules
- Collect and prepare concrete examples

You can build upon existing results from other work at the group.

Your Profile. You should have a background in formal methods (e.g., from relevant KIT lectures).

Contact

Wolfram Pfeifer
Mattias Ulbrich

wolfram.pfeifer@kit.edu
ulbrich@kit.edu

Office: 50.34, R228
Office: 50.34, R227