

Masterarbeit / Praxis der Forschung

Combine Ownership Types and Dynamic Frames for Convenient and Flexible Framing Specifications

Background. Formal program verification is a powerful technology to ensure that a program's effects are as desired. However, formal verification can be quite a challenging endeavour. One of the major challenge is the so called Frame Problem: showing that a program does not affect certain parts of the memory.

Goal. The goal of the work in this thesis is to bring two successful solutions for the frame problem together: Ownership types and Dynamic Frames. The former scales very well while the latter is very general and precise. We want to combine the benefits of both paradigms to obtain a very flexible frame specification technology.

Task. Your task is to integrate the framing technology of Dynamic Frames for JML (as implemented in our verification tool KeY) with an ownership type system defined in the Java Checker Framework.

Your profile. You should be interested in programming languages and in Java in particular. You should have completed the Formal Methods (Formale Systeme) Course at KIT or equivalent.

Kontakt

Dr. Mattias Ulbrich

ulbrich@kit.edu

50.34 R229