

Bachelor Thesis

Erweiterung der Theorie für Finale Felder in KeY

Hintergrund. Deduktive Programmverifikation beschäftigt sich mit dem formalen Nachweis der Korrektheit von Programmen. Was „korrekt“ für ein konkretes Programm bedeutet, wird über eine formale Spezifikation definiert und mit einem logischem Kalkül automatisch oder (in komplizierteren Fällen) benutzergeführt bewiesen.

KeY ist ein interaktiver Theorembeweiser aus unserer Forschungsgruppe, mit dem man die Einhaltung von Java-Programmen gegenüber einer formalen Spezifikation nachweisen kann. Allerdings ist die Anwendung von Theorembeweisern nicht immer einfach. Die Eigenschaften von Programmiersprachen (Java) müssen in der Logik kodiert werden, um sie zu übertragen. Im Fall von KeY werden finale (d.h. unveränderliche) Objektfelder wegen ihrer log. Modellierung nicht optimal behandelt. KeY unterscheidet nämlich nicht zwischen unveränderlichen und veränderlich Speicherstellen. Dies führt dazu, dass die eigentlich konstanten finalen Felder doch veränderlich sind, was die Beweiskomplexität erhöhen kann.



Aufgabe. In dieser Arbeit möchten wir die Behandlung von finalen Felder in KeY verbessern. Finale Felder sind, sobald Sie einmal geschrieben wurden, unveränderlich und können daher in der Modellierung außerhalb des regulären Heapspeichers gespeichert werden. Die Arbeit umfasst dabei die neben der theoretischen Behandlung der neuen Modellierung auch die praktische Umsetzung innerhalb von KeY.

Ihr Profil. Sie sollten solide Programmier-Kenntnisse in Java besitzen und das Modul *Formale Systeme* erfolgreich abgeschlossen haben.

Kontakt

Mattias Ulbrich/Alexander Weigl weigl@kit.edu Office: 50.34, R224