Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
Prof. Dr. Bernhard Beckert

Praxis der Forschung

Inferring JML Contracts for KeY from System Dependence Graphs

Hintergrund. Die beiden am KIT entwickelten Tools JOANA und KeY erlauben die statische Analyse von Java-Programmen. Ziel von JOANA ist es, die Nichtinterferenz-Eigenschaft (d. h. öffentliche Ausgaben werden von geheimen Eingaben nicht beeinflusst) von einem Programm nachzuweisen. Die Analyse von JOANA findet rein syntaktisch mit Hilfe von Systemabhängigkeitsgraphen (SDGs) statt. Das erlaubt vollautomatisierte und schnelle Analysen; Programme mit bis zu 100k Zeilen Code können analysiert werden. KeY wiederum ist ein Theorembeweiser, der zwar allgemeinere Eigenschaften von Programmen verifizieren kann, aber deutlich weniger skaliert als JOANA.

Projektbeschreibung. Das Ziel diese Projekts ist es, die hochskalierbaren SDG-basierten Ansätze, auf denen JOANA beruht, für die Inferenz korrekter Programmeigenschaften zu verwenden. Diese Eigenschaften (z. B. Lese- und Schreibzugriffe einer Methode, Informationsflussverträge, u. a.) sollen in Form von Programmspezifikationen erzeugt werden.

Ihr Profil. Sie sind an formalen Systemen bzw. formalen Sprachen interessiert. Sie können kleinere Softwaresysteme implementieren. Wissen wie beispielsweise in der Vorlesung *Formale Systeme* vermittelt wird vorausgesetzt.

Kontakt
Mihai Herda herda@kit.edu 50.34 R227