Karlsruher Institut für Technologie

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

Inferring JML Contracts for KeY from System Dependence Graphs

Projektgruppe „Praxis der Forschung“
Wintersemester 2017/18

1 Hintergrund

Die beiden am KIT entwickelten Tools JOANA und KeY erlauben die statische Analyse von Java-Programmen. Ziel von JOANA ist es, die *Noninterference*-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 (SDG) statt. Das erlaubt voll automatisierte 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.

2 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.

3 Kontakt / Betreuer

Mihai Herda herda@kit.edu, Raum 227 (Geb. 50.34)