Informatik Kolloquium
Formale Verifikation objekt-orientierter Software

Dr. Bernhard Beckert, U. Koblenz

17. Juni 2004, 14:00 Uhr, Gebäude 57 (Rotunde)

Zusammenfassung

Die Forschung auf dem Gebiet der Formalen Methoden, und insbesondere der deduktiven Programmverifikation, hat in den letzten 5 Jahren erstaunliche Fortschritte gemacht. Die Praxisrelevanz wurde in zahlreichen Fallstudien mit realitätsnahen Aufgabenstellungen nachgewiesen. Bisher unterstützen jedoch Werkzeuge und Methoden zur formalen Software-Verifikation die in der Praxis verwendeten Beschreibungsformalismen (wie UML) und Programmiersprachen (wie Java) nur ungenügend.

In meinem Vortrag gebe ich eine Überblick über das KeY-Projekt, das darauf abzielt, diese Probleme zu überwinden und den Einsatz formaler Methoden im industriellen Kontext zu ermöglichen und zu unterstützen. Der Kerngedanke des KeY-Projektes ist, ein kommerzielles CASE-Werkzeug um Funktionalität für formale Spezifikation und deduktive Verifikation zu erweitern. Dies erlaubt eine schrittweise Integration formaler Methoden in den Software-Entwicklungsprozess unter Beibehaltung der gewohnten Modellierungs- und Programmierumgebung des Benutzers.

Ein wesentlicher Teil des KeY-Projektes ist der Entwurf einer axiomatischen Semantik der Programmiersprache Java Card. Ich beschreibe die dafür verwendete Dynamische Logik, die wesentlichen Ideen und Prinzipien des für diese Logik entwickelten Kalküls und demonstriere, wie mit seiner Hilfe Java-Card-Programme verifiziert werden können.