Informatik-Kolloquium

Rheinisch-Westfälische Technische Hochschule Aachen
Lehrstuhl für Informatik I

EINLADUNG

Zeit: Dienstag, 20. November 2001, 16.00 Uhr

Ort: Raum AH I, Ahornstr.55

Referent: A.o. Univ.-Prof. Dr. Helmut Veith, TU Wien

Thema: Verfahren zur Komplexitätsreduktion im Model Checking

Abstract:

Model Checking ist eine automatische Verifikationsmethode, die sich aus theoretischen Anfängen zu einem wichtigen industriellen Werkzeug zur Analyse von Hardware und zunehmend auch Software entwickelt hat. Der Erfolg der Methode beruht auf der Kombination zahlreicher Techniken zur effizienten Komprimierung und Einschränkung des Zustandsraumes des betrachteten Systems, etwa durch spezielle Datenstrukturen ("symbolische Verifikation") oder durch Reduktion auf einen geeigneten homomorphen Teilraum ("Abstraktion".) Im Falle einer Spezifikationsverletzung können diagnostische Gegenbeispiele erzeugt werden, die der Analyse des fehlerhaften Systemverhaltens durch den Benutzer dienen. Der Vortrag wird nach einer kurzen Einführung in die Grundlagen des Model Checking durch theoretische Resultate und praktische Erfahrungen darlegen, dass traditionelle symbolische Methoden alleine in vielen Fällen nicht ausreichend sind, und durch abstraktions-basierte Methoden ergänzt werden müssen. Diese Resultate motivieren eine vor kurzem entwickelte symbolische Abstraktionsmethode, die im Zentrum des Vortrags steht. In dieser Methode wird eine Folge zunehmend exakterer Approximationen des Zustandsraums durch ein adaptives Verfahren automatisch generiert. Ein Kernpunkt dieses neuen Verfahrens ist die automatische Analyse von diagnostischen Gegenbeispielen auf den approximierten Zustandsräumen. Da die von herkömmlichen Model-Checkern generierten Gegenbeispiele nur ein kleines Fragment von Spezifikationen abdecken, analysieren wir den Begriff des Gegenbeispiels im Model Chekking. Wir definieren eine einfache Klasse endlicher baum-ähnlicher Graphen, und zeigen, dass diese Graphen als Gegenbeispiele für eine grosse Klasse von Spezifikationslogiken geeignet sind. In Verbindung mit symbolischen Algorithmen zur Erzeugung solcher Gegenbeispiele zeigt dies die Vollständigkeit und Effizienz des dargestellen Abstraktionsverfahrens.

Es laden ein: Die Dozenten der Informatik