Reparatur und Generierung formaler Modelle mittels Software Synthese

Joshua Schmidt

Die Erstellung formaler Modelle ist eine langwierige Aufgabe und zumeist nicht trivial. Unter Verwendung von Beweisern und einem geeigneten Model Checker wird ein Modell schrittweise verifiziert und verfeinert.

Der Vortrag befasst sich mit der weitesgehenden Automatisierung des Entwicklungsprozesses formaler Modelle in B und Event-B. In Zusammenarbeit mit Sebastian Krings und Prof. Dr. Michael Leuschel arbeite ich im Rahmen meiner Masterarbeit am Lehrstuhl für Softwaretechnik und Programmiersprachen der Heinrich-Heine-Universität Düsseldorf an diesem Thema.

Die Grundlage bildet ein Software Synthese Verfahren eingeführt von Microsoft Research (Sumit Gulwani et al.), welches anhand von Beispielen in Form von Ein- und Ausgabe in der Lage ist Programme zu generieren die dem beschriebenen Verhalten genügen. Das Verfahren basiert auf der Komposition von Programmkomponenten dargestellt als Formeln. Diese beschreiben jeweils eine Zeile des Programms in Form eines Drei-Adress-Code. Durch verschiedene Constraints werden unter anderem Ein- und Ausgabe von Komponenten verknüpft oder die syntaktische Korrektheit einer Lösung garantiert. Das Verfahren ist interaktiv und fordert gegebenenfalls eine Validierung einzelner Beispiele durch den Benutzer, so dass im besten Fall eine eindeutige Lösung für das gewünschte Verhalten gefunden werden kann.

Zum einen sind wir in der Lage Invariantenverletzungen automatisch zu reparieren. Der Model Checker liefert eine Folge von Zuständen welche letztlich einen Zustand erreicht der eine Invariante verletzt. Die so erhaltenen Transitionen werden nach einer Validierung des Benutzers als Initialisierung für die Synthese verwendet. Dementsprechend kann entweder die Invariante des Modells gelockert oder der Guard einer Operation verstärkt werden. Sollte ein Durchlauf des Model Checkers fehlerfrei sein können wir das Modell interaktiv erweitern. Durch Angabe von positiven und negativen Transitionen können neue Operationen mit bestenfalls bereits passenden Guards synthetisiert werden. Des weiteren ist es möglich durch manuelle Angabe von Zuständen den Guard einer Operation oder die Invariante des Modells zu verändern.

Letztlich bieten all diese Möglichkeiten ein interaktives Werkzeug zur Reparatur und Generierung formaler Modelle.