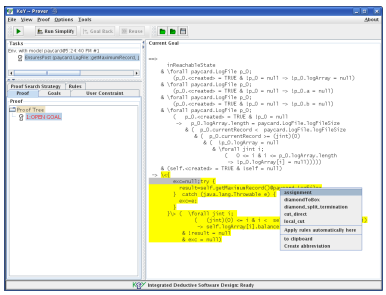
Universität Karlsruhe (TH)
Institut für Theoretische Informatik
Logik und Formale Methoden – Prof. Dr. P. H. Schmitt

Studienarbeit

Wohldefinierte Spezifikationen in KeY



Beschreibung

Moderne Spezifikationssprachen wie die Java Modeling Language (JML) erlauben es, Quellcode mit formalen "Verträgen" zu versehen, die das Verhalten z.B. einer Java-Methode beschreiben. Dabei wird einerseits festgelegt, welche Verpflichtungen ein Aufrufer der Methode vor dem Aufruf zu erfüllen hat, und andererseits, welche Eigenschaften nach der Ausführung der Methode gelten müssen.

Ein solcher Vertrag für eine Methode `divide(a,b)` könnte z.B. aussagen: Wenn die Methode für zwei Zahlen a und b aufgerufen wird, so liefert sie als Ergebnis den Quotienten von a und b. Diese Spezifikation ist aber problematisch, weil b den Wert 0 haben könnte. Ähnliche Probleme ergeben sich z.B. bei Deferenzierungen von `null`-Zeigern. Andererseits sind Ausdrücke wie `o == null || o.attr == 3` für gewöhnlich zulässig, da hier der rechte Teilausdruck nur ausgewertet wird, falls die Referenz `o` von `null` verschieden ist.

Dass ein Programm tatsächlich mit einer Spezifikation übereinstimmt, kann mit Hilfe eines Verifikationssystems nachgewiesen werden, wie z.B. dem am Institut mitentwickelten KeY-System. Es gibt dabei verschiedene Ansätze, mit der potentiellen Undefiniertheit von Spezifikationsausdrücken umzugehen. Einer davon ist es, Beweisverpflichtungen zu erzeugen, die sicherstellen, dass keine undefinierten Ausdrücke zur Auswertung kommen.

Dieser Ansatz soll in der angebotenen Studienarbeit behandelt werden. Die Aufgabe ist, basierend auf verschiedenen existierenden Vorschlägen für die Formulierung einer solchen Beweisverpflichtung eine konkrete Technik zu entwickeln und diese im KeY-System zu implementieren.

Voraussetzungen

Sie sollten über Programmiererfahrung (insbesondere mit Java) verfügen und die Vorlesung "Formale Systeme" erfolgreich besucht haben. Vorkenntnisse über JML oder Verifikation wären von Vorteil, sind aber nicht notwendig, sofern Sie Interesse mitbringen, sich in diese Themen einzuarbeiten.

Kontakt

Mattias Ulbrich: `mulbrich@ira.uka.de`, Geb. 50.34 Raum 106
Benjamin Weiß: `bweiss@ira.uka.de`, Geb. 50.34 Raum 309