Verification of Business Rules Programs

Bruno Berstel – Da Silva

Dissertation
zur Erlangung des Doktorgrades
der Technischen Fakultät
der Albert-Ludwigs-Universität Freiburg

April 2012

Zusammenfassung

Der Beitrag dieser Arbeit ist der (unserem Wissen nach) erste formale Ansatz zur Verifikation von Geschäftsregel-Programmen. Wir schlagen eine Verifikationsmethode vor, um die Korrektheit von Geschäftsregel-Programmen kompositionell zu beweisen. Der Ansatz ermöglicht Autoren von Geschäftsregeln und Entwicklern einer Werkzeugumgebung, Eigenschaften der Ausführung von Geschäftsregel-Programmen zu verstehen, formal zu beschreiben und zu beweisen. Der übergeordnete Beitrag der Arbeit ist, die logischen Grundlagen bereit zu stellen, um Geschäftsregeln überhaupt erst als Gegenstand der wissenschaftlichen Untersuchung in Semantik und Verifikation einführen zu können.

Schichtenarchitekturen benutzten in wachsendem Maße die sogenannten Geschäftsregeln, um die Logikschicht (auch: Businessschicht) zu kodieren. Die Erfassung und die Ausführung von Geschäftsregel-Programmen wird durch ein Geschäftsregel-Managementsystem (GRMS) unterstützt. Ein Geschäftsregel-Programm besteht aus einer Menge von voneinander unabhängigen Regeln, d.h., bedingten Zuweisungsinstruktionen, die in einem modularen, Fall-basierten Ansatz gesammelt werden. Ein Geschäftsregel-Programm ist deklarativ in dem Sinne, dass es nicht den Kontrollfluss spezifiziert; die Regeln werden auf der gegebenen Menge von Objekten ausgeführt, nach und nach für jede Regel und jedes Objekt, in nicht-festgelegter Reihenfolge.

Die wissenschaftliche Forschung hat sich bisher auf die Effizienz der Ausführung von Geschäftsregel-Programmen durch ein GRMS konzentriert. Eine Vielfalt von Kompilierungs- und Ausführungsschemas sind entwickelt worden, so insbesondere der bekannte Rete-Algorithmus. Die Verifikation von Geschäftsregel-Programmen wurde bisher als Gegenstand wissenschaftlicher Forschung vernachlässigt. Der Bedarf an Korrektheit ist jedoch für Geschäftsregel-Programme nicht weniger einleuchtend als für sicherheitskritische Systeme, auch wenn die auf die Spiel stehenden Risiken ökonomisch sind, und üblicherweise nicht lebensbedrohlich.

Die Arbeit besteht aus drei Hauptteilen.

Im ersten Teil präsentieren wir eine *Formalisierung des Ausführungsverhaltens* von Geschäftsregel-Programmen. Bisher exisistierende Beschreibungen hingen inhärent von den Eigenheiten des jeweiligen Kompilierungsschemas ab. Die Aufgabe, das Ausführungsverhalten eines Geschäftsregel-Programms formal und allgemein zu erfassen, wird erschwert durch die schiere Vielfalt der Kompilierungs- und Ausführungsschemas, die in existierenden GRMS benutzt werden. Wer haben ein allgemeines und gleichzeit formal einfaches Rahmenwerk entworfen, das es uns in die Lage versetzt, das Ausführungsverhalten von Geschäftsregel-Programmen zu beschreiben und die Hauptunterschiede zwischen den verschiedenen Ausführungsschemas herauszustellen. Die dank der Formalisierung des Ausführungsverhalten von Geschäftsregel-Programmen mögliche präzise Beobachtungsweise führt zu der Erkenntnis, dass die Einfachheit von Geschäftsregeln nur oberflächig gilt. Tatsächlich kann das Zwischenspiel von Ausführungen von einer oder mehreren Regeln auf einem oder mehreren, möglicherweise geteilten Objekten (die nicht-deterministisch aus einer endlich, aber unbeschränkt großen Menge ausgewählt werden) extrem komplex sein, und dies schon für kleine Beispiele.

Eine Ausführung ist formal eine Folge von Zuständen. Um die Unbeschränkt-

heit der Größe der Objekt-Mengen in den jeweiligen Zuständen berücksichtigen zu können, modellieren wir einen Zustand als eine Struktur der Logik erster Stufe. Wir können der Vielfalt der Ausführungsschemas (die neuen Alternativen zum Rete-Algorithmus eingeschlossen) Rechnung tragen, indem wir Konzepte einführen, die es uns erlauben, zwischen der Anwendbarkeit und der Auswählbarkeit einer Regel zu unterscheiden.

Im zweiten Teil der Arbeit führen wir *Korrektheitsspezifikationen* für Geschäftsregel-Programmen ein. Bisher bestand die einzige Möglichkeit, die Korrektheit eines Geschäftsregel-Programms zu beurteilen, darin, jede Regel des Programms einzeln zu betrachten und ihre Anwendung auf einzelne Objekte im Hinblick auf mögliche Verhaltensmuster zu untersuchen. Es war nicht möglich, den globalen Effekt der Anwendung eines ganzen Geschäftsregel-Programms auf eine Objekt-Menge zu erfassen.

Die Schwierigkeit, formal die Korrektheit von Geschäftsregel-Programmen zu definieren, stammt aus der Diskrepanz zwischen dem lokalen Verhalten während der Ausführung einer Regel-Anwendung und dem globalen Effekt des gesamten Geschäftsregel-Programms. Das lokale Verhalten bezieht sich nur auf das Objekt, auf das die Regel angewandt wird; der globale Effekt bezieht sich auf die gesamte, also endliche aber unbeschränkte Menge von Objekten, auf der das Programm ausgeführt wird.

Wir definieren die Bedeutung eines Hoare-Tripels für ein Programm und globale Zusicherungen als eine konservative Erweiterung der Bedeutung eines Hoare-Tripels für eine einzelne Regel-Anwendung und lokale Zusicherungen. Wir erhalten so Korrektheitsspezifikationen, die dem modularen und dem deklarativen, d.h., Kontroll-unspezifischen Aufbau von Geschäftsregel-Programmen gerecht werden.

Im dritten und letzten Teil der Arbeit führen wir eine *kompositionelle Verifikationsmethode* für Geschäftsregel-Programme ein. Die Schwierigkeit bei der Kompositionalität stammt aus den möglichen Interferenzen zwischen Regel-Anwendungen während der Ausführung eines Programms. Daher kann der Beweis einer Korrektheitseigenschaft für ein Geschäftsregel-Programm nicht einfach der Zerlegung des Programms in seine syntaktischen Bestandteile, also der Regeln, folgen. Geleitet von der Intuition hinter der Owicki-Gries-Methode für parallele Programme, präsentieren wir ein Beweissystem mit einem erweiterten, auf Geschäftsregeln angepassten Begriff der Kompositionalität.

In dem Beweissystem kann ein globales Hoare-Tripel für ein Programm von den lokalen Hoare-Tripeln für dessen einzelne Regeln abgeleitet werden. Wir beweisen, dass das Beweissystem ‘sound’ und relativ vollständig ist (wir benutzen relative Vollständigkeit in dem gleichen Sinn wie bei Hoare-Logik). Wir leiten Beweisregeln für wichtige Klassen von Geschäftsregel-Programmen und von Zusicherungen als Spezialfälle der allgemeinen Beweisregel ab. Wir benutzen verschiedene Beispiele, um die praktische Anwendung der allgemeinen Beweisregel und ihrer Spezialfälle zu veranschaulichen.

In einem nicht-technischen Anhang zu dieser Arbeit demonstrieren wir das praktische Potential unseres Ansatzes im Kontext eines existierenden kommerziellen Geschäftsregel-Managementsystems. Dieses GRMS verfügt über ein leichtgewichtiges Analyse-Modul (unter dem Namen “Rule Static Analysis”). Wir zeigen, dass den verschiedenen Analyse- und Verifikationsfunktionalitäten des GRMS dank des in dieser Arbeit vorgestellten Ansatzes zur formalen Verifikation eine solide Fundierung gegeben werden kann.