Formalizing the logic of event-B
Partial functions, definitional extensions, and automated theorem proving

Author(s):
Schmalz, Matthias

Publication Date:
2012

Permanent Link:
https://doi.org/10.3929/ethz-a-007577749 →

DISS. ETH NO. 20516

Formalizing the Logic of Event-B

Partial Functions, Definitional Extensions, and Automated Theorem Proving

A dissertation submitted to
ETH ZURICH
for the degree of
Doctor of Sciences

presented by

Matthias Schmalz
Diplom der Informatik, Universität zu Lübeck
born on October 5, 1981
citizen of Germany

accepted on the recommendation of

Prof. Dr. David Basin
Prof. Dr. Cliff Jones
Prof. Dr. Peter Müller
Prof. Dr. Tobias Nipkow

2012

Abstract

The basic motivation behind this thesis is to develop methods and tools for building highly reliable computerized systems. The work builds on the formal method *Event-B*, the corresponding development environment *Rodin*, and the theorem prover *Isabelle/HOL*. Event-B provides a methodology for developing models of complex systems. A major strength of Event-B is its carefully designed refinement calculus, which helps to break big problems down to manageable pieces. A major weakness of Event-B and Rodin is that the underlying logic is poorly understood; this has led to unsound proofs and impedes enhancements of the logic. Another problem is that it is difficult to improve the performance of Rodin's theorem prover on domains to which it has not been applied before. Isabelle/HOL is a theorem prover with strong theoretical foundations and powerful facilities to adapt its proof methods to new domains. Like Rodin, Isabelle/HOL can be used to develop models of systems, but it offers less user guidance and lacks several useful features of Rodin. The contribution of this thesis is to develop a comprehensive theoretical foundation of Event-B's logic and to bring Rodin together with Isabelle/HOL, creating a tool that has the advantages of both worlds.

The specification of Event-B's logic covers abstract syntax, semantics, proofs, and methods for definitional theory extensions. Since Event-B's logic closely resembles higher-order logic, I define its semantics by an embedding into higher-order logic with the benefit that several meta-results on higher-order logic can be straightforwardly transferred to Event-B. Event-B explicitly supports partial functions; as is often the case for logics of partial functions, some design decisions are difficult to make and to explain. I therefore carefully analyze the impact of the non-trivial design decisions underlying Event-B's logic; my analysis provides useful information for planning future changes of Event-B and for developing other logics of partial functions. By integrating Isabelle/HOL as a theorem prover into Rodin, Rodin obtains a proof tactic that improves over existing tactics in terms of soundness, adaptability to new domains, and sometimes even performance.

Although this research has been driven by the aim to improve Event-B and Rodin, it has led to results of a more general interest. One of them is *directed rewriting*, a term rewriting technique for logics of partial functions that has been implemented in several theorem provers, but lacks a widely known theoretical justification. I show under which conditions directed rewriting is safe and sound, and I demonstrate that directed rewriting significantly reduces the need for solving preconditions of rewrite rules during proofs.

Another result of general interest concerns the embedding of logics of partial functions into classical logics. Such embeddings typically suffer an exponential blowup, if connectives and quantifiers are interpreted in Kleene semantics. I propose an embedding that applies to a broader class of logics of partial functions than existing embeddings. With my parametric complexity analysis and empirical evaluation I refute the plausible and widely accepted belief that the exponential overhead of such embeddings is unacceptably high for practical applications.

Zusammenfassung

Gegenstand dieser Dissertation sind Methoden zur Entwicklung qualitativ hochwertiger computerbasierter Systeme. Ausgangspunkte sind die formale Methode *Event-B*, die zugehörige Entwicklungsumgebung *Rodin* und der generische Theorembeweiser *Isabelle* instanziiert mit Logik höherer Stufe (Isabelle/HOL). Event-B ermöglicht es, verschiedenste Arten von komplexen Systemen auf intuitive Art und Weise zu modellieren und deren Korrektheit zu beweisen. Der Erfolg von Event-B wird jedoch dadurch relativiert, dass sich mithilfe verschiedener Versionen von Rodin die Korrektheit fehlerhafter Systeme beweisen lässt. Grund dafür waren Programmierfehler in Rodins Theorembeweiser, die häufig auf ein mangelhaftes Verständnis der zugrunde liegenden Logik zurückzuführen sind. Dieses mangelhafte Verständnis der Logik behindert auch die Weiterentwicklung von Event-B. Eine weitere Schwäche von Rodins Theorembeweiser besteht darin, dass seine Suchstrategien sich nur mit sehr grossem Aufwand verändern lassen. Der Theorembeweiser Isabelle/HOL zeichnet sich dagegen dadurch aus, dass Fehler in Beweisen äusserst unwahrscheinlich sind und sich dessen Beweisstrategien mit geringem Aufwand für spezifische Anwendungsfälle optimieren lassen. Isabelle/HOL kann zwar grundsätzlich auch zum Modellieren von Systemen verwendet werden, ist in dieser Hinsicht jedoch deutlich weniger intuitiv zu bedienen als Rodin. Der erste Beitrag dieser Dissertation ist eine systematische Beschreibung der Logik von Event-B, die gängigen wissenschaftlichen Qualitätskriterien genügt. Der zweite Beitrag besteht in der Integration von Isabelle/HOL in Rodin, so dass eine Entwicklungsumgebung entsteht, die die Vorteile von Event-B und Isabelle/HOL vereint.

Die Beschreibung der Logik von Event-B beinhaltet deren Syntax, Semantik, Beweiskalküle sowie Methoden zur Erweiterung von Theorien mithilfe von Definitionen. Da die Logik von Event-B viele Ähnlichkeiten mit Logik höherer Stufe hat, definiere ich deren Semantik mithilfe einer Einbettung in Logik höherer Stufe. Dies hat den Vorteil, dass verschiedenste Erkenntnisse über Logik höherer Stufe sich einfach auf Event-B übertragen lassen. Die Logik von Event-B bietet verschiedene Mechanismen, die die Modellierung von partiellen Funktionen erleichtern, den Aufbau der Logik selbst jedoch verkomplizieren. Ich analysiere, wie diese Mechanismen zusammenwirken; dies erleichtert es, die Auswirkungen von zukünftigen Veränderungen der Logik vorherzusagen. Durch die Anbindung von Isabelle/HOL erhält Rodin eine Beweisstrategie, die bestehenden Beweisstrategien in Bezug auf Korrektheit, Anpassbarkeit und manchmal auch Performanz überlegen ist.

Auch wenn das primäre Ziel dieses Forschungsprojekts die Verbesserung von Event-B und Rodin ist, haben manche der behandelten Beweistechniken Anwendungen ausserhalb von Event-B. Eine dieser Techniken ist *Directed Rewriting*, eine Termersetzungsstrategie für Logiken mit partiellen Funktionen. Obwohl diese Strategie bereits in mehreren Theorembeweisern implementiert wurde, gab es bislang keine allgemein bekannte Erklärung für deren Korrektheit. Ich erkläre, unter welchen

Bedingungen directed Rewriting korrekt ist, und ich zeige empirisch, dass directed Rewriting Termersetzungsbeweise in praktisch relevanten Szenarien erheblich vereinfacht.

Ein weiteres Ergebnis mit Anwendungen ausserhalb von Event-B betrifft die Einbettung von Logiken mit partiellen Funktionen in klassische Logiken. Dieses Problem ist insbesondere dann schwierig, wenn boolesche Junktoren und Quantoren gemäss Kleene Semantik interpretiert werden. Ich definiere eine Einbettungen, die eine grössere Klasse von Logiken mit partiellen Funktionen abdeckt als bereits bekannte Einbettungen. Weiterhin untersuche ich die Effizienz meiner Einbettung sowohl mit einer parametrischen Komplexitätsanalyse als auch mithilfe von Experimenten; mit meiner Analyse widerlege ich die weitverbreitete Annahme, dass Einbettungen von Kleene Logiken in klassische Logiken für praktische Anwendungen zu ineffizient sind.