DISS. ETH NO. 17671

Proofs for the Working Engineer

A dissertation submitted to

ETH ZURICH

for the degree of

Doctor of Sciences

presented by

Farhad Dinshaw Mehta

Master of Science, Technische Universität München
Bachelor of Technology, Indian Institute of Technology Delhi

born 11.01.1980
citizen of India

accepted on the recommendation of

Prof. Jean-Raymond Abrial
Prof. Peter Müller
Prof. Cliff Jones

2008

Abstract

Over the last couple of decades the advantages of including formal proof within the development process for computer based systems has become increasingly clear. This has lead to a plethora of logics and proof tools that propose to fulfill this need. Nevertheless, the inclusion of theorem proving within the development process, even in domains where clear benefits can be expected, is rather an exception than the rule.

One of the main goals of the formal methods endeavour is to bring the activity of formal theorem proving closer to the engineer developing computer based systems. This thesis makes some important practical contributions towards realising this goal. It hopes to shows that proper tool support can not only ease theorem proving, but also strenghten its role as a design aid. It shows that it is feasible to integrate interactive proof within a reactive development environment for formal systems. It shows that it is possible to design a proof tool whose reasoning capabilities can be easily extended using external theorem provers. It proposes a representation for the proofs constructed using such an extensible proof tool, such that these proofs can be incrementally reused, refactored, and revalidated. On the more theoretical side, but with major practical implications, it shows how one can formally reason about partial functions without abandoning the well understood domain of classical two-valued predicate calculus.

The ideas presented here have been used to design and implement the proof infrastructure for the RODIN platform which is an open, extensible, industry-strength formal development environment for safety critical systems. Nevertheless, the contributions made in this thesis stand on their own and are independent of the tool implementing them. This thesis is therefore not a description of a working proof tool, but the resulting tool is a proof of the feasibility of the ideas presented in this thesis.

Zusammenfassung

Das Ziel dieser Arbeit ist, dem Entwickler computergestützte formale Beweise näherzubringen. In den letzten Jahrzehnten ist mehr und mehr klar geworden, dass es vorteilhaft ist, formale Beweise in den Entwicklungsprozess von computerbasierten Systemen miteinzubeziehen. Dadurch ist eine Vielzahl von Logiken und Beweiswerkzeugen entstanden, die versprechen, diesen Ansatz in die Tat umzusetzen. Trotzdem ist es eher die Ausnahme als die Regel, dass formale Beweise in den Entwicklungsprozess miteinbezogen werden, selbst in Bereichen, in denen deutliche Gewinne erzielt werden können.

Wir beginnen, indem wir versuchen, Gründe für die langsame Akzeptanz des formalen Beweisens bei Entwicklern zu finden. Wir zeigen auf, dass praktische Anwendungen spezielle, aber überschaubare Anforderungen an Beweiswerkzeuge stellen. Damit computergestütztes Beweisen industriell genutzt werden kann, müssen diese Anforderungen untersucht werden. Dies hat Konsequenzen für das Design von Beweiswerkzeugen.

Wir zeigen in dieser Arbeit, dass computergestütztes Beweisen als ein ingineurswissenschaftliches Werkzeug verwendet werden kann, so dass Beweise ein praktikabler Teil des Endproduktes werden. Wir erklären darüber hinaus, wie Beweise die Entwicklung von computerbasierten Systemen unterstützen.

Die hier vorgestellten Ideen sind verwendet worden, um die Beweisinfrastruktur der RODIN Plattform zu entwickeln. Die RODIN Plattform ist eine freie, erweiterbare, praxisnahe Entwicklungsumgebung für sicherheitskritische Systeme. Dennoch sind die Beiträge dieser Arbeit unabhängig von dem Werkzeug, in dem sie umgesetzt wurden. Diese Arbeit ist daher keine Beschreibung eines Beweiswerkzeugs, jedoch ist das Werkzeug ein Beweis für die Umsetzbarkeit der Ideen aus dieser Arbeit.