J Autom Reasoning (2016) 56:201–203
DOI 10.1007/s10817-016-9363-7

Interactive Theorem Proving

Preface of the Special Issue

Gerwin Klein[1,2] · Ruben Gamboa[3]

Received: 3 February 2016 / Accepted: 4 February 2016 / Published online: 20 February 2016

Abstract This special issue collects current efforts towards the construction of formal proofs with the use of interactive theorem provers, which combine formal proof-checking and proof-finding tools with human guidance.

Keywords Formal verification · Interactive theorem proving · Formal logic

Computing is perhaps the only feasible way to construct non-trivial, completely formal mathematical proofs, formal in the sense that proof proceeds nearly step-by-step in a logical system with clear axioms and rules of inference. Most proofs do not benefit from this level of formal rigor, but some do, either for aesthetic reasons such as "Proofs from the Book," or because the theorems are of practical importance, e.g., in security settings or for hardware verification. Such proofs can be difficult, sometimes tedious, and beyond the state of the art in completely automated theorem proving, so the proofs require close interaction between human and computer.

This special issue collects current efforts in this approach to formal proof. It consists of extended submissions selected from ITP 2014, the 5th International Conference on Interactive Theorem Proving held during 13–16 July 2014 in Vienna, as part of the Federated Logic Conference (FLoC, July 10–24, 2014), which in turn was part of the Vienna Summer of Logic (July 9–24, 2014).

ITP 2014 was the 5th conference on Interactive Theorem Proving and related areas, ranging from theoretical foundations to implementation aspects and applications in program verification, security, and formalization of mathematics. The inaugural meeting of ITP was held during 11–14 July 2010 in Edinburgh, Scotland, as part of the Federated Logic Conference

✉ Ruben Gamboa
ruben@uwyo.edu

[1] NICTA, Sydney, Australia

[2] University of New South Wales, Sydney, Australia

[3] University of Wyoming, Laramie, WY, USA

(FLoC, 9–21 July 2010). ITP is the evolution of the TPHOLs conference series to the broad field of interactive theorem proving. TPHOLs meetings took place every year from 1988 until 2009.

There were 59 submissions to ITP 2014. The Committee decided to accept 35 papers, 4 of which were rough diamonds. Of these 35 papers, 7 extended submissions were accepted for publication in this special issue of the Journal of Automated Reasoning. The papers appearing here are substantially extended from those presented at ITP and were reviewed to full journal standards. They span topics from the formal verification of interactive theorem prover implementations, over program analysis and application verification, to mathematics, logic, and improvements to interactive theorem systems themselves.

The paper by Arthan, "On Definitions of Constants and Types in HOL," introduces a new definitional principle for HOL, which generalizes the previous mechanisms for defining constants in various implementations of HOL. Importantly from a logical perspective, the paper shows that this principle is conservative, so it can be used to introduce hidden constants in the context of structured proofs. The new mechanism has already been implemented in major systems.

The paper by Kumar, Arthan, Myreen, and Owens, "Self-Formalisation of Higher-Order Logic," describes a formalized semantics for the HOL logic, including a definitional principle. This verifies the inference mechanisms of HOL, and also certifies an implementation of a theorem prover for HOL.

The paper by Matichuk, Murray, and Wenzel, "Eisbach: A Proof Method Language for Isabelle," describes a novel language for describing proof methods. This allows users interacting with the system Isabelle to suggest proofs in a higher-level than is afforded by Isar, the most popular interface to Isabelle. This aims to re-use the definition of similar proof methods, making it easier to scale proofs in Isabelle.

The paper by Blazy, Laporte, and Picardie, "Verified Abstract Interpretation Techniques for Disassembling Low-level Self-modifying Code," extends the techniques of static analysis of binary code to support code that modifies itself dynamically. This presents a major challenge, because static analysis works on control-flow graphs that can be built from the static structure of code, but which may not be valid with code that modifies itself. The paper describes how abstract interpretation can be used to bridge this gap automatically, and how this process has been verified in the Coq proof assistant.

The paper by Bourke, van Glabbeek, and Höfner, "Mechanizing a Process Algebra for Network Protocols," describes an approach to modeling Mobile Ad hoc Networks and Wireless Mesh Networks in Isabelle/HOL using process algebra. A key innovation presented in this paper is the use of terms in the process algebra to describe the state of a single node in the network, and an approach to lifting global invariants expressed at the level of individual nodes to a network of nodes.

The paper by Doczkal and Smolka, "Completeness and Decidability Results for CTL in Constructive Type Theory," presents a formal proof in Coq/Ssreflect of the small-model property of CTL and the completeness of a Hilbert-style system for CTL. The proof is constructive, so the verification introduces an inductive semantics for CTL which agrees (constructively) with the traditional path semantics of CTL on finite models.

The paper by Avigad, Lewis, and Roux, "A heuristic prover for real inequalities," develops a new approach to proving inequalities, in particular inequalities that are likely to appear in interactive theorem proving. The general approach is to make use of canonical normal forms to describe terms, and to use specialized modules which communicate indirectly through a common blackboard.

As editors, we are very proud of the contributions to this special issue. We thank all the authors for their contributions and efforts, as well as the anonymous reviewers for their thoughtful and thorough comments.

December 2015,
Gerwin Klein and Ruben Gamboa