Lecture Notes in Computer Science 10499

More information about this series at http://www.springer.com/series/7407

Mauricio Ayala-Rincón · César A. Muñoz (Eds.)

Interactive Theorem Proving

8th International Conference, ITP 2017
Brasília, Brazil, September 26–29, 2017
Proceedings

Springer

Editors
Mauricio Ayala-Rincón
University of Brasília
Brasília D.F.
Brazil

César A. Muñoz
NASA
Hampton, VA
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-66106-3 ISBN 978-3-319-66107-0 (eBook)
DOI 10.1007/978-3-319-66107-0

Library of Congress Control Number: 2017949523

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the proceedings of the 8th Conference on Interactive Theorem Proving (ITP 2017) held in Brasília, Brazil, on September 26–29, 2017. The conference was organized by the departments of Computer Science and Mathematics of the Universidade de Brasília.

The ITP conference series is concerned with all topics related to interactive theorem proving, ranging from theoretical foundations to applications in program verification, security, and formalization of mathematics. ITP succeeded TPHOLs, which took place every year from 1988 until 2009. Since 2010, ITP has been held in Edinburgh (2010), Nijmegen (2011), Princeton (2012), Rennes (2013), Vienna (2014), Nanjing (2015), and Nancy (2016).

ITP 2017 was part of the Brasília Spring on Automated Reasoning and was co-located with the 26th International Conference on Automated Reasoning with Analytic Tableaux and Related Methods (Tableaux 2017) and the 11th International Symposium on Frontiers of Combining Systems (FroCoS 2017). In addition to the three main conferences, four workshops took place: 12th Logical and Semantic Frameworks with Applications (LSFA 2017), 5th Workshop for Proof eXchange for Theorem Proving (PxTP 2017), EPS - Encyclopedia of Proof Systems, and DaLí - Dynamic Logic: New Trends and Applications. The Brasília Spring on Automated Reasoning also included four tutorials: Proof Compressions and the Conjecture NP = PSPACE, General Methods in Proof Theory for Modal and Substructural Logics, From Proof Systems to Complexity Bounds, and PVS for Computer Scientists.

There were 65 submissions. Each submission was reviewed by at least 3 members of the Program Committee. The reviews were written by the 36 committee members and 69 external reviewers. An electronic PC meeting was held using the EasyChair system. The PC decided to accept 28 regular submissions and 2 rough diamond contributions. The program also included 3 invited talks by Moa Johansson on Automated Theory Exploration for Interactive Theorem Proving: An Introduction to the Hipster System, Cezary Kaliszyk on Automating Formalization by Statistical and Semantic Parsing of Mathematics, and Leonardo de Moura on Whitebox Automation. Cezary Kaliszyk, Katalin Bimbó, and Jasmin Blanchette presented joint TABLEAUX/FroCoS/ITP invited talks.

We would like to thank the PC members for their work, especially during the paper selection process, all the reviewers for writing high-quality reviews, the invited speakers for accepting our invitation and delivering insightful talks, and the authors who submitted their contributions to ITP 2017. Many people helped to make ITP 2017 a success. In particular, we are very grateful to Cláudia Nalon and Daniele Nantes-Sobrinho, who served as Local Organizers at the Universidade de Brasília. Claudia and Daniele worked hard and were highly instrumental in guaranteeing the success of the Brasília Spring on Automated Reasoning.

Last but not least, we are thankful to the sponsors of ITP 2017: Microsoft, the European Association for Artificial Intelligence (EurAI), the District Federal Research Support Foundation (FAPDF), the Coordination of Personnel Training in Higher Education of the Brazilian Education Ministry (CAPES), the Brazilian National Council for Scientific and Technological Development (CNPq), and the Departments of Computer Science and Mathematics of the Universidade de Brasília (UnB).

September 2017

Mauricio Ayala-Rincón
César Muñoz

Organization

Program Committee

Mauricio Ayala-Rincón	Universidade de Brasília (Co-chair), Brazil
César Muñoz	NASA (Co-chair), USA
María Alpuente	Universitat Politècnica de València, Spain
Vander Alves	Universidade de Brasília, Brazil
June Andronick	CSIRO—Data61 and UNSW, Australia
Jeremy Avigad	Carnegie Mellon University, USA
Sylvie Boldo	Inria, France
Ana Bove	Chalmers University of Technology, Sweden
Adam Chlipala	MIT, USA
Gilles Dowek	Inria and ENS Paris-Saclay, France
Aaron Dutle	NASA, USA
Amy Felty	University of Ottawa, Canada
Marcelo Frias	IT Buenos Aires, Argentina
Ruben Gamboa	University of Wyoming, USA
Herman Geuvers	Radboud University Nijmegen, The Netherlands
Elsa Gunter	University of Illinois at Urbana-Champaign, USA
John Harrison	Intel Corporation, USA
Nao Hirokawa	JAIST, Japan
Matt Kaufmann	University of Texas at Austin, USA
Mark Lawford	McMaster University, Canada
Andreas Lochbihler	Institute of Information Security, ETH Zurich, Switzerland
Assia Mahboubi	Inria, France
Panagiotis Manolios	Northeastern University, USA
Gopalan Nadathur	University of Minnesota, USA
Keiko Nakata	SAP Potsdam, Germany
Adam Naumowicz	Institute of Informatics, University of Bialystok, Poland
Tobias Nipkow	TU München, Germany
Scott Owens	University of Kent, UK
Sam Owre	SRI International, USA
Lawrence Paulson	University of Cambridge, UK
Leila Ribeiro	Universidade Federal do Rio Grande do Sul, Brazil
Claudio Sacerdoti Coen	University of Bologna, Italy
Augusto Sampaio	Universidade Federal de Pernambuco, Brazil
Monika Seisenberger	Swansea University, UK
Christian Sternagel	Universtity of Innsbruck, Austria
Sofiene Tahar	Concordia University, Canada
Christian Urban	King's College London, UK
Josef Urban	Czech Technical University in Prague, Czech Republic

ITP Steering Committee

Lawrence Paulson (Chair)	University of Cambridge, UK
David Basin	ETH Zurich, Switzerland
Yves Bertot	Inria, France
Amy Felty	University of Ottawa, Canada
Panagiotis Manolios	Northeastern University, USA
César Muñoz	NASA, USA
Michael Norrish	CSIRO—Data61 and ANU, Australia
Sofiène Tahar	Concordia University, Canada
Christian Urban	King's College London, UK
Jasmin Blanchette (Ex-officio)	Vrije Universiteit Amsterdam, The Netherlands

Organizing Committee

Cláudia Nalon	Universidade de Brasília, Brazil
Daniele Nantes-Sobrinho	Universidade de Brasília, Brazil
Elaine Pimentel	Universidade Federal do Rio Grande do Norte, Brazil
João Marcos	Universidade Federal do Rio Grande do Norte, Brazil

Additional Reviewers

Akbarpour, Behzad
Altenkirch, Thorsten
Asperti, Andrea
Azzi, Guilherme
Ballis, Demis
Bannister, Callum
Beckert, Bernhard
Berger, Ulrich
Besson, Frédéric
Brown, Chad
Castro, Thiago
Chau, Cuong
Claessen, Koen
Cohen, Cyril
Collins, Pieter
Daghar, Alaeddine
Danielsson, Nils Anders
Demeo, William
Escobar, Santiago
Faissole, Florian
Foster, Simon
Färber, Michael
Gacek, Andrew
Goel, Shilpi
Grabowski, Adam
Gutiérrez, Raúl
Helali, Ghassen
Herbelin, Hugo
Hunt, Warren A.
Iyoda, Juliano
Kaliszyk, Cezary
Keller, Chantal
Korniłowicz, Artur
Kozen, Dexter
Krebbers, Robbert
Kullmann, Oliver
Lammich, Peter
Larchey-Wendling, Dominique
Lawrence, Andrew
Lee, Holden
Magaud, Nicolas
Maggesi, Marco
Mahmoud, Mohamed Yousri
Maietti, Maria Emilia
Maric, Filip
Matichuk, Daniel
Melquiond, Guillaume
Miné, Antoine
Miquey, Étienne
Moscato, Mariano
Nakano, Keisuke
Narkawicz, Anthony

Nordvall Forsberg, Fredrik
Norrish, Michael
Popescu, Andrei
Rashid, Adnan
Setzer, Anton
Sewell, Thomas
Siddique, Umair
Sozeau, Matthieu
Sternagel, Thomas
Tan, Yong Kiam
Teixeira, Leopoldo
Théry, Laurent
Titolo, Laura
Van Oostrom, Vincent
Villanueva, Alicia
Wiedijk, Freek
Young, William D.

Local Sponsors

Coordination of Personnel Training in Higher Education of the Brazilian Education Ministry (CAPES)

District Federal Research Support Foundation (FAPDF)

Brazilian National Council for Scientific and Technological Development (CNPq)

Department of Computer Science
Universidade de Brasília - UnB

Department of Mathematics
Universidade de Brasília - UnB

Invited Talks

Whitebox Automation

Leonardo de Moura[1], Jeremy Avigad[2], Gabriel Ebner[3], Jared Roesch[4], and Sebastian Ullrich[5]

[1] Microsoft Research
leonardo@microsoft.com
[2] Carnegie Mellon University
avigad@andrew.cmu.edu
[3] Vienna University of Technology
gebner@gebner.org
[4] University of Washington
jroesch@cs.washington.edu
[5] Karlsruhe Institute of Technology
ullrich@kit.edu

Abstract. We describe the metaprogramming language currently in use in Lean, a new open source theorem prover that is designed to bridge the gap between interactive use and automation. Lean implements a version of the Calculus of Inductive Constructions. Its elaborator and unification algorithms are designed around the use of type classes, which support algebraic reasoning, programming abstractions, and other generally useful means of expression. Lean also has parallel compilation and checking of proofs, and provides a server mode that supports a continuous compilation and rich user interaction in editing environments such as Emacs, Vim, and Visual Studio Code. Lean currently has a conditional term rewriter, and several components commonly found in state-of-the-art Satisfiability Modulo Theories (SMT) solvers such as forward chaining, congruence closure, handling of associative and commutative operators, and E-matching. All these components are available in the metaprogramming framework, and can be combined and customized by users.

In this talk, we provide a short introduction to the Lean theorem prover and its metaprogramming framework. We also describe how this framework extends Lean's object language with an API to many of Lean's internal structures and procedures, and provides ways of reflecting object-level expressions into the metalanguage. We provide evidence to show that our implementation is performant, and that it provides a convenient and flexible way of writing not only small-scale interactive tactics, but also more substantial kinds of automation.

We view this as important progress towards our overarching goal of bridging the gap between interactive and automated reasoning. Users who develop libraries for interactive use can now more easily develop special-purpose automation to go with them thereby encoding procedural heuristics and expertise alongside factual knowledge. At the same time, users who want to use Lean as a back end to assist in complex verification tasks now have flexible means of adapting Lean's libraries and automation to their specific needs. As a result, our metaprogramming language opens up new opportunities, allowing for more

natural and intuitive forms of interactive reasoning, as well as for more flexible and reliable forms of automation.

More information about Lean can be found at http://leanprover.github.io. The interactive book "Theorem Proving in Lean"[1] is the standard reference for Lean. The book is available in PDF and HTML formats. In the HTML version, all examples and exercises can be executed in the reader's web browser.

[1] https://leanprover.github.io/theorem_proving_in_lean.

Automated Theory Exploration for Interactive Theorem Proving

An Introduction to the Hipster System

Moa Johansson

Department of Computer Science and Engineering,
Chalmers University of Technology, Gothenburg, Sweden
moa.johansson@chalmers.se

Abstract. Theory exploration is a technique for automatically discovering new interesting lemmas in a mathematical theory development using testing. In this paper I will present the theory exploration system Hipster, which automatically discovers and proves lemmas about a given set of datatypes and functions in Isabelle/HOL. The development of Hipster was originally motivated by attempts to provide a higher level of automation for proofs by induction. Automating inductive proofs is tricky, not least because they often need auxiliary lemmas which themselves need to be proved by induction. We found that many such basic lemmas can be discovered automatically by theory exploration, and importantly, quickly enough for use in conjunction with an interactive theorem prover without boring the user.

Automating Formalization by Statistical and Semantic Parsing of Mathematics

Cezary Kaliszyk[1], Josef Urban[2], and Jiří Vyskočil[2]

[1] University of Innsbruck, Innsbruck, Austria
cezary.kaliszyk@uibk.ac.at
[2] Czech Technical University in Prague, Prague, Czech Republic

Abstract. We discuss the progress in our project which aims to automate formalization by combining natural language processing with deep semantic understanding of mathematical expressions. We introduce the overall motivation and ideas behind this project, and then propose a context-based parsing approach that combines efficient statistical learning of deep parse trees with their semantic pruning by type checking and large-theory automated theorem proving. We show that our learning method allows efficient use of large amount of contextual information, which in turn significantly boosts the precision of the statistical parsing and also makes it more efficient. This leads to a large improvement of our first results in parsing theorems from the Flyspeck corpus.

Contents