Lecture Notes in Computer Science 10895

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Jeremy Avigad · Assia Mahboubi (Eds.)

Interactive Theorem Proving

9th International Conference, ITP 2018
Held as Part of the Federated Logic Conference, FloC 2018
Oxford, UK, July 9–12, 2018
Proceedings

Springer

Editors
Jeremy Avigad
Carnegie Mellon University
Pittsburgh, PA
USA

Assia Mahboubi
Inria
Nantes
France

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-94820-1 ISBN 978-3-319-94821-8 (eBook)
https://doi.org/10.1007/978-3-319-94821-8

Library of Congress Control Number: 2018947441

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Printed on acid-free paper

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

Preface

The International Conference on Interactive Theorem Proving (ITP) is a premier venue for publishing research in the area of logical frameworks and interactive proof assistants. Its topics include both theoretical foundations and implementation aspects of the technology, as well as applications to verifying hardware and software systems to ensure their safety and security, and applications to the formal verification of mathematical results.

ITP grew out of TPHOLs conferences and ACL2 workshops that began in the early 1990s. Previous editions of ITP have taken place in Brasília (Brazil), Nancy (France), Nanjing (China), Vienna (Austria), Rennes (France), Princeton (USA), Berg en Dal (The Netherlands), and Edinburgh (UK).

This ninth edition, ITP 2018, was part of the Federated Logic Conference (FLoC) 2018, and took place in Oxford, UK, during July 9–12, 2018. We thank the FLoC Organizing Committee for undertaking the Herculean task of planning and organizing the event.

In all, 55 regular papers and ten short papers were submitted to the conference. Each paper was reviewed by at least three people, either members of the Program Committee or external reviewers. The committee ultimately accepted 32 regular papers and five short papers.

ITP 2018 included memorial lectures in honor of Mike Gordon and Vladimir Voevodsky, two influential figures in interactive theorem proving who had passed away over the course of the previous year. John Harrison was invited to present the lecture for Gordon, and Daniel Grayson was invited to present the lecture for Voevodsky. In addition, Jean-Christophe Filliâtre was invited to present a third keynote talk.

The present volume collects all the scientific contributions to the conference as well as abstracts of the three keynote presentations. We are grateful to the members of the ITP Steering Committee for their guidance and advice, and especially grateful to our colleagues on the Program Committee and the external reviewers, whose careful reviews and thoughtful deliberations served to maintain the high quality of the conference. We extend our thanks to the authors of all submitted papers and the ITP community at large, without whom the conference would not exist.

Finally, we are grateful for Springer for once again publishing these proceedings as a volume in the LNCS series, and we thank the editorial team for the smooth interactions.

June 2018

Jeremy Avigad
Assia Mahboubi

Organization

Program Committee

Andreas Abel	Gothenburg University, Sweden
Benedikt Ahrens	University of Birmingham, UK
June Andronick	CSIRO's Data 61 and UNSW, Australia
Jeremy Avigad	Carnegie Mellon University, USA
Jasmin Christian Blanchette	Vrije Universiteit Amsterdam, The Netherlands
Adam Chlipala	Massachusetts Institute of Technology, USA
Thierry Coquand	Chalmers University of Technology, Sweden
Karl Crary	Carnegie Mellon University, USA
Leonardo de Moura	Microsoft, USA
Delphine Demange	University of Rennes 1/IRISA, France
Timothy Griffin	University of Cambridge, UK
Thomas Hales	University of Pittsburgh, USA
John Harrison	Amazon Web Services, USA
Chung-Kil Hur	Seoul National University, South Korea
Johannes Hölzl	Vrije Universiteit Amsterdam, The Netherlands
Jacques-Henri Jourdan	MPI-SWS, Germany
Cezary Kaliszyk	University of Innsbruck, Austria
Ambrus Kaposi	Eötvös Loránd University, Hungary
Chantal Keller	LRI, Université Paris-Sud, France
Assia Mahboubi	Inria, France
Panagiotis Manolios	Northeastern University, USA
Mariano Moscato	National Institute of Aerospace, USA
Magnus O. Myreen	Chalmers University of Technology, Sweden
Tobias Nipkow	Technical University of Munich, Germany
Lawrence Paulson	University of Cambridge, UK
André Platzer	Carnegie Mellon University, USA
Andrei Popescu	Middlesex University London, UK
Matthieu Sozeau	Inria, France
Pierre-Yves Strub	École Polytechnique, France
Enrico Tassi	Inria, France
Zachary Tatlock	University of Washington, USA
Laurent Théry	Inria, France
Cesare Tinelli	The University of Iowa, USA
Alwen Tiu	The Australian National University, Australia
Makarius Wenzel	sketis.net, Germany
Freek Wiedijk	Radboud University, The Netherlands

Additional Reviewers

Åman Pohjola, Johannes
Ahrendt, Wolfgang
Anguili, Carlo
Becker, Heiko
Booij, Auke
Bourke, Timothy
Brecknell, Matthew
Brunner, Julian
Chen, Zilin
Cordwell, Katherine
Czajka, Łukasz
Dawson, Jeremy
Eberl, Manuel
Filliâtre, Jean-Christophe
Fleury, Mathias
Fulton, Nathan
Gammie, Peter
Geuvers, Herman
Hou, Zhe
Immler, Fabian
Jung, Ralf
Komendantskaya, Ekaterina
Kovács, András Kovács
Kraus, Nicolai
Larchey-Wendling, Dominique
Le Roux, Stephane
Lewis, Robert
Martins, João G.
Mitsch, Stefan
Murray, Toby
Mörtberg, Anders
Nagashima, Yutaka
Naumowicz, Adam
Ringer, Talia
Rot, Jurriaan
Sanan, David
Scapin, Enrico
Schmaltz, Julien
Schürmann, Carsten
Sewell, Thomas
Sickert, Salomon
Sison, Robert
Sternagel, Christian
Tanaka, Miki
Tassarotti, Joseph
Thiemann, René
Traytel, Dmitriy
Turaga, Prathamesh
Verbeek, Freek
Villadsen, Jørgen

Abstracts of Invited Talks

Deductive Program Verification

Jean-Christophe Filliâtre[1,2]

[1] Lab. de Recherche en Informatique, Univ. Paris-Sud, CNRS, Orsay, F-91405
[2] Inria Saclay – Île-de-France, Orsay, F-91893
Jean-Christophe.Filliatre@lri.fr

Abstract. Among formal methods, the deductive verification approach consists in first building verification conditions and then resorting to traditional theorem proving. Most deductive verification tools involve a high degree of proof automation through the use of SMT solvers. Yet there may be a substantial part of interactive theorem proving in program verification, such as inserting logical cuts, ghost code, or inductive proofs via lemma functions. In this talk, I will show how the Why3 tool for deductive verification resembles more and more a traditional ITP, while stressing key differences between the two.

Keywords: Deductive verification · Theorem proving

Voevodsky's Work on Formalization of Proofs and the Foundations of Mathematics

Daniel R. Grayson

Abstract. A consistent thread running through the three decades of Voevodsky's work is the application of the ideas of homotopy theory in new and surprising ways, first to motives, and then to formalization of proofs and the foundations of mathematics. I will present the story of the latter development, focusing on the points of interest to mathematicians.

Mike Gordon: Tribute to a Pioneer in Theorem Proving and Formal Verification

John Harrison

Amazon Web Services
jrh013@gmail.com

Abstract. Prof. Michael J. C. Gordon, FRS was a great pioneer in both computer-aided formal verification and interactive theorem proving. His own work and that of his students helped to explore and map out these new fields and in particular the fruitful connections between them. His seminal HOL theorem prover not only gave rise to many successors and relatives, but was also the framework in which many new ideas and techniques in theorem proving and verification were explored for the first time. Mike's untimely death in August 2017 was a tragedy first and foremost for his family, but was felt as a shocking loss too by many of us who felt part of his extended family of friends, former students and colleagues throughout the world. Mike's intellectual example as well as his unassuming nature and personal kindness will always be something we treasure. In my talk here I will present an overall perspective on Mike's life and the whole arc of his intellectual career. I will also spend time looking ahead, for the research themes he helped to establish are still vital and exciting today in both academia and industry.

Contents