Lecture Notes in Computer Science 7406

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

Lennart Beringer Amy Felty (Eds.)

Interactive Theorem Proving

Third International Conference, ITP 2012
Princeton, NJ, USA, August 13-15, 2012
Proceedings

Springer

Volume Editors

Lennart Beringer
Princeton University
Department of Computer Science
35 Olden Street
Princeton, NJ 08540, USA
E-mail: eberinge@cs.princeton.edu

Amy Felty
University of Ottawa, School of Electrical Engineering and Computer Science
800 King Edward Ave.
Ottawa, ON K1N 6N5, Canada
E-mail: afelty@eecs.uottawa.ca

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-32346-1 e-ISBN 978-3-642-32347-8
DOI 10.1007/978-3-642-32347-8
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: Applied for

CR Subject Classification (1998): I.2.3, F.4.1, F.4.3, I.2.2, I.2.4, F.3, D.2.4, F.1.1, K.6.5

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at ITP 2012, the Third International Conference on Interactive Theorem Proving. The conference was held August 13–15 in Princeton, New Jersey, USA, organized by the General Co-chairs Andrew W. Appel and Lennart Beringer.

ITP brings together researchers working in interactive theorem proving and related areas, ranging from theoretical foundations to implementation aspects and applications in program verification, security, and formalization of mathematics. ITP 2012 was the third annual conference in this series. The first meeting was held July 11–14, 2010, in Edinburgh, UK, as part of the Federated Logic Conference (FLoC). The second meeting took place August 22–25, 2011, in Berg en Dal, The Netherlands. ITP evolved from the previous TPHOLs series (Theorem Proving in Higher-Order Logics), which took place every year from 1988 to 2009.

There were 40 submissions to ITP 2012, each of which was reviewed by at least four Program Committee members. Out of the 40 submissions, 36 were regular papers and four were rough diamonds. Unlike previous editions of TPHOLs/ITP, this year's call for papers requested "submissions to be accompanied by verifiable evidence of a suitable implementation." In accordance with this, almost all submissions came with the source files of a corresponding formalization, which were thoroughly inspected by the reviewers and influenced the acceptance decisions. The Program Committee accepted 25 papers, which include 21 regular papers and four rough diamonds, all of which appear in this volume. We were pleased to be able to assemble a strong program covering topics such as program verification, security, formalization of mathematics and theorem prover development. The Program Committee also invited three leading researchers to present invited talks: Gilles Barthe (IMDEA, Spain), Lawrence Paulson (University of Cambridge, UK), and André Platzer (Carnegie Mellon University, USA). In addition, the Program Committee invited Andrew Gacek (Rockwell Collins) to give a tutorial on the Abella system. We thank all these speakers for also contributing articles to these proceedings.

ITP 2012 also featured two associated workshops held the day before the conference: The Coq Workshop 2012 and Isabelle Users Workshop 2012, bringing together users and developers in each of these communities to discuss issues specific to these two widely used tools.

The work of the Program Committee and the editorial process were facilitated by the EasyChair conference management system. We are grateful to Springer for publishing these proceedings, as they have done for all ITP and TPHOLs meetings since 1993.

Many people contributed to the success of ITP 2012. The Program Committee worked hard at reviewing papers, holding extensive discussions during the

on-line Program Committee meeting, and making final selections of accepted papers and invited speakers. Thanks are also due to the additional referees enlisted by Program Committee members. Finally, we would like to thank Andrew W. Appel and his staff for taking care of all the local arrangements, Princeton University for the administrative and financial support, and NEC Laboratories, Princeton, for their additional sponsorship.

June 2012

Lennart Beringer
Amy Felty

Conference Organization

General Co-chairs

Andrew Appel	Princeton University, USA
Lennart Beringer	Princeton University, USA

Program Co-chairs

Lennart Beringer	Princeton University, USA
Amy Felty	University of Ottawa, Canada

Program Committee

Andreas Abel	LMU Munich, Germany
Nick Benton	Microsoft Research Cambridge, UK
Stefan Berghofer	secunet Security Networks AG, Germany
Lennart Beringer	Princeton University, USA
Yves Bertot	INRIA Sophia-Antipolis, France
Adam Chlipala	MIT, USA
Ewen Denney	SGT/NASA Ames, USA
Peter Dybjer	Chalmers University of Technology, Sweden
Amy Felty	University of Ottawa, Canada
Herman Geuvers	Radboud University of Nijmegen, The Netherlands
Georges Gonthier	Microsoft Research Cambridge, UK
Jim Grundy	Intel Corp., USA
Elsa Gunter	University of Illinois at Urbana-Champaign, USA
Hugo Herbelin	INRIA Roquencourt-Paris, France
Joe Hurd	Galois, Inc., USA
Reiner Hähnle	Technical University of Darmstadt, Germany
Matt Kaufmann	University of Texas at Austin, USA
Gerwin Klein	NICTA/University of New South Wales, Australia
Assia Mahboubi	INRIA Saclay, France
Conor McBride	University of Strathclyde, UK
Alberto Momigliano	University of Milan, Italy
Magnus O. Myreen	University of Cambridge, UK
Tobias Nipkow	TU Munich, Germany
Sam Owre	SRI, USA

Christine Paulin-Mohring	Université Paris-Sud, France
David Pichardie	INRIA Rennes, France
Brigitte Pientka	McGill University, Canada
Randy Pollack	Harvard University, USA
Julien Schmaltz	Open University of the Netherlands
Bas Spitters	Radboud University of Nijmegen, The Netherlands
Sofiene Tahar	Concordia University, Canada
Makarius Wenzel	Université Paris-Sud, France

Additional Reviewers

Abbasi, Naeem
Andronick, June
Appel, Andrew W.
Aravantinos, Vincent
Boespflug, Mathieu
Boldo, Sylvie
Brown, Chad
Bubel, Richard
Cave, Andrew
Chamarthi, Harsh Raju
Contejean, Evelyne
Dockins, Robert
Dominguez, Cesar
Filliâtre, Jean-Christophe
Gustafsson, Daniel
Hölzl, Johannes
Jacobs, Bart
Ji, Ran
Joosten, Sebastiaan
Kennedy, Andrew
Khan-Afshar, Sanaz
Krebbers, Robbert
Krstić, Sava
Licata, Daniel R.
Liu, Liya
Makarov, Evgeny
Matthews, John
McKinna, James
Melquiond, Guillaume
Mhamdi, Tarek
Murray, Toby
O'Connor, Russell
Paganelli, Gabriele
Payet, Etienne
Popescu, Andrei
Pous, Damien
Preoteasa, Viorel
Román-Díez, Guillermo
Schmidt, Renate
Senjak, Christoph-Simon
Sewell, Thomas
Siles, Vincent
Spiwack, Arnaud
Stewart, Gordon
Swierstra, Wouter
Trinder, Phil
Tuttle, Mark
Urban, Christian
van Gastel, Bernard
Verbeek, Freek
Wehrman, Ian
Wetzler, Nathan
Zeilberger, Noam

Table of Contents

Invited Talks

Invited Tutorial

Formalization of Mathematics I

Program Abstraction and Logics

Data Structures and Synthesis

Security

(Non-)Termination and Automata

Program Verification

Rough Diamonds I: Reasoning about Program Execution

Theorem Prover Development

Formalization of Mathematics II

Rough Diamonds II: Prover Infrastructure and Modeling Styles