

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

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

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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 Bergen 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
Lennart Beringer

Princeton University, USA
Princeton University, USA

Program Co-chairs

Lennart Beringer
Amy Felty

Princeton University, USA
University of Ottawa, Canada

Program Committee

Andreas Abel
Nick Benton
Stefan Berghofer
Lennart Beringer
Yves Bertot
Adam Chlipala
Ewen Denney
Peter Dybjer
Amy Felty
Herman Geuvers

LMU Munich, Germany
Microsoft Research Cambridge, UK
secunet Security Networks AG, Germany
Princeton University, USA
INRIA Sophia-Antipolis, France
MIT, USA
SGT/NASA Ames, USA
Chalmers University of Technology, Sweden
University of Ottawa, Canada
Radboud University of Nijmegen,
The Netherlands

Georges Gonthier
Jim Grundy
Elsa Gunter

Microsoft Research Cambridge, UK
Intel Corp., USA
University of Illinois at Urbana-Champaign,
USA

Hugo Herbelin
Joe Hurd
Reiner Hähnle
Matt Kaufmann
Gerwin Klein

INRIA Roquencourt-Paris, France
Galois, Inc., USA
Technical University of Darmstadt, Germany
University of Texas at Austin, USA
NICTA/University of New South Wales,
Australia

Assia Mahboubi
Conor McBride
Alberto Momigliano
Magnus O. Myreen
Tobias Nipkow
Sam Owre

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

Table of Contents

Invited Talks

MetiTarski: Past and Future.....	1
<i>Lawrence C. Paulson</i>	
Computer-Aided Cryptographic Proofs	11
<i>Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz, and Santiago Zanella Béguelin</i>	
A Differential Operator Approach to Equational Differential Invariants (Invited Paper)	28
<i>André Platzer</i>	

Invited Tutorial

Abella: A Tutorial	49
<i>Andrew Gacek</i>	

Formalization of Mathematics I

A Cantor Trio: Denumerability, the Reals, and the Real Algebraic Numbers	51
<i>Ruben Gamboa and John Cowles</i>	
Construction of Real Algebraic Numbers in COQ.....	67
<i>Cyril Cohen</i>	
A Refinement-Based Approach to Computational Algebra in COQ.....	83
<i>Maxime Dénès, Anders Mörtberg, and Vincent Siles</i>	

Program Abstraction and Logics

Bridging the Gap: Automatic Verified Abstraction of C	99
<i>David Greenaway, June Andronick, and Gerwin Klein</i>	
Abstract Interpretation of Annotated Commands	116
<i>Tobias Nipkow</i>	
Verifying and Generating WP Transformers for Procedures on Complex Data	133
<i>Patrick Michel and Arnd Poetzsch-Heffter</i>	

Data Structures and Synthesis

Bag Equivalence via a Proof-Relevant Membership Relation	149
<i>Nils Anders Danielsson</i>	
Applying Data Refinement for Monadic Programs to Hopcroft’s Algorithm.	166
<i>Peter Lammich and Thomas Tuerk</i>	
Synthesis of Distributed Mobile Programs Using Monadic Types in Coq	183
<i>Marino Miculan and Marco Paviotti</i>	

Security

Towards Provably Robust Watermarking	201
<i>David Baelde, Pierre Courtieu, David Gross-Amblard, and Christine Paulin-Mohring</i>	
Priority Inheritance Protocol Proved Correct	217
<i>Xingyuan Zhang, Christian Urban, and Chunhan Wu</i>	
Formalization of Shannon’s Theorems in SSReflect-Coq	233
<i>Reynald Affeldt and Manabu Hagiwara</i>	

(Non-)Termination and Automata

Stop When You Are Almost-Full: Adventures in Constructive Termination	250
<i>Dimitrios Vytiniotis, Thierry Coquand, and David Wahlstedt</i>	
Certification of Nontermination Proofs	266
<i>Christian Sternagel and René Thiemann</i>	
A Compact Proof of Decidability for Regular Expression Equivalence . . .	283
<i>Andrea Asperti</i>	

Program Verification

Using Locales to Define a Rely-Guarantee Temporal Logic	299
<i>William Mansky and Elsa L. Gunter</i>	
Charge! – A Framework for Higher-Order Separation Logic in Coq	315
<i>Jesper Bengtson, Jonas Braband Jensen, and Lars Birkedal</i>	

Rough Diamonds I: Reasoning about Program Execution

Mechanised Separation Algebra	332
<i>Gerwin Klein, Rafal Kolanski, and Andrew Boyton</i>	
Directions in ISA Specification	338
<i>Anthony Fox</i>	

Theorem Prover Development

More SPASS with Isabelle: Superposition with Hard Sorts and Configurable Simplification	345
<i>Jasmin Christian Blanchette, Andrei Popescu, Daniel Wand, and Christoph Weidenbach</i>	
A Language of Patterns for Subterm Selection	361
<i>Georges Gonthier and Enrico Tassi</i>	

Formalization of Mathematics II

Numerical Analysis of Ordinary Differential Equations in Isabelle/HOL	377
<i>Fabian Immler and Johannes Hölzl</i>	
Proof Pearl: A Probabilistic Proof for the Girth-Chromatic Number Theorem	393
<i>Lars Noschinski</i>	

Rough Diamonds II: Prover Infrastructure and Modeling Styles

Standalone Tactics Using OpenTheory	405
<i>Ramana Kumar and Joe Hurd</i>	
Functional Programs: Conversions between Deep and Shallow Embeddings	412
<i>Magnus O. Myreen</i>	
Author Index	419