

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

Sandrine Blazy Christine Paulin-Mohring
David Pichardie (Eds.)

Interactive Theorem Proving

4th International Conference, ITP 2013
Rennes, France, July 22-26, 2013
Proceedings

Volume Editors

Sandrine Blazy
Université Rennes 1, IRISA
Campus de Beaulieu
35042 Rennes Cedex, France
E-mail: sandrine.blazy@irisa.fr

Christine Paulin-Mohring
Université Paris-Sud, LRI
Bat 650, Univ. Paris Sud
91405 Orsay Cedex, France
E-mail: christine.paulin@lri.fr

David Pichardie
Inria Rennes-Bretagne Atlantique
Campus de Beaulieu
35042 Rennes Cedex, France
E-mail: david.pichardie@inria.fr

ISSN 0302-9743
ISBN 978-3-642-39633-5
DOI 10.1007/978-3-642-39634-2
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-39634-2

Library of Congress Control Number: 2013942669

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 2013

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, 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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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 2013, the 4th International Conference on Interactive Theorem Proving. The conference was held during July 23–26 in Rennes, France.

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 2013 was the fourth annual conference in this series. The first meeting was held during July 11–14, 2010, in Edinburgh, UK, as part of the Federated Logic Conference (FLoC). The second meeting took place during August 22–25, 2011, in Berg en Dal, The Netherlands. The third meeting was held during August 13–15 in Princeton, New Jersey, USA. ITP evolved from the previous TPHOLs series (Theorem Proving in Higher-Order Logics), which took place every year from 1988 to 2009.

There were 66 submissions to ITP 2013, each of which was reviewed by at least three Program Committee members. Out of the 66 submissions, 53 were regular papers and 13 were rough diamonds. This year, the 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 influenced the acceptance decisions. The Program Committee accepted 33 papers, which include 26 regular papers and seven 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: Dominique Bolignano (Prove & Run, France), Rustan Leino (Microsoft Research, USA), and Carsten Schürmann (IT University of Copenhagen, Denmark). In addition, the Program Committee invited Assia Mahboubi and Enrico Tassi (Inria, France) to give a tutorial on the Mathematical Components library and Panagiotis Manolios (Northeastern University, USA) to give a tutorial on counterexample generation in interactive theorem provers. We thank all these speakers for also contributing articles to these proceedings.

ITP 2013 also featured two associated workshops held the day before the conference: the AI4FM 2013 workshop and the Coq Workshop 2013. 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 2013. 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 reviewers

enlisted by Program Committee members. Finally, we would like to thank our sponsors: Inria, the University of Rennes 1, SISCom Bretagne, Rennes Metropole and Région Bretagne.

May 2013

Sandrine Blazy
Christine Paulin-Mohring
David Pichardie

Organization

Program Committee

Wolfgang Ahrendt	Chalmers University, Sweden
Jeremy Avigad	Carnegie Mellon University, USA
Nick Benton	Microsoft Research, UK
Lennart Beringer	Princeton University, USA
Sandrine Blazy	Université Rennes 1, France
Adam Chlipala	MIT, USA
Thierry Coquand	Chalmers University, Sweden
Amy Felty	University of Ottawa, Canada
Ruben Gamboa	University of Wyoming, USA
Herman Geuvers	Radboud University Nijmegen, The Netherlands
Elsa Gunter	University of Illinois at Urbana-Champaign, USA
David Hardin	Rockwell Collins, Inc., USA
John Harrison	Intel Corporation, USA
Gerwin Klein	NICTA and UNSW, Australia
Assia Mahboubi	Inria - École polytechnique, France
Panagiotis Manolios	Northeastern University, USA
Conor McBride	University of Strathclyde, UK
Cesar Munoz	NASA, USA
Magnus O. Myreen	University of Cambridge, UK
Tobias Nipkow	TU München, Germany
Michael Norrish	NICTA and ANU, Australia
Sam Owre	SRI International, USA
Christine Paulin-Mohring	Université Paris-Sud 11, France
Lawrence Paulson	University of Cambridge, UK
David Pichardie	Inria Rennes, France
Brigitte Pientka	McGill University, Canada
Laurence Pierre	TIMA, France
Lee Pike	Galois, Inc., USA
Claudio Sacerdoti Coen	University of Bologna, Italy
Julien Schmaltz	Open University of the Netherlands, The Netherlands
Makoto Takeyama	AIST/COVS, Japan
René Thiemann	University of Innsbruck, Austria
Laurent Théry	Inria Sophia-Antipolis, France
Makarius Wenzel	Université Paris-Sud 11, France

Additional Reviewers

Andronick, June	Huffman, Brian
Asperti, Andrea	Huisman, Marieke
Baelde, David	Hur, Chung-Kil
Bell, Christian J.	Hölzl, Johannes
Bengtson, Jesper	Immler, Fabian
Bertot, Yves	Jackson, Paul
Blanchette, Jasmin Christian	Joosten, Bas
Boldo, Sylvie	Kaliszyk, Cezary
Campbell, Brian	Kumar, Ramana
Capretta, Venanzio	Lammich, Peter
Cave, Andrew	Licata, Daniel R.
Cohen, Cyril	Lumsdaine, Peter
Courtieu, Pierre	Matichuk, Daniel
Dagit, Jason	Popescu, Andrei
Danielsson, Nils Anders	Ricciotti, Wilmer
Daum, Matthias	Schlesinger, Cole
Demange, Delphine	Slind, Konrad
Diatchki, Iavor	Sternagel, Christian
Dénès, Maxime	Stewart, Gordon
Feliachi, Abderrahmane	Tassi, Enrico
Ferreira, Francisco	Verbeek, Freek
Fuhs, Carsten	Wiedijk, Freek
Gacek, Andrew	Winwood, Simon
Gammie, Peter	Wolff, Burkhard
Greenaway, David	Ziliani, Beta
Gregoire, Benjamin	

Table of Contents

Invited Talks

Applying Formal Methods in the Large	1
<i>Dominique Bolignano</i>	
Automating Theorem Proving with SMT	2
<i>K. Rustan M. Leino</i>	
Certifying Voting Protocols	17
<i>Carsten Schürmann</i>	

Invited Tutorials

Counterexample Generation Meets Interactive Theorem Proving: Current Results and Future Opportunities	18
<i>Panagiotis Manolios</i>	
Canonical Structures for the Working Coq User	19
<i>Assia Mahboubi and Enrico Tassi</i>	

Regular Papers

MaSh: Machine Learning for Sledgehammer	35
<i>Daniel Kühlwein, Jasmin Christian Blanchette, Cezary Kaliszyk, and Josef Urban</i>	
Scalable LCF-Style Proof Translation	51
<i>Cezary Kaliszyk and Alexander Krauss</i>	
Lightweight Proof by Reflection Using a Posteriori Simulation of Effectful Computation	67
<i>Guillaume Claret, Lourdes del Carmen González Huesca, Yann Régis-Gianas, and Beta Ziliani</i>	
Automatic Data Refinement	84
<i>Peter Lammich</i>	
Data Refinement in Isabelle/HOL	100
<i>Florian Haftmann, Alexander Krauss, Ondřej Kunčar, and Tobias Nipkow</i>	
Light-Weight Containers for Isabelle: Efficient, Extensible, Nestable	116
<i>Andreas Lochbihler</i>	

Ordinals in HOL: Transfinite Arithmetic up to (and Beyond) ω_1	133
<i>Michael Norrish and Brian Huffman</i>	
Mechanising Turing Machines and Computability Theory in Isabelle/HOL	147
<i>Jian Xu, Xingyuan Zhang, and Christian Urban</i>	
A Machine-Checked Proof of the Odd Order Theorem	163
<i>Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovjev, Enrico Tassi, and Laurent Théry</i>	
Kleene Algebra with Tests and Coq Tools for while Programs	180
<i>Damien Pous</i>	
Program Analysis and Verification Based on Kleene Algebra in Isabelle/HOL	197
<i>Alasdair Armstrong, Georg Struth, and Tjark Weber</i>	
Pragmatic Quotient Types in Coq	213
<i>Cyril Cohen</i>	
Mechanical Verification of SAT Refutations with Extended Resolution	229
<i>Nathan Wetzler, Marijn J.H. Heule, and Warren A. Hunt Jr.</i>	
Formalizing Bounded Increase	245
<i>René Thiemann</i>	
Formal Program Optimization in Nuprl Using Computational Equivalence and Partial Types	261
<i>Vincent Rahli, Mark Bickford, and Abhishek Anand</i>	
Type Classes and Filters for Mathematical Analysis in Isabelle/HOL . . .	279
<i>Johannes Hölzl, Fabian Immler, and Brian Huffman</i>	
Formal Reasoning about Classified Markov Chains in HOL	295
<i>Liya Liu, Osman Hasan, Vincent Aravantinos, and Sofiène Tahar</i>	
Practical Probability: Applying pGCL to Lattice Scheduling	311
<i>David Cock</i>	
Adjustable References	328
<i>Viktor Vafeiadis</i>	
Handcrafted Inversions Made Operational on Operational Semantics . . .	338
<i>Jean-François Monin and Xiaomu Shi</i>	

Circular Coinduction in Coq Using Bisimulation-Up-To Techniques	354
<i>Jörg Endrullis, Dimitri Hendriks, and Martin Bodin</i>	
Program Extraction from Nested Definitions	370
<i>Kenji Miyamoto, Fredrik Nordvall Forsberg, and Helmut Schwichtenberg</i>	
Subformula Linking as an Interaction Method	386
<i>Kaustuv Chaudhuri</i>	
Automatically Generated Infrastructure for De Bruijn Syntaxes	402
<i>Emmanuel Polonowski</i>	
Shared-Memory Multiprocessing for Interactive Theorem Proving	418
<i>Makarius Wenzel</i>	
A Parallelized Theorem Prover for a Logic with Parallel Execution	435
<i>David L. Rager, Warren A. Hunt Jr., and Matt Kaufmann</i>	
Rough Diamonds	
Communicating Formal Proofs: The Case of Flyspeck	451
<i>Carst Tankink, Cezary Kaliszyk, Josef Urban, and Herman Geuvers</i>	
Square Root and Division Elimination in PVS	457
<i>Pierre Neron</i>	
The Picard Algorithm for Ordinary Differential Equations in Coq	463
<i>Evgeny Makarov and Bas Spitters</i>	
Stateless Higher-Order Logic with Quantified Types	469
<i>Evan Austin and Perry Alexander</i>	
Implementing Hash-Consed Structures in Coq	477
<i>Thomas Braibant, Jacques-Henri Jourdan, and David Monniaux</i>	
Towards Certifying Network Calculus	484
<i>Etienne Mabilie, Marc Boyer, Loïc Fejoz, and Stephan Merz</i>	
Steps towards Verified Implementations of HOL Light	490
<i>Magnus O. Myreen, Scott Owens, and Ramana Kumar</i>	
Author Index	497