

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 of Computer Science, Saarbruecken, Germany

Matt Kaufmann Lawrence C. Paulson (Eds.)

Interactive Theorem Proving

First International Conference, ITP 2010
Edinburgh, UK, July 11-14, 2010
Proceedings

Volume Editors

Matt Kaufmann
University of Texas at Austin, Department of Computer Science
Austin, TX 78712, USA
E-mail: kaufmann@cs.utexas.edu

Lawrence C. Paulson
University of Cambridge, Computer Laboratory
Cambridge, CB3 0FD, UK
E-mail: lp15@cam.ac.uk

Library of Congress Control Number: 2010929576

CR Subject Classification (1998): F.3, F.4.1, D.2.4, D.2, I.2.3, D.3

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

ISSN 0302-9743
ISBN-10 3-642-14051-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-14051-8 Springer Berlin Heidelberg New York

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.

springer.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

This volume contains the papers presented at ITP 2010: the First International Conference on Interactive Theorem Proving. It was held during July 11–14, 2010 in Edinburgh, Scotland as part of the Federated Logic Conference (FLoC, July 9–21, 2010) alongside the other FLoC conferences and workshops.

ITP combines the communities of two venerable meetings: the TPHOLs conference and the ACL2 workshop. The former conference originated in 1988 as a workshop for users of the HOL proof assistant. The first two meetings were at the University of Cambridge, but afterwards they were held in a variety of venues. By 1992, the workshop acquired the name *Higher-Order Logic Theorem Proving and Its Applications*. In 1996, it was christened anew as *Theorem Proving in Higher-Order Logics*, TPHOLs for short, and was henceforth organized as a conference. Each of these transitions broadened the meeting’s scope from the original HOL system to include other proof assistants based on forms of higher-order logic, including Coq, Isabelle and PVS. TPHOLs has regularly published research done using ACL2 (the modern version of the well-known Boyer-Moore theorem prover), even though ACL2 implements a unique computational form of first-order logic. The ACL2 community has run its own series of workshops since 1999. By merging TPHOLs with the ACL2 workshop, we include a broader community of researchers who work with interactive proof tools.

With our enlarged community, it was not surprising that ITP attracted a record-breaking 74 submissions, each of which was reviewed by at least three Programme Committee members. The Programme Committee accepted 33 papers and asked two leading researchers, Gerwin Klein and Benjamin Pierce, to present invited lectures about their work. We were able to assemble a strong programme covering topics such as counter-example generation, hybrid system verification, translations from one formalism to another, and cooperation between tools. Several verification case studies were presented, with applications to computational geometry, unification, real analysis, etc. The tool used most in the presented papers was Coq, followed by Isabelle/HOL.

Of the 33 accepted papers, five were “proof pearls” (concise and elegant worked examples) and three were “rough diamonds” (promising ideas in an early form). All 33 papers are included in these proceedings; unlike with TPHOLs, there are no separate proceedings consisting of “Track B” papers.

We would like to thank Moshe Vardi (FLoC General Chair), Leonid Libkin and Gordon Plotkin (FLoC Co-chairs), and the other members of the FLoC Organizing Committee. David Aspinall took care of ITP local arrangements, while Michael Norrish looked after ITP’s satellite workshops. We gratefully acknowledge the generous support of FLoC’s sponsors: the EPSRC (the UK’s Engineering and Physical Sciences Research Council), NSF (the US National Science Foundation), the Association for Symbolic Logic, CADE Inc. (Conference on Automated

Deduction), Hewlett-Packard Corporation, Microsoft Research, Google Inc., and Intel Corporation.

Every aspect of the editorial process, including the production of these proceedings, was facilitated by the EasyChair conference management system. We are grateful to the EasyChair team, Andrei Voronkov and Bartek Klin, for their advice and for fixing problems quickly as they arose. We are grateful to Springer for publishing these proceedings, as they have done for TPHOLs and its predecessors since 1993.

Next year's conference, ITP 2011, will be held at the Radboud University Nijmegen, The Netherlands. This site was chosen by a ballot of the interactive theorem proving research community.

This volume is dedicated to Susan Paulson, the second editor's wife, who went into hospital around the time that these proceedings were being assembled. She had been struggling with cancer for several years. As of this writing, she was not expected to live long enough to see this volume in print.

April 2010

Matt Kaufmann
Lawrence Paulson

Conference Organization

Programme Chairs

Matt Kaufmann University of Texas at Austin, USA
Lawrence Paulson University of Cambridge, UK

Workshop Chair

Michael Norrish NICTA, Australia

Programme Committee

Thorsten Altenkirch	Joe Hurd	David Pichardie
David Aspinall	Gerwin Klein	Brigitte Pientka
Jeremy Avigad	Xavier Leroy	Lee Pike
Gilles Barthe	Assia Mahboubi	Sandip Ray
Jens Brandt	Panagiotis Manolios	José Luis Ruiz Reina
Thierry Coquand	John Matthews	David Russinoff
Ruben Gamboa	J Moore	Peter Sewell
Georges Gonthier	César Muñoz	Konrad Slind
David Greve	Tobias Nipkow	Sofiène Tahar
Elsa L. Gunter	Michael Norrish	Christian Urban
John Harrison		

Local Arrangements

David Aspinall University of Edinburgh, UK

External Reviewers

Andreas Abel	Amjad Gawanmeh	Tarek Mhamdi
Sanaz Afshad	Thomas Genet	Aleksandar Nanevski
Mauricio Ayala-Rincón	Eugene Goldberg	Anthony Narkawicz
Peter Baumgartner	Alwyn Goodloe	Henrik Nilsson
Stefan Berghofer	David Greenaway	Steven Obua
Yves Bertot	Florian Haftmann	Nicolas Oury
Sandrine Blazy	Osman Hasan	Scott Owens
David Cachera	Daniel Hedin	Ioana Pasca
Harsh Raju Chamarthi	Joe Hendrix	Randy Pollack
James Chapman	Brian Huffman	François Pottier
Arthur Charguéraud	Ian Johnson	Vlad Rusu
Kaustuv Chaudhuri	Andrew Kennedy	Susmit Sarkar
Cyril Cohen	Rafal Kolanski	Carsten Schuermann
Juan Manuel Crespo	Alexander Krauss	Peter-Michael Seidel
Eugene Creswick	John Launchbury	Matthieu Sozeau
Nils Anders Danielsson	Hanbing Liu	Sam Staton
Iavor Diatchki	Liya Liu	Rob Sumners
Lucas Dixon	Luc Maranget	Andrew Tolmach
Levent Erkök	Andrew McCreight	Tiphaine Turpin
Germain Faure	James McKinna	Makarius Wenzel
Andrew Gacek	Stephan Merz	Iain Whiteside

Table of Contents

Invited Talks

A Formally Verified OS Kernel. Now What?	1
<i>Gerwin Klein</i>	
Proof Assistants as Teaching Assistants: A View from the Trenches	8
<i>Benjamin C. Pierce</i>	

Proof Pearls

A Certified Denotational Abstract Interpreter	9
<i>David Cachera and David Pichardie</i>	
Using a First Order Logic to Verify That Some Set of Reals Has No Lebesgue Measure	25
<i>John Cowles and Ruben Gamboa</i>	
A New Foundation for Nominal Isabelle	35
<i>Brian Huffman and Christian Urban</i>	
(Nominal) Unification by Recursive Descent with Triangular Substitutions	51
<i>Ramana Kumar and Michael Norrish</i>	
A Formal Proof of a Necessary and Sufficient Condition for Deadlock-Free Adaptive Networks	67
<i>Freek Verbeek and Julien Schmaltz</i>	

Regular Papers

Extending COQ with Imperative Features and Its Application to SAT Verification	83
<i>Michaël Armand, Benjamin Grégoire, Arnaud Spiwack, and Laurent Théry</i>	
A Tactic Language for Declarative Proofs	99
<i>Serge Autexier and Dominik Dietrich</i>	
Programming Language Techniques for Cryptographic Proofs	115
<i>Gilles Barthe, Benjamin Grégoire, and Santiago Zanella Béguelin</i>	
Nitpick: A Counterexample Generator for Higher-Order Logic Based on a Relational Model Finder	131
<i>Jasmin Christian Blanchette and Tobias Nipkow</i>	

Formal Proof of a Wave Equation Resolution Scheme: The Method Error	147
<i>Sylvie Boldo, François Clément, Jean-Christophe Filliâtre, Micaela Mayero, Guillaume Melquiond, and Pierre Weis</i>	
An Efficient Coq Tactic for Deciding Kleene Algebras	163
<i>Thomas Braibant and Damien Pous</i>	
Fast LCF-Style Proof Reconstruction for Z3	179
<i>Sascha Böhme and Tjark Weber</i>	
The Optimal Fixed Point Combinator	195
<i>Arthur Charguéraud</i>	
Formal Study of Plane Delaunay Triangulation	211
<i>Jean-François Dufourd and Yves Bertot</i>	
Reasoning with Higher-Order Abstract Syntax and Contexts: A Comparison	227
<i>Amy Felty and Brigitte Pientka</i>	
A Trustworthy Monadic Formalization of the ARMv7 Instruction Set Architecture	243
<i>Anthony Fox and Magnus O. Myreen</i>	
Automated Machine-Checked Hybrid System Safety Proofs	259
<i>Herman Geuvers, Adam Koprowski, Dan Synek, and Eelis van der Weegen</i>	
Coverset Induction with Partiality and Subsorts: A Powerlist Case Study	275
<i>Joe Hendrix, Deepak Kapur, and José Meseguer</i>	
Case-Analysis for Rippling and Inductive Proof	291
<i>Moa Johansson, Lucas Dixon, and Alan Bundy</i>	
Importing HOL Light into Coq	307
<i>Chantal Keller and Benjamin Werner</i>	
A Mechanized Translation from Higher-Order Logic to Set Theory	323
<i>Alexander Krauss and Andreas Schropp</i>	
The Isabelle Collections Framework	339
<i>Peter Lammich and Andreas Lochbihler</i>	
Interactive Termination Proofs Using Termination Cores	355
<i>Panagiotis Manolios and Daron Vroon</i>	
A Framework for Formal Verification of Compiler Optimizations	371
<i>William Mansky and Elsa Gunter</i>	

On the Formalization of the Lebesgue Integration Theory in HOL	387
<i>Tarek Mhamdi, Osman Hasan, and Sofiène Tahar</i>	
From Total Store Order to Sequential Consistency: A Practical Reduction Theorem	403
<i>Ernie Cohen and Bert Schirmer</i>	
Equations: A Dependent Pattern-Matching Compiler	419
<i>Matthieu Sozeau</i>	
A Mechanically Verified AIG-to-BDD Conversion Algorithm	435
<i>Sol Swords and Warren A. Hunt Jr</i>	
Inductive Consequences in the Calculus of Constructions	450
<i>Daria Walukiewicz-Chrzaszcz and Jacek Chrzaszcz</i>	
Validating QBF Invalidity in HOL4	466
<i>Tjark Weber</i>	
Rough Diamonds	
Higher-Order Abstract Syntax in Isabelle/HOL	481
<i>Douglas J. Howe</i>	
Separation Logic Adapted for Proofs by Rewriting	485
<i>Magnus O. Myreen</i>	
Developing the Algebraic Hierarchy with Type Classes in Coq	490
<i>Bas Spitters and Eelis van der Weegen</i>	
Author Index	495