

*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*

Marko Van Eekelen Herman Geuvers  
Julien Schmaltz Freek Wiedijk (Eds.)

# Interactive Theorem Proving

Second International Conference, ITP 2011  
Berg en Dal, The Netherlands, August 22-25, 2011  
Proceedings

## Volume Editors

Marko Van Eekelen  
Open Universiteit, Faculteit Informatica  
Postbus 2960, 6401 DL Heerlen, The Netherlands  
E-mail: marko.vaneekelen@ou.nl

Herman Geuvers  
Radboud Universiteit Nijmegen, FNWI/ICIS/IS  
Postbus 9010, 6500 GL Nijmegen, The Netherlands  
E-mail: herman@cs.ru.nl

Julien Schmaltz  
Open Universiteit, Faculteit Informatica  
Postbus 2960, 6401 DL Heerlen, The Netherlands  
E-mail: julien.schmaltz@ou.nl

Freek Wiedijk  
Radboud Universiteit Nijmegen, FNWI/ICIS/IS  
Postbus 9010, 6500 GL Nijmegen, The Netherlands  
E-mail: freek@cs.ru.nl

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-22862-9 e-ISBN 978-3-642-22863-6  
DOI 10.1007/978-3-642-22863-6  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011933581

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

© Springer-Verlag Berlin Heidelberg 2011

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](http://www.springer.com))

# Preface

This volume contains the papers presented at ITP 2011: the Second International Conference on Interactive Theorem Proving. It was held during August 22–25, 2011 in Bergen Dal, The Netherlands.

ITP brings together researchers working in all areas of interactive theorem proving. ITP is the evolution of the TPHOLs conference series to the broad field of interactive theorem proving. The inaugural meeting of ITP was held during July 11–14, 2010 in Edinburgh, Scotland, as part of the Federated Logic Conference (FLoC, July 9–21, 2010). TPHOLs meetings took place every year from 1988 until 2009.

There were 50 submissions to ITP 2011, each of which was reviewed by at least four Program Committee members. Out of the 50 submissions, 42 were regular papers and 8 were rough diamonds. The Program Committee accepted 21 regular papers, including one proof pearl and four rough diamonds. All 25 papers are included in the proceedings. The Program Committee also invited two leading researchers from Industry, Georges Gonthier (Microsoft Research) and Mike Kishinevsky (Intel Corporation), and two leading researchers from academia, Don Batory (University of Texas at Austin) and Bart Jacobs (Radboud University Nijmegen), to present invited lectures.

Two system demos were given at ITP 2011. Each demo consisted in an in-depth presentation of 90 minutes about the application of an ITP system on a real example. Details about the practical use of ACL2 and KeY were presented.

ITP 2011 featured seven associated workshops that took place on August 26 and August 27. The workshops were the following: The Third Coq Workshop, the Third Workshop on Dependently Typed Programming, the 10th KeY Symposium, the 6th International Workshop on Logical Frameworks and Meta-Languages: Theory and Practice, the ITP 2011 Workshop on Mathematical Wikis, the Third Workshop on Modules and Libraries for Proof Assistants, the 6th International Workshop on Systems Software Verification.

We would like to thank our Local Chair Nicole Messink for the valuable and efficient support in planning and running ITP. We would like to thank all the local organizers for their help during the event.

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 ITP 2010 and TPHOLs and its predecessors since 1993.

Finally, we would like to thank our sponsors: The Netherlands Organisation for Scientific Research (NWO) and The Royal Netherlands Academy of Arts and Sciences (KNAW).

June 2011

Herman Geuvers  
Freek Wiedijk  
Marko Van Eekelen  
Julien Schmaltz

# Organization

## Program Committee

David Aspinall	University of Edinburgh, UK
Jeremy Avigad	Carnegie Mellon University, USA
Stefan Berghofer	Technische Universität München, Germany
Yves Bertot	INRIA, France
Sandrine Blazy	IRISA - Université Rennes 1, France
Jens Brandt	University of Kaiserslautern, Germany
Jared Davis	The University of Texas at Austin, USA
Amy Felty	University of Ottawa, Canada
Jean-Christophe Filliâtre	CNRS, France
Herman Geuvers	Radboud University Nijmegen, The Netherlands
Elsa Gunther	University of Illinois at Urbana-Champaign, USA
John Harrison	Intel Corporation, USA
Reiner Hähnle	Chalmers University of Technology, Sweden
Matt Kaufmann	University of Texas at Austin, USA
Gerwin Klein	NICTA and UNSW, Australia
Assia Mahboubi	INRIA Saclay – Île-de-France, France
Panagiotis Manolios	Northeastern University, USA
John Matthews	Galois Connections, Inc., USA
Paul Miner	NASA, USA
J Moore	University of Texas at Austin, USA
Greg Morrisett	Harvard University, USA
Magnus O. Myreen	University of Cambridge, UK
Tobias Nipkow	Technische Universität München, Germany
Michael Norrish	NICTA, Australia
Sam Owre	SRI International, USA
Christine Paulin-Mohring	Université Paris-Sud, France
Lawrence Paulson	University of Cambridge, UK
Brigitte Pientka	McGill University, Canada
Lee Pike	Galois, Inc., USA
Sandip Ray	University of Texas at Austin, USA
Jose-Luis Ruiz-Reina	University of Seville, Spain
David Russinoff	AMD, USA
Julien Schmaltz	Open University of The Netherlands / Radboud University Nijmegen, The Netherlands
Konrad Slind	Rockwell Collins Advanced Technology Center

Sofiène Tahar  
Marko Van Eekelen

Makarius Wenzel  
Freek Wiedijk

Concordia University, Canada  
Radboud University Nijmegen,  
The Netherlands  
University of Paris Sud, France  
Radboud University Nijmegen,  
The Netherlands

## Additional Reviewers

Abbasi, Naeem  
Ahrendt, Wolfgang  
Akbarpour, Behzad  
Andronick, June  
Baelde, David  
Bai, Yu  
Bardou, Romain  
Bobot, Francois  
Boespflug, Mathieu  
Bosma, Wieb  
Campbell, Brian  
Cave, Andrew  
Chamarthi, Harsh Raju  
Cohen, Cyril  
Contejean, Evelyne  
Delahaye, David  
Diatchki, Iavor  
Dixon, Lucas  
Erkok, Levent  
Forest, Julien  
Goodloe, Alwyn  
Gunter, Elsa  
Hasan, Osman  
Hendrix, Joe  
Herencia-Zapana, Heber  
Huffman, Brian  
Hurd, Joe  
Jain, Mitesh  
Ji, Ran  
Kersten, Rody  
Khan-Afshar, Sanaz  
Klebanov, Vladimir  
Krauss, Alexander  
Kunz, César  
Lensink, Leonard

Liu, Hanbing  
Longuet, Delphine  
Madlener, Ken  
Maier, Patrick  
Martin-Mateos, Francisco-Jesus  
McKinna, James  
Mhamdi, Tarek  
Munoz, Cesar  
Naumann, David  
Papavasileiou, Vasilis  
Pasca, Ioana  
Pollack, Randy  
Popescu, Andrei  
Pottier, Loïc  
Preoteasa, Viorel  
Rager, David  
Rutten, Luc  
Sacchini, Jorge Luis  
Schaefer, Ina  
Schfer, Jan  
Seidel, Peter-Michael  
Sewell, Thomas  
Shankar  
Smetsers, Sjaak  
Spitters, Bas  
Starostin, Artem  
Tankink, Carst  
Tews, Hendrik  
Théry, Laurent  
Urban, Christian  
Verbeek, Freek  
Weber, Tjark  
Whiteside, Iain  
Winwood, Simon  
Wolff, Burkhardt

# Table of Contents

## Invited Papers

Towards Verification of Product Lines (Abstract) . . . . .	1
<i>Don Batory</i>	
Advances in the Formalization of the Odd Order Theorem . . . . .	2
<i>Georges Gonthier</i>	
Logical Formalisation and Analysis of the Mifare Classic Card in PVS . . . . .	3
<i>Bart Jacobs and Ronny Wichers Schreur</i>	
Challenges in Verifying Communication Fabrics . . . . .	18
<i>Michael Kishinevsky, Alexander Gotmanov, and Yuriy Viktorov</i>	

## Regular Papers

Verifying Object-Oriented Programs with Higher-Order Separation Logic in Coq . . . . .	22
<i>Jesper Bengtson, Jonas Braband Jensen, Filip Sieczkowski, and Lars Birkedal</i>	
Relational Decomposition . . . . .	39
<i>Lennart Beringer</i>	
Structural Analysis of Narratives with the Coq Proof Assistant . . . . .	55
<i>Anne-Gwenn Bosser, Pierre Courtieu, Julien Forest, and Marc Cavazza</i>	
Towards Robustness Analysis Using PVS . . . . .	71
<i>Renaud Clavel, Laurence Pierre, and Régis Leveugle</i>	
Verified Synthesis of Knowledge-Based Programs in Finite Synchronous Environments . . . . .	87
<i>Peter Gammie</i>	
Point-Free, Set-Free Concrete Linear Algebra . . . . .	103
<i>Georges Gonthier</i>	
A Formalization of Polytime Functions . . . . .	119
<i>Sylvain Heraud and David Nowak</i>	
Three Chapters of Measure Theory in Isabelle/HOL . . . . .	135
<i>Johannes Hölzl and Armin Heller</i>	



Termination of Isabelle Functions via Termination of Rewriting . . . . .	152
<i>Alexander Krauss, Christian Sternagel, René Thiemann, Carsten Fuhs, and Jürgen Giesl</i>	
Validating QBF Validity in HOL4 . . . . .	168
<i>Ramana Kumar and Tjark Weber</i>	
Proving Valid Quantified Boolean Formulas in HOL Light . . . . .	184
<i>Ondřej Kunčar</i>	
Applying ACL2 to the Formalization of Algebraic Topology: Simplicial Polynomials . . . . .	200
<i>Laureano Lambán, Francisco-Jesús Martín-Mateos, Julio Rubio, and Jose-Luis Ruiz-Reina</i>	
Animating the Formalised Semantics of a Java-Like Language . . . . .	216
<i>Andreas Lochbihler and Lukas Bulwahn</i>	
Formalization of Entropy Measures in HOL . . . . .	233
<i>Tarek Mhamdi, Osman Hasan, and Sofiène Tahar</i>	
On the Generation of Positivstellensatz Witnesses in Degenerate Cases . . . . .	249
<i>David Monniaux and Pierre Corbineau</i>	
A Verified Runtime for a Verified Theorem Prover . . . . .	265
<i>Magnus O. Myreen and Jared Davis</i>	
Verified Efficient Enumeration of Plane Graphs Modulo Isomorphism . . .	281
<i>Tobias Nipkow</i>	
Mechanised Computability Theory . . . . .	297
<i>Michael Norrish</i>	
Automatic Differentiation in ACL2 . . . . .	312
<i>Peter Reid and Ruben Gamboa</i>	
seL4 Enforces Integrity . . . . .	325
<i>Thomas Sewell, Simon Winwood, Peter Gammie, Toby Murray, June Andronick, and Gerwin Klein</i>	

## Proof Pearls

A Formalisation of the Myhill-Nerode Theorem Based on Regular Expressions (Proof Pearl) . . . . .	341
<i>Chunhan Wu, Xingyuan Zhang, and Christian Urban</i>	

**Rough Diamonds**

LCF-Style Bit-Blasting in HOL4 .....	357
<i>Anthony C.J. Fox</i>	
Lem: A Lightweight Tool for Heavyweight Semantics .....	363
<i>Scott Owens, Peter Böhm, Francesco Zappa Nardelli, and Peter Sewell</i>	
Composable Discovery Engines for Interactive Theorem Proving .....	370
<i>Phil Scott and Jacques Fleuriot</i>	
Heterogeneous Proofs: Spider Diagrams Meet Higher-Order Provers ....	376
<i>Matej Urbas and Mateja Jamnik</i>	
<b>Author Index</b> .....	<b>383</b>