Preface


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 Austing) 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
Sofi`ene 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
Hendrix, 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, Burkhart
# Table of Contents

## Invited Papers

Towards Verification of Product Lines (Abstract) ............................................. 1  
*Don Batory*

Advances in the Formalization of the Odd Order Theorem ............................. 2  
*Georges Gonthier*

Logical Formalisation and Analysis of the Mifare Classic Card in PVS ............... 3  
*Bart Jacobs and Ronny Wichers Schreur*

Challenges in Verifying Communication Fabrics ......................................... 18  
*Micahel Kishinevsky, Alexander Gotmanov, and Yuriy Viktorov*

## Regular Papers

Verifying Object-Oriented Programs with Higher-Order Separation Logic in Coq .......................................................... 22  
*Jesper Bengtson, Jonas Braband Jensen, Filip Sieczkowski, and Lars Birkedal*

Relational Decomposition ............................................................................. 39  
*Lennart Beringer*

Structural Analysis of Narratives with the Coq Proof Assistant ......................... 55  
*Anne-Gwenn Bosser, Pierre Courtieu, Julien Forest, and Marc Cavazza*

Towards Robustness Analysis Using PVS ..................................................... 71  
*Renaud Clavel, Laurence Pierre, and Régis Leveugle*

Verified Synthesis of Knowledge-Based Programs in Finite Synchronous Environments ............................................................... 87  
*Peter Gammie*

Point-Free, Set-Free Concrete Linear Algebra .............................................. 103  
*Georges Gonthier*

A Formalization of Polytime Functions ......................................................... 119  
*Sylvain Heraud and David Nowak*

Three Chapters of Measure Theory in Isabelle/HOL ..................................... 135  
*Johannes Hölzle and Armin Heller*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Termination of Isabelle Functions via Termination of Rewriting</td>
<td>152</td>
</tr>
<tr>
<td>Alexander Krauss, Christian Sternagel, René Thiemann, Carsten Fuhs,</td>
<td></td>
</tr>
<tr>
<td>and Jürgen Giesl</td>
<td></td>
</tr>
<tr>
<td>Validating QBF Validity in HOL4</td>
<td>168</td>
</tr>
<tr>
<td>Ramana Kumar and Tjark Weber</td>
<td></td>
</tr>
<tr>
<td>Proving Valid Quantified Boolean Formulas in HOL Light</td>
<td>184</td>
</tr>
<tr>
<td>Ondřej Kunčar</td>
<td></td>
</tr>
<tr>
<td>Applying ACL2 to the Formalization of Algebraic Topology: Simplicial</td>
<td>200</td>
</tr>
<tr>
<td>Polynomials</td>
<td></td>
</tr>
<tr>
<td>Laureano Lambán, Francisco-Jesús Martín–Mateos, Julio Rubio, and</td>
<td></td>
</tr>
<tr>
<td>José-Luis Ruiz–Reina</td>
<td></td>
</tr>
<tr>
<td>Animating the Formalised Semantics of a Java-Like Language</td>
<td>216</td>
</tr>
<tr>
<td>Andreas Lochbihler and Lukas Bulwahn</td>
<td></td>
</tr>
<tr>
<td>Formalization of Entropy Measures in HOL</td>
<td>233</td>
</tr>
<tr>
<td>Tarek Mhamdi, Osman Hasan, and Sofiène Tahar</td>
<td></td>
</tr>
<tr>
<td>On the Generation of Positivstellensatz Witnesses in Degenerate Cases</td>
<td>249</td>
</tr>
<tr>
<td>David Monniaux and Pierre Corbineau</td>
<td></td>
</tr>
<tr>
<td>A Verified Runtime for a Verified Theorem Prover</td>
<td>265</td>
</tr>
<tr>
<td>Magnus O. Myreen and Jared Davis</td>
<td></td>
</tr>
<tr>
<td>Verified Efficient Enumeration of Plane Graphs Modulo Isomorphism</td>
<td>281</td>
</tr>
<tr>
<td>Tobias Nipkow</td>
<td></td>
</tr>
<tr>
<td>Mechanised Computability Theory</td>
<td>297</td>
</tr>
<tr>
<td>Michael Norrish</td>
<td></td>
</tr>
<tr>
<td>Automatic Differentiation in ACL2</td>
<td>312</td>
</tr>
<tr>
<td>Peter Reid and Ruben Gamboa</td>
<td></td>
</tr>
<tr>
<td>seL4 Enforces Integrity</td>
<td>325</td>
</tr>
<tr>
<td>Thomas Sewell, Simon Winwood, Peter Gammie, Toby Murray, June</td>
<td></td>
</tr>
<tr>
<td>Andronick, and Gerwin Klein</td>
<td></td>
</tr>
<tr>
<td>Proof Pearls</td>
<td></td>
</tr>
<tr>
<td>A Formalisation of the Myhill-Nerode Theorem Based on Regular</td>
<td>341</td>
</tr>
<tr>
<td>Expressions (Proof Pearl)</td>
<td></td>
</tr>
<tr>
<td>Chunhan Wu, Xingyuan Zhang, and Christian Urban</td>
<td></td>
</tr>
</tbody>
</table>
Rough Diamonds

LCF-Style Bit-Blasting in HOL4 ........................................... 357
Anthony C.J. Fox

Lem: A Lightweight Tool for Heavyweight Semantics ............... 363
Scott Owens, Peter Böhm, Francesco Zappa Nardelli, and Peter Sewell

Composable Discovery Engines for Interactive Theorem Proving .... 370
Phil Scott and Jacques Fleuriot

Heterogeneous Proofs: Spider Diagrams Meet Higher-Order Provers .... 376
Matej Urbas and Mateja Jamnik

Author Index ................................................................. 383