

10th International Conference on Interactive Theorem Proving

ITP 2019, September 9–12, 2019, Portland, OR, USA

Edited by

John Harrison

John O’Leary

Andrew Tolmach



Editors

John Harrison

Amazon AWS, Portland, OR, USA
jrh013@gmail.com

John O'Leary

Intel Corporation, Hillsboro, Oregon, USA
john.w.oleary@intel.com

Andrew Tolmach

Portland State University, Portland, OR, USA
tolmach@pdx.edu

ACM Classification 2012

Theory of computation → Logic

ISBN 978-3-95977-122-1

Published online and open access by

Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at <https://www.dagstuhl.de/dagpub/978-3-95977-122-1>.

Publication date

September, 2019

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at <https://portal.dnb.de>.

License

This work is licensed under a Creative Commons Attribution 3.0 Unported license (CC-BY 3.0):
<https://creativecommons.org/licenses/by/3.0/legalcode>.



In brief, this license authorizes each and everybody to share (to copy, distribute and transmit) the work under the following conditions, without impairing or restricting the authors' moral rights:

- Attribution: The work must be attributed to its authors.

The copyright is retained by the corresponding authors.

Digital Object Identifier: 10.4230/LIPIcs.ITP.2019.0

ISBN 978-3-95977-122-1

ISSN 1868-8969

<https://www.dagstuhl.de/lipics>

LIPICs – Leibniz International Proceedings in Informatics

LIPICs is a series of high-quality conference proceedings across all fields in informatics. LIPICs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

Editorial Board

- Luca Aceto (*Chair*, Gran Sasso Science Institute and Reykjavik University)
- Christel Baier (TU Dresden)
- Mikolaj Bojanczyk (University of Warsaw)
- Roberto Di Cosmo (INRIA and University Paris Diderot)
- Javier Esparza (TU München)
- Meena Mahajan (Institute of Mathematical Sciences)
- Dieter van Melkebeek (University of Wisconsin-Madison)
- Anca Muscholl (University Bordeaux)
- Luke Ong (University of Oxford)
- Catuscia Palamidessi (INRIA)
- Thomas Schwentick (TU Dortmund)
- Raimund Seidel (Saarland University and Schloss Dagstuhl – Leibniz-Zentrum für Informatik)

ISSN 1868-8969

<https://www.dagstuhl.de/lipics>

■ Contents

Preface	
<i>John Harrison, John O’Leary, and Andrew Tolmach</i>	0:ix

Invited Talks

A Million Lines of Proof About a Moving Target	
<i>June Andronick</i>	1:1–1:1
What Makes a Mathematician Tick?	
<i>Kevin Buzzard</i>	2:1–2:1
An Increasing Need for Formality	
<i>Martin Dixon</i>	3:1–3:1

Regular Papers

A Verified Compositional Algorithm for AI Planning	
<i>Mohammad Abdulaziz, Charles Gretton, and Michael Norrish</i>	4:1–4:19
Proving Tree Algorithms for Succinct Data Structures	
<i>Reynald Affeldt, Jacques Garrigue, Xuanrui Qi, and Kazunari Tanaka</i>	5:1–5:19
Data Types as Quotients of Polynomial Functors	
<i>Jeremy Avigad, Mario Carneiro, and Simon Hudon</i>	6:1–6:19
Primitive Floats in Coq	
<i>Guillaume Bertholon, Érik Martin-Dorel, and Pierre Roux</i>	7:1–7:20
A Certificate-Based Approach to Formally Verified Approximations	
<i>Florent Bréhard, Assia Mahboubi, and Damien Pous</i>	8:1–8:19
Higher-Order Tarski Grothendieck as a Foundation for Formal Proof	
<i>Chad E. Brown, Cezary Kaliszzyk, and Karol Pqk</i>	9:1–9:16
Generic Authenticated Data Structures, Formally	
<i>Matthias Brun and Dmitriy Traytel</i>	10:1–10:18
A Verified and Compositional Translation of LTL to Deterministic Rabin Automata	
<i>Julian Brunner, Benedikt Seidl, and Salomon Sickert</i>	11:1–11:19
Formalizing Computability Theory via Partial Recursive Functions	
<i>Mario Carneiro</i>	12:1–12:17
Formal Proofs of Tarjan’s Strongly Connected Components Algorithm in Why3, Coq and Isabelle	
<i>Ran Chen, Cyril Cohen, Jean-Jacques Lévy, Stephan Merz, and Laurent Théry</i> ...	13:1–13:19
First-Order Guarded Coinduction in Coq	
<i>Lukasz Czajka</i>	14:1–14:18

10th International Conference on Interactive Theorem Proving (ITP 2019).

Editors: John Harrison, John O’Leary, and Andrew Tolmach

Leibniz International Proceedings in Informatics



Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Formalizing the Solution to the Cap Set Problem <i>Sander R. Dahmen, Johannes Hölzl, and Robert Y. Lewis</i>	15:1–15:19
Nine Chapters of Analytic Number Theory in Isabelle/HOL <i>Manuel Eberl</i>	16:1–16:19
A Certifying Extraction with Time Bounds from Coq to Call-By-Value λ -Calculus <i>Yannick Forster and Fabian Kunze</i>	17:1–17:19
Formal Proof and Analysis of an Incremental Cycle Detection Algorithm <i>Armaël Guéneau, Jacques-Henri Jourdan, Arthur Charguéraud, and François Pottier</i>	18:1–18:20
A Formalization of Forcing and the Unprovability of the Continuum Hypothesis <i>Jesse Michael Han and Floris van Doorn</i>	19:1–19:19
Refinement with Time – Refining the Run-Time of Algorithms in Isabelle/HOL <i>Maximilian P. L. Haslbeck and Peter Lammich</i>	20:1–20:18
Virtualization of HOL4 in Isabelle <i>Fabian Immler, Jonas Rädle, and Makarius Wenzel</i>	21:1–21:18
Generating Verified LLVM from Isabelle/HOL <i>Peter Lammich</i>	22:1–22:19
Proof Pearl: Purely Functional, Simple and Efficient Priority Search Trees and Applications to Prim and Dijkstra <i>Peter Lammich and Tobias Nipkow</i>	23:1–23:18
A Verified LL(1) Parser Generator <i>Sam Lasser, Chris Casinghino, Kathleen Fisher, and Cody Roux</i>	24:1–24:18
Binary-Compatible Verification of Filesystems with ACL2 <i>Mihir Parang Mehta and William R. Cook</i>	25:1–25:18
Ornaments for Proof Reuse in Coq <i>Talia Ringer, Nathaniel Yazdani, John Leo, and Dan Grossman</i>	26:1–26:19
Verifying That a Compiler Preserves Concurrent Value-Dependent Information-Flow Security <i>Robert Sison and Toby Murray</i>	27:1–27:19
Quantitative Continuity and Computable Analysis in COQ <i>Florian Steinberg, Laurent Théry, and Holger Thies</i>	28:1–28:21
Deriving Proved Equality Tests in Coq-Elpi: Stronger Induction Principles for Containers in Coq <i>Enrico Tassi</i>	29:1–29:18
Complete Non-Orders and Fixed Points <i>Akihisa Yamada and Jérémy Dubut</i>	30:1–30:16
Verified Decision Procedures for Modal Logics <i>Minchao Wu and Rajeev Goré</i>	31:1–31:19
Characteristic Formulae for Liveness Properties of Non-Terminating CakeML Programs <i>Johannes Áman Pohjola, Henrik Rostedt, and Magnus O. Myreen</i>	32:1–32:19

Short Papers

The DPRM Theorem in Isabelle <i>Jonas Bayer, Marco David, Abhik Pal, Benedikt Stock, and Dierk Schleicher</i>	33:1–33:7
Hammering Mizar by Learning Clause Guidance <i>Jan Jakubův and Josef Urban</i>	34:1–34:8
Declarative Proof Translation <i>Cezary Kaliszyk and Karol Pqk</i>	35:1–35:7
Formalization of the Domination Chain with Weighted Parameters <i>Daniel E. Severín</i>	36:1–36:7

■ Preface

The International Conference on Interactive Theorem Proving (ITP) is the main venue for the presentation of research into interactive theorem proving frameworks and their applications. It has evolved organically starting with a HOL workshop back in 1988, gradually widening to include other higher-order systems and interactive theorem provers generally, as well as their applications. This year's conference, in Portland OR, USA, is the tenth to be held under the ITP name, following Edinburgh 2010, Nijmegen 2011, Princeton 2012, Rennes 2013, Vienna 2014, Nanjing 2015, Nancy 2016, Brasilia 2017 and Oxford 2018; those in 2010, 2014 and 2018 were under the umbrella organization of the Federated Logic Conference (FLoC).

This year's conference attracted a total of 72 submissions (61 long papers and 11 short papers); with the exception of the very first ITP in 2010 (which received 74 submissions) this is the largest number of submissions received by ITP or its predecessor conferences. Each paper was systematically reviewed by at least three program committee members or appointed external reviewers, as a result of which the PC winnowed down the selection to be presented at the conference: 33 papers (29 long papers and 4 short). As a consequence of limited time for presentation at the conference, many interesting papers had to be rejected. We thank the authors of both accepted and rejected papers for their submissions, as well as the PC members and external reviewers for their invaluable work.

As well as all the regular papers, we are very pleased to have invited keynote talks by June Andronick (Data 61, CSIRO), Kevin Buzzard (Imperial College) and Martin Dixon (Intel).

The present volume collects all the accepted papers contributed to the conference as well as abstracts of the three invited presentations. This year, for the first time, we are publishing the proceedings in the LIPIcs series, motivated by its commitment to open access. We thank all those at Dagstuhl for their responsive feedback on all matters associated with the production of the finished proceedings.

Finally, we are grateful to Portland State University for logistical support, to several corporate donors who helped to support the conference, and to the ITP Steering Committee for their guidance throughout.

July 2019

John Harrison
John O'Leary
Andrew Tolmach



■ Program Committee

Andreas Abel	Gothenburg University, Sweden
David Aspinall	The University of Edinburgh, Scotland
Jeremy Avigad	Carnegie Mellon University, USA
Mauricio Ayala-Rincon	Universidade de Brasilia, Brasil
Yves Bertot	Inria, France
Sandrine Blazy	University of Rennes 1 – IRISA, France
Arthur Charguéraud	Inria, France
Koen Claessen	Chalmers University of Technology, Sweden
Gilles Dowek	Inria and ENS Paris-Saclay, France
Amy Felty	University of Ottawa, Canada
Jean-Christophe Filliatre	CNRS, France
Ruben Gamboa	University of Wyoming, USA
Shilpi Goel	Centaur Technology, Inc., USA
John Harrison	Amazon AWS, USA (co-chair)
Jean-Baptiste Jeannin	University of Michigan, USA
Cezary Kaliszyk	University of Innsbruck, Austria
Gerwin Klein	Data61, CSIRO and UNSW Sydney, Australia
Joe Leslie-Hurd	Intel, USA
Assia Mahboubi	Inria, France
Guillaume Melquiond	Inria, France
Leonardo de Moura	Microsoft, USA
Magnus Myreen	Chalmers University of Technology, Sweden
Tobias Nipkow	Technical University of Munich, Germany
John O’Leary	Intel, USA (co-chair)
Sam Owre	SRI, USA
Lawrence Paulson	University of Cambridge, UK
Christine Rizkallah	UNSW Sydney, Australia
Alexey Solovyev	Independent mobile software developer
Sofiene Tahar	Concordia University, Canada
Andrew Tolmach	Portland State University, USA (co-chair)
Christian Urban	King’s College London, UK
Josef Urban	Czech Technical University in Prague, Czech Republic



■ External Reviewers

Waqar Ahmad
Asad Ahmed
Idir Ait Sadoune
Ariane A. Almeida
Sidney Amani
Callum Bannister
Lasse Blaauwbroek
Chad Brown
Ali Bukhari
David Butler
Evelyne Contejean
Pierre-Evariste Dagand
Thaynara Arielly de Lima
Flavio L. C. De Moura
Larry Diehl
Christian Doczkal
Simon Doherty
Yannick Forster
Thibault Gauthier
Amjad Gawanmeh
Georges Gonthier
Ganesh Gopalakrishnan
Benjamin Gregoire
Maximilian Paul Louis Haslbeck
Ahmed Irfan
Guilhem Jabber
Jacques-Henri Jourdan
Manfred Kerber
Quentin Ladeveze
Peter Lammich
Xavier Leroy
Michael McInerney
Michael Norrish
Julian Parsert
Edward Pierzchalski
Nir Piterman
Johannes Åman Pohjola
Andrei Popescu
Thiago Mendonça Ferreira Ramos
Adnan Rashid
Thomas Sewell
Umair Siddique
Marielle Stoelinga
Rob Sumners
René Thiemann
Alwen Tiu
Aaron Tomb
Prathamesh Turaga
Vincent Van Oostrom
Marco Vassena



