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

John Harrison, John O’Leary, and Andrew Tolmach ............................... 0.ix

Invited Talks

A Million Lines of Proof About a Moving Target
June Andronick .............................................................................. 1:1–1:1

What Makes a Mathematician Tick?
Kevin Buzzard .................................................................................. 2:1–2:1

An Increasing Need for Formality
Martin Dixon ...................................................................................... 3:1–3:1

Regular Papers

A Verified Compositional Algorithm for AI Planning
Mohammad Abdulaziz, Charles Gretton, and Michael Norrish ................. 4:1–4:19

Proving Tree Algorithms for Succinct Data Structures
Reynald Affeldt, Jacques Garrigue, Xuanrui Qi, and Kazunari Tanaka ......... 5:1–5:19

Data Types as Quotients of Polynomial Functors
Jeremy Avigad, Mario Carneiro, and Simon Hudon ................................. 6:1–6:19

Primitive Floats in Coq
Guillaume Bertholon, Érik Martin-Dorel, and Pierre Roux ....................... 7:1–7:20

A Certificate-Based Approach to Formally Verified Approximations
Florent Bréhard, Assia Mahboubi, and Damien Pous .............................. 8:1–8:19

Higher-Order Tarski Grothendieck as a Foundation for Formal Proof
Chad E. Brown, Cezary Kaliszyk, and Karol Pąk .................................. 9:1–9:16

Generic Authenticated Data Structures, Formally
Matthias Brun and Dmitriy Traytel .................................................... 10:1–10:18

A Verified and Compositional Translation of LTL to
Deterministic Rabin Automata
Julian Brummer, Benedikt Seidl, and Salomon Sickert .............................. 11:1–11:19

Formalizing Computability Theory via Partial Recursive Functions
Mario Carneiro ................................................................................... 12:1–12:17

Formal Proofs of Tarjan’s Strongly Connected Components Algorithm in Why3,
Coq and Isabelle
Ran Chen, Cyril Cohen, Jean-Jacques Lévy, Stephan Merz, and Laurent Théry ... 13:1–13:19

First-Order Guarded Coinduction in Coq
Łukasz Czajka .................................................................................... 14:1–14:18
Contents

Formalizing the Solution to the Cap Set Problem

Nine Chapters of Analytic Number Theory in Isabelle/HOL
   Manuel Eberl ................................................................. 16:1–16:19

A Certifying Extraction with Time Bounds from Coq to Call-By-Value \( \lambda \)-Calculus
   Yannick Forster and Fabian Kanze ....................................... 17:1–17:19

Formal Proof and Analysis of an Incremental Cycle Detection Algorithm
   Arnaël Guéneau, Jacques-Henri Jourdan, Arthur Charguéraud, and
   François Pottier .......................................................... 18:1–18:20

A Formalization of Forcing and the Unprovability of the Continuum Hypothesis
   Jesse Michael Han and Floris van Doorn ............................ 19:1–19:19

Refinement with Time – Refining the Run-Time of Algorithms in Isabelle/HOL
   Maximilian P. L. Haslbeck and Peter Lammich .......................... 20:1–20:18

Virtualization of HOL4 in Isabelle
   Fabian Immler, Jonas Rädle, and Makarius Wenzel ...................... 21:1–21:18

Generating Verified LLVM from Isabelle/HOL
   Peter Lammich ............................................................. 22:1–22:19

Proof Pearl: Purely Functional, Simple and Efficient Priority Search Trees and
Applications to Prim and Dijkstra
   Peter Lammich and Tobias Nipkow ..................................... 23:1–23:18

A Verified LL(1) Parser Generator
   Sam Lasser, Chris Casinghino, Kathleen Fisher, and Cody Roux ........ 24:1–24:18

Binary-Compatible Verification of Filesystems with ACL2
   Mihir Parang Mehta and William R. Cook ............................... 25:1–25:18

Ornaments for Proof Reuse in Coq
   Talia Ringer, Nathaniel Yazdani, John Leo, and Dan Grossman ........ 26:1–26:19

Verifying That a Compiler Preserves Concurrent Value-Dependent
Information-Flow Security
   Robert Sison and Toby Murray .......................................... 27:1–27:19

Quantitative Continuity and Computable Analysis in Coq
   Florian Steinberg, Laurent Théry, and Holger Thies .................. 28:1–28:21

Deriving Proved Equality Tests in Coq-Elpi: Stronger Induction Principles for
Containers in Coq
   Enrico Tassi ............................................................... 29:1–29:18

Complete Non-Orders and Fixed Points
   Akihisa Yamada and Jérémy Dubut ..................................... 30:1–30:16

Verified Decision Procedures for Modal Logics
   Minchao Wu and Rajeev Goré ........................................... 31:1–31:19

Characteristic Formulae for Liveness Properties of Non-Terminating
CakeML Programs
   Johannes Åman Pohjola, Henrik Rostedt, and Magnus O. Myreen ....... 32:1–32:19
Short Papers

The DPRM Theorem in Isabelle
   Jonas Bayer, Marco David, Abhik Pal, Benedikt Stock, and Dierk Schleicher ...... 33:1–33:7

Hammering Mizar by Learning Clause Guidance
   Jan Jakubův and Josef Urban ................................................ 34:1–34:8

Declarative Proof Translation
   Cezary Kaliszyk and Karol Pąk .............................................. 35:1–35:7

Formalization of the Domination Chain with Weighted Parameters
   Daniel E. Severín .............................................................. 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 Blaauboer
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 Pierzhalski
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