

14th International Conference on Interactive Theorem Proving

ITP 2023, July 31 to August 4, 2023, Białystok, Poland

Edited by

Adam Naumowicz

René Thiemann



Editors

Adam Naumowicz 

University of Białystok, Poland
adamn@math.uwb.edu.pl

René Thiemann 

University of Innsbruck, Austria
rene.thiemann@uibk.ac.at

ACM Classification 2012

Theory of computation → Interactive proof systems; Theory of computation → Higher order logic; Software and its engineering → Formal methods; Theory of computation → Program reasoning; Computing methodologies → Theorem proving algorithms

ISBN 978-3-95977-284-6

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/978-3-95977-284-6>.

Publication date

July, 2023

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 4.0 International license (CC-BY 4.0):
<https://creativecommons.org/licenses/by/4.0/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.2023.0

ISBN 978-3-95977-284-6

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*, Reykjavik University, IS and Gran Sasso Science Institute, IT)
- Christel Baier (TU Dresden, DE)
- Mikolaj Bojanczyk (University of Warsaw, PL)
- Roberto Di Cosmo (Inria and Université de Paris, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Daniel Král' (Masaryk University - Brno, CZ)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN)
- Anca Muscholl (University of Bordeaux, FR)
- Chih-Hao Luke Ong (University of Oxford, GB and Nanyang Technological University, SG)
- Phillip Rogaway (University of California, Davis, US)
- Eva Rotenberg (Technical University of Denmark, Lyngby, DK)
- Raimund Seidel (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)

ISSN 1868-8969

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

■ Contents

Preface	
<i>Adam Naumowicz and René Thiemann</i>	0:ix

Invited Talks

Formalisation of Additive Combinatorics in Isabelle/HOL	
<i>Angeliki Koutsoukou-Argyraiki</i>	1:1–1:2
Interactive and Automated Proofs in Modal Separation Logic	
<i>Robbert Krebbers</i>	2:1–2:1

Regular Papers

A Formal Analysis of RANKING	
<i>Mohammad Abdulaziz and Christoph Madlener</i>	3:1–3:18
Fast, Verified Computation for Candle	
<i>Oskar Abrahamsson and Magnus O. Myreen</i>	4:1–4:17
Formalizing Functions as Processes	
<i>Beniamino Accattoli, Horace Blanc, and Claudio Sacerdoti Coen</i>	5:1–5:21
An Elementary Formal Proof of the Group Law on Weierstrass Elliptic Curves in Any Characteristic	
<i>David Kurniadi Angdinata and Junyan Xu</i>	6:1–6:19
A Proof-Producing Compiler for Blockchain Applications	
<i>Jeremy Avigad, Lior Goldberg, David Levit, Yoav Seginer, and Alon Titelman</i>	7:1–7:19
No Unification Variable Left Behind: Fully Grounding Type Inference for the HDM System	
<i>Roger Bosman, Georgios Karachalias, and Tom Schrijvers</i>	8:1–8:18
Automated Theorem Proving for Metamath	
<i>Mario Carneiro, Chad E. Brown, and Josef Urban</i>	9:1–9:19
Reimplementing Mizar in Rust	
<i>Mario Carneiro</i>	10:1–10:18
Now It Compiles!: Certified Automatic Repair of Uncompilable Protocols	
<i>Luís Cruz-Filipe and Fabrizio Montesi</i>	11:1–11:19
Lessons for Interactive Theorem Proving Researchers from a Survey of Coq Users	
<i>Ana de Almeida Borges, Annalí Casanueva Artís, Jean-Rémy Falleri, Emilio Jesús Gallego Arias, Érik Martin-Dorel, Karl Palmiskog, Alexander Serebrenik, and Théo Zimmermann</i>	12:1–12:18
Formalizing Norm Extensions and Applications to Number Theory	
<i>María Inés de Frutos-Fernández</i>	13:1–13:18

14th International Conference on Interactive Theorem Proving (ITP 2023).

Editors: Adam Naumowicz and René Thiemann



Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Tealeaves: Structured Monads for Generic First-Order Abstract Syntax Infrastructure	
<i>Lawrence Dunn, Val Tannen, and Steve Zdancewic</i>	14:1–14:20
Closure Properties of General Grammars – Formally Verified	
<i>Martin Dvorak and Jasmin Blanchette</i>	15:1–15:16
Formalising Yoneda Ext in Univalent Foundations	
<i>Jarl G. Tøxerås Flaten</i>	16:1–16:17
LISA – A Modern Proof System	
<i>Simon Guilloud, Sankalp Gambhir, and Viktor Kunčák</i>	17:1–17:19
Semantic Foundations of Higher-Order Probabilistic Programs in Isabelle/HOL	
<i>Michikazu Hirata, Yasuhiko Minamide, and Tetsuya Sato</i>	18:1–18:18
MizAR 60 for Mizar 50	
<i>Jan Jakubův, Karel Chvalovský, Zarathustra Goertzel, Cezary Kaliszyk, Mirek Olšák, Bartosz Piotrowski, Stephan Schulz, Martin Suda, and Josef Urban</i> .	19:1–19:22
Constructive Final Semantics of Finite Bags	
<i>Philipp Joram and Niccolò Veltri</i>	20:1–20:19
Proof Pearl: Faithful Computation and Extraction of μ -Recursive Algorithms in Coq	
<i>Dominique Larchey-Wendling and Jean-François Monin</i>	21:1–21:17
Group Cohomology in the Lean Community Library	
<i>Amelia Livingston</i>	22:1–22:17
A Formalisation of Gallagher’s Ergodic Theorem	
<i>Oliver Nash</i>	23:1–23:16
An Extensible User Interface for Lean 4	
<i>Wojciech Nawrocki, Edward W. Ayers, and Gabriel Ebner</i>	24:1–24:20
Bel-Games: A Formal Theory of Games of Incomplete Information Based on Belief Functions in the Coq Proof Assistant	
<i>Pierre Pomeret-Coquot, Hélène Fargier, and Érik Martin-Dorel</i>	25:1–25:19
Proof Repair Infrastructure for Supervised Models: Building a Large Proof Repair Dataset	
<i>Tom Reichel, R. Wesley Henderson, Andrew Touchet, Andrew Gardner, and Talia Ringer</i>	26:1–26:20
POSIX Lexing with Bitcoded Derivatives	
<i>Chengsong Tan and Christian Urban</i>	27:1–27:18
A Sound and Complete Projection for Global Types	
<i>Dawit Tirore, Jesper Bengtson, and Marco Carbone</i>	28:1–28:19
Real-Time Double-Ended Queue Verified (Proof Pearl)	
<i>Balazs Toth and Tobias Nipkow</i>	29:1–29:18
Certifying Higher-Order Polynomial Interpretations	
<i>Niels van der Weide, Deivid Vale, and Cynthia Kop</i>	30:1–30:20

Slice Nondeterminism <i>Niels F. W. Voorneveld</i>	31:1–31:19
Foundational Verification of Stateful P4 Packet Processing <i>Qinshi Wang, Mengying Pan, Shengyi Wang, Ryan Doenges, Lennart Beringer, and Andrew W. Appel</i>	32:1–32:20
Independently Sorted Theorem Proving for Mathematical Foundations <i>Yiming Xu and Michael Norrish</i>	33:1–33:18
Formalizing Results on Directed Sets in Isabelle/HOL (Proof Pearl) <i>Akihisa Yamada and Jérémy Dubut</i>	34:1–34:13
Formalising the <i>Proj</i> Construction in Lean <i>Jujian Zhang</i>	35:1–35:17

Short Papers

Fermat’s Last Theorem for Regular Primes <i>Alex J. Best, Christopher Birkbeck, Riccardo Brasca, and Eric Rodriguez Boidi</i> ...	36:1–36:8
Implementing More Explicit Definitional Expansions in Mizar <i>Adam Grabowski and Artur Kornilowicz</i>	37:1–37:8
Formalizing Almost Development Closed Critical Pairs <i>Christina Kohl and Aart Middeldorp</i>	38:1–38:8

■ 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 takes place in Białystok in Poland. It is hosted by the Mizar group of the University of Białystok. Previous ITP conferences took place in Edinburgh 2010, Nijmegen 2011, Princeton 2012, Rennes 2013, Vienna 2014, Nanjing 2015, Nancy 2016, Brasilia 2017, Oxford 2018, Portland 2019, Paris 2020, Rome 2021 and Haifa 2022; those in 2010, 2014, 2018 and 2022 were under the umbrella organization of the Federated Logic Conference (FLoC).

This year's conference attracted a total of 78 submissions (70 regular papers and 8 short papers). 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: 36 papers (33 regular papers and 3 short papers). 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 talks by Angeliki Koutsoukou-Argyraiki (University of Cambridge) and Robbert Krebbers (Radboud University Nijmegen). The present volume collects all the accepted papers contributed to the conference as well as abstracts of the two invited talks. This is the fourth time that the ITP proceedings are published in the LIPIcs series. We thank all those at Dagstuhl for their responsive feedback on all matters associated with the production of the finished proceedings.

We are grateful to all of the local organizers and thankful to the ITP Steering Committee for their guidance throughout.

Adam Naumowicz and René Thiemann



Organisation

Programme Chairs

Adam Naumowicz	University of Białystok, Poland
René Thiemann	University of Innsbruck, Austria

Programme Committee

Andreas Abel	Jesús Aransay	Jeremy Avigad
Mauricio Ayala-Rincon	Christoph Benz Müller	Jasmin Blanchette
Sandrine Blazy	Sylvie Boldo	Cyril Cohen
Liron Cohen	Luis Cruz-Filipe	Ruben Gamboa
Jason Gross	John Harrison	Hugo Herbelin
Cezary Kaliszyk	Chantal Keller	Peter Lammich
Andreas Lochbihler	Marco Maggesi	Assia Mahboubi
Magnus O. Myreen	Cláudia Nalon	Tobias Nipkow
Michael Norrish	John O’Leary	Lawrence Paulson
Andrei Popescu	Bas Spitters	Josef Urban
Makarius Wenzel	Freek Wiedijk	Akihisa Yamada

Local Organisation

Czesław Byliński
 Adam Grabowski
 Artur Korniłowicz
 Roman Matuszewski
 Karol Pąk

External Reviewers

Rajashree Agrawal	Johannes Áman Pohjola	Thaynara Arielly de Lima
Alexander Best	Timothy Bourke	Mario Carneiro
Felix Cherubini	Vikraman Choudhury	Stefan Ciobaca
Evelyne Contejean	Sander Dahmen	Jérémy Dubut
Manuel Eberl	Andres Erbsen	Daniil Frumin
David Fuenmayor	Lorenzo Gheri	Daniel Gratzer
Ariel Grunfeld	Roberto Guanciale	Stepan Holub
Matthias Hutzler	Jules Jacobs	Jacques-Henri Jourdan
Ohad Kammar	Dominik Kirst	Bram Kohlen
Amélie Ledein	Milan Lopuhaä-Zwakenberg	Aart Middeldorp
Houda Mouhcine	Julian Parsert	Bartosz Piotrowski
Nicolas Pouillard	Ivan Prokić	Pierre-Marie Pédrot
Robert Rubbens	Joshua Schneider	Carlos Simpson
Matthieu Sozeau	Christoph Sprenger	Runzhou Tao
Dmitriy Traytel	Daniel Ventura	Yuting Wang