

12th International Conference on Interactive Theorem Proving

ITP 2021, June 29–July 1, 2021, Rome, Italy (Virtual Conference)

Edited by

Liron Cohen

Cezary Kaliszyk



Editors

Liron Cohen 

Ben-Gurion University, Be'er Sheva, Israel
cliron@cs.bgu.ac.il

Cezary Kaliszyk 

University of Innsbruck, Austria
cezary.kaliszyk@uibk.ac.at

ACM Classification 2012

Theory of computation → Logic

ISBN 978-3-95977-188-7

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/978-3-95977-188-7>.

Publication date

June, 2021

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.2021.0

ISBN 978-3-95977-188-7

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)
- 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>Liron Cohen and Cezary Kaliszyk</i>	0:vii

Invited Papers and Talks

The CakeML Project’s Quest for Ever Stronger Correctness Theorems	
<i>Magnus O. Myreen</i>	1:1–1:10
Synthesis of Safe Pointer-Manipulating Programs	
<i>Nadia Polikarpova</i>	2:1–2:1
Bounded-Deducibility Security	
<i>Andrei Popescu, Thomas Bauereiss, and Peter Lammich</i>	3:1–3:20

Regular Papers

A Graphical User Interface Framework for Formal Verification	
<i>Edward W. Ayers, Mateja Jamnik, and W. T. Gowers</i>	4:1–4:16
A Formalization of Dedekind Domains and Class Groups of Global Fields	
<i>Anne Baanen, Sander R. Dahmen, Ashvni Narayanan, and Filippo A. E. Nuccio Mortarino Majno di Capriglio</i>	5:1–5:19
A Formally Verified Checker for First-Order Proofs	
<i>Seulkee Baek</i>	6:1–6:13
Value-Oriented Legal Argumentation in Isabelle/HOL	
<i>Christoph Benz Müller and David Fuenmayor</i>	7:1–7:20
Unsolvability of the Quintic Formalized in Dependent Type Theory	
<i>Sophie Bernard, Cyril Cohen, Assia Mahboubi, and Pierre-Yves Strub</i>	8:1–8:18
Itauto: An Extensible Intuitionistic SAT Solver	
<i>Frédéric Besson</i>	9:1–9:18
Verified Progress Tracking for Timely Dataflow	
<i>Matthias Brun, Sára Decova, Andrea Lattuada, and Dmitriy Traytel</i>	10:1–10:20
Syntactic-Semantic Form of Mizar Articles	
<i>Czesław Byliński, Artur Kornilowicz, and Adam Naumowicz</i>	11:1–11:17
Homotopy Type Theory in Isabelle	
<i>Joshua Chen</i>	12:1–12:8
Flexible Coinduction in Agda	
<i>Luca Ciccone, Francesco Dagnino, and Elena Zucca</i>	13:1–13:19
A Verified Decision Procedure for Univariate Real Arithmetic with the BKR Algorithm	
<i>Katherine Cordwell, Yong Kiam Tan, and André Platzer</i>	14:1–14:20

12th International Conference on Interactive Theorem Proving (ITP 2021).

Editors: Liron Cohen and Cezary Kaliszyk



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

Formalising a Turing-Complete Choreographic Language in Coq <i>Luís Cruz-Filipe, Fabrizio Montesi, and Marco Peressotti</i>	15:1–15:18
A Natural Formalization of the Mutilated Checkerboard Problem in Naproche <i>Adrian De Lon, Peter Koepke, and Anton Lorenzen</i>	16:1–16:11
A Variant of Wagner’s Theorem Based on Combinatorial Hypermaps <i>Christian Doczkal</i>	17:1–17:17
Formalized Haar Measure <i>Floris van Doorn</i>	18:1–18:17
A Mechanised Proof of the Time Invariance Thesis for the Weak Call-By-Value λ -Calculus <i>Yannick Forster, Fabian Kunze, Gert Smolka, and Maximilian Wuttke</i>	19:1–19:20
Mechanising Complexity Theory: The Cook-Levin Theorem in Coq <i>Lennard Gäher and Fabian Kunze</i>	20:1–20:18
Proving Quantum Programs Correct <i>Kesha Hietala, Robert Rand, Shih-Han Hung, Liyi Li, and Michael Hicks</i>	21:1–21:19
Formalization of Basic Combinatorics on Words <i>Štěpán Holub and Štěpán Starosta</i>	22:1–22:17
Synthetic Undecidability and Incompleteness of First-Order Axiom Systems in Coq <i>Dominik Kirst and Marc Hermes</i>	23:1–23:20
Complete Bidirectional Typing for the Calculus of Inductive Constructions <i>Meven Lennon-Bertrand</i>	24:1–24:19
A Mechanized Proof of the Max-Flow Min-Cut Theorem for Countable Networks <i>Andreas Lochbihler</i>	25:1–25:18
A Formal Proof of Modal Completeness for Provability Logic <i>Marco Maggesi and Cosimo Perini Brogi</i>	26:1–26:18
Formal Verification of Termination Criteria for First-Order Recursive Functions <i>Cesar A. Muñoz, Mauricio Ayala-Rincón, Mariano M. Moscato, Aaron M. Dutle, Anthony J. Narkawicz, Ariane A. Almeida, Andréia B. Avelar, and Thiago M. Ferreira Ramos</i>	27:1–27:17
Verified Double Sided Auctions for Financial Markets <i>Raja Natarajan, Suneel Sarswat, and Abhishek Kr Singh</i>	28:1–28:18
Reaching for the Star: Tale of a Monad in Coq <i>Pierre Nigron and Pierre-Évariste Dagand</i>	29:1–29:19
Specifying Message Formats with Contiguity Types <i>Konrad Slind</i>	30:1–30:17
Proof Pearl : Playing with the Tower of Hanoi Formally <i>Laurent Théry</i>	31:1–31:16
Verifying an HTTP Key-Value Server with Interaction Trees and VST <i>Hengchu Zhang, Wolf Honoré, Nicolas Koh, Yao Li, Yishuai Li, Li-Yao Xia, Lennart Beringer, William Mansky, Benjamin Pierce, and Steve Zdancewic</i>	32:1–32:19

■ 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, the twelfth to be held under the ITP name, is co-located with the 36th Annual Symposium on Logic in Computer Science (LICS 2021), and was to be held in Rome, Italy. However, due to the COVID-19 global pandemic, the conference will be held in an online format for the first time. Previous ITP conferences took place in Edinburgh 2010, Nijmegen 2011, Princeton 2012, Rennes 2013, Vienna 2014, Nanjing 2015, Nancy 2016, Brasilia 2017, Oxford 2018 and Portland 2019; 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 57 submissions (51 long papers and 6 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: 29 papers (28 long papers and 1 short). 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 Nadia Polikarpova (University of California, San Diego, joint talk with LICS), Andrei Popescu (University of Sheffield), and Magnus Myreen (Chalmers). The present volume collects all the accepted papers contributed to the conference as well as the latter two invited papers. This is the second 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, as well as the EasyConferences staff for their support in the logistics.

We are grateful to Daniele Gorla for offering to organize ITP in Rome and his flexibility in changing the format in face of the pandemic. We would like to also extend this thanks to all authors and speakers, as we are certain that adjusting to the new format of the conference required some additional effort. Finally we are thankful to the ITP Steering Committee for their guidance throughout.



