

# 13th International Conference on Interactive Theorem Proving

ITP 2022, August 7–10, 2022, Haifa, Israel

Edited by

June Andronick

Leonardo de Moura



*Editors*

**June Andronick**

Proofcraft, UNSW and the seL4 Foundation, Australia  
june.andronick@proofcraft.systems

**Leonardo de Moura** 

Microsoft Research, Redmond, WA, US  
leonardo@microsoft.com

*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 978-3-95977-252-5**

*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/978-3-95977-252-5>.

*Publication date*

August, 2022

*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.2022.0

ISBN 978-3-95977-252-5

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>June Andronick and Leonardo de Moura</i> .....	0:ix

## Invited Talks

Modelling and Verifying Properties of Biological Neural Networks	
<i>Amy Felty</i> .....	1:1–1:2
User Interface Design in the HolPy Theorem Prover	
<i>Bohua Zhan</i> .....	2:1–2:1

## Regular Papers

Candle: A Verified Implementation of HOL Light	
<i>Oskar Abrahamsson, Magnus O. Myreen, Ramana Kumar, and Thomas Sewell</i> ...	3:1–3:17
Use and Abuse of Instance Parameters in the Lean Mathematical Library	
<i>Anne Baanen</i> .....	4:1–4:20
A Complete, Mechanically-Verified Proof of the Banach-Tarski Theorem in ACL2(R)	
<i>Jagadish Bapanapally and Ruben Gamboa</i> .....	5:1–5:15
Dandelion: Certified Approximations of Elementary Functions	
<i>Heiko Becker, Mohit Tekriwal, Eva Darulova, Anastasia Volkova, and Jean-Baptiste Jeannin</i> .....	6:1–6:19
The Zoo of Lambda-Calculus Reduction Strategies, And Coq	
<i>Małgorzata Biernacka, Witold Charatonik, and Tomasz Drab</i> .....	7:1–7:19
Seventeen Provers Under the Hammer	
<i>Martin Desharnais, Petar Vukmirović, Jasmin Blanchette, and Makarius Wenzel</i> .....	8:1–8:18
Formalising Szemerédi’s Regularity Lemma in Lean	
<i>Yaël Dillies and Bhavik Mehta</i> .....	9:1–9:19
Formalized functional analysis with semilinear maps	
<i>Frédéric Dupuis, Robert Y. Lewis, and Heather Macbeth</i> .....	10:1–10:19
Formalising Fisher’s Inequality: Formal Linear Algebraic Proof Techniques in Combinatorics	
<i>Chelsea Edmonds and Lawrence C. Paulson</i> .....	11:1–11:19
Synthetic Kolmogorov Complexity in Coq	
<i>Yannick Forster, Fabian Kunze, and Nils Lauer mann</i> .....	12:1–12:19
Verifying a Sequent Calculus Prover for First-Order Logic with Functions in Isabelle/HOL	
<i>Asta Halkjær From and Frederik Krogsdal Jacobsen</i> .....	13:1–13:22

13th International Conference on Interactive Theorem Proving (ITP 2022).

Editors: June Andronick and Leonardo de Moura



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

Formalizing the Ring of Adèles of a Global Field <i>María Inés de Frutos-Fernández</i> .....	14:1–14:18
A Verified Cyclicity Checker: For Theories with Overloaded Constants <i>Arve Gengelbach and Johannes Áman Pohjola</i> .....	15:1–15:18
The Isabelle ENIGMA <i>Zarathustra A. Goertzel, Jan Jakubův, Cezary Kaliszyk, Miroslav Olšák, Jelle Piepenbrock, and Josef Urban</i> .....	16:1–16:21
Accelerating Verified-Compiler Development with a Verified Rewriting Engine <i>Jason Gross, Andres Erbsen, Jade Philipoom, Miraya Poddar-Agrawal, and Adam Chlipala</i> .....	17:1–17:18
Automatic Test-Case Reduction in Proof Assistants: A Case Study in Coq <i>Jason Gross, Théo Zimmermann, Miraya Poddar-Agrawal, and Adam Chlipala</i> .....	18:1–18:18
Undecidability of Dyadic First-Order Logic in Coq <i>Johannes Hostert, Andrej Dudenhefner, and Dominik Kirst</i> .....	19:1–19:19
Taming an Authoritative Armv8 ISA Specification: L3 Validation and CakeML Compiler Verification <i>Hrutvik Kanabar, Anthony C. J. Fox, and Magnus O. Myreen</i> .....	20:1–20:22
Formalization of Randomized Approximation Algorithms for Frequency Moments <i>Emin Karayel</i> .....	21:1–21:21
Computational Back-And-Forth Arguments in Constructive Type Theory <i>Dominik Kirst</i> .....	22:1–22:12
Formalizing the Divergence Theorem and the Cauchy Integral Formula in Lean <i>Yury Kudryashov</i> .....	23:1–23:19
Refinement of Parallel Algorithms down to LLVM <i>Peter Lammich</i> .....	24:1–24:18
Proof Pearl: Formalizing Spreads and Packings of the Smallest Projective Space $PG(3,2)$ Using the Coq Proof Assistant <i>Nicolas Magaud</i> .....	25:1–25:17
Formalizing a Diophantine Representation of the Set of Prime Numbers <i>Karol Pąk and Cezary Kaliszyk</i> .....	26:1–26:8
Kalas: A Verified, End-To-End Compiler for a Choreographic Language <i>Johannes Áman Pohjola, Alejandro Gómez-Londoño, James Shaker, and Michael Norrish</i> .....	27:1–27:18
Deeper Shallow Embeddings <i>Jacob Prinz, G. A. Kavvos, and Leonidas Lampropoulos</i> .....	28:1–28:18
Reflexive Tactics for Algebra, Revisited <i>Kazuhiko Sakaguchi</i> .....	29:1–29:22
Formalizing Algorithmic Bounds in the Query Model in EasyCrypt <i>Alley Stoughton, Carol Chen, Marco Gaboardi, and Weihao Qu</i> .....	30:1–30:21

Formalization of a Stochastic Approximation Theorem  
*Koundinya Vajjha, Barry Trager, Avraham Shinnar, and Vasily Pestun* ..... 31:1–31:18

Mechanizing Soundness of Off-Policy Evaluation  
*Jared Yeager, J. Eliot B. Moss, Michael Norrish, and Philip S. Thomas* ..... 32:1–32:20

Compositional Verification of Interacting Systems Using Event Monads  
*Bohua Zhan, Yi Lv, Shuling Wang, Gehang Zhao, Jifeng Hao, Hong Ye, and Bican Xia* ..... 33:1–33:21





## ■ 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 thirteenth to be held under the ITP name, is co-located with the Federated Logic Conference (FLoC 2022), Haifa, Israel. 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 66 submissions (63 regular papers and 3 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: 31 papers (30 regular papers and 1 short paper). 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 Amy Felty (School of Electrical Engineering and Computer Science, University of Ottawa) and Bohua Zhan (State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences). The present volume collects all the accepted papers contributed to the conference as well as the two invited papers. This is the third 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 FLoC organizers and thankful to the ITP Steering Committee for their guidance throughout.



