

17th International Conference on Interactive Theorem Proving

ITP 2026, July 26–29, 2026, Lisbon, Portugal

Edited by

Ekaterina Komendantskaya

Tobias Nipkow



Editors

Ekaterina Komendantskaya 

Southampton University, UK

Heriot-Watt University, Edinburgh, UK

E.Komendantskaya@soton.ac.uk

Tobias Nipkow 

Technical University of Munich, Germany

<https://www.proof.cit.tum.de/~nipkow>

ACM Classification 2012

Theory of computation → Interactive proof systems; Theory of computation → Higher order logic; Theory of computation → Type theory; Theory of computation → Program verification; Theory of computation → Logic and verification

ISBN 978-3-95977-436-9

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/978-3-95977-436-9>.

Publication date

July, 2026

Bibliographic information published by the Deutsche Nationalbibliothek

The Deutsche Nationalbibliothek lists all publications of this volume 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.2026.0

ISBN 978-3-95977-436-9

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

- Christel Baier (TU Dresden, DE)
- Roberto Di Cosmo (Inria and Université Paris Cité, FR)
- Faith Ellen (University of Toronto, CA)
- Javier Esparza (TU München, DE)
- Holger Hermanns (Universität des Saarlandes, Saarbrücken, DE and Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Wadern, DE)
- Daniel Král' (Leipzig University, DE and Max Planck Institute for Mathematics in the Sciences, Leipzig, DE – Chair)
- Sławomir Lasota (University of Warsaw, PL)
- Meena Mahajan (Institute of Mathematical Sciences, Chennai, IN)
- Chih-Hao Luke Ong (Nanyang Technological University, SG)
- Eva Rotenberg (IT University of Copenhagen, DK)
- Pierre Senellart (ENS, Université PSL, Paris, France)
- Alexandra Silva (Cornell University, Ithaca, US)

ISSN 1868-8969

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

■ Contents

Preface

<i>Ekaterina Komendantskaya and Tobias Nipkow</i>	0:ix
---	------

Invited Talks

Nitro Isolation Engine: Formally Verifying a Production Hypervisor

<i>Hanno Becker, Nathan Chong, Robert Dockins, Jim Grundy, Jason Hu, Ike Mulder, Dominic P. Mulligan, Paul Mure, Bryan Parno, Lawrence C. Paulson, and Konrad Slind</i>	1:1–1:2
---	---------

Developing a Quantum Crypto Theorem Prover from Scratch

<i>Dominique Unruh</i>	2:1–2:18
------------------------------	----------

Regular Papers

Complex Bounded Operators in Isabelle/HOL

<i>Dominique Unruh and José Manuel Rodríguez Caballero</i>	3:1–3:19
--	----------

Formally Verified Liveness with Multiparty Session Types in Rocq

<i>Omer Keskin, Nobuko Yoshida, and Rob van Glabbeek</i>	4:1–4:21
--	----------

Enhancing Interactive Theorem Prover Error Messages with Hints

<i>Maria Khakimova, Sára Juhošová, Jaro Reinders, and Jesper Cockx</i>	5:1–5:19
--	----------

Lazy Proof Automation for Separation Logic

<i>Valentin Mikhalechuk, Vladimir Gladstein, and Ilya Sergey</i>	6:1–6:18
--	----------

Certified Intersection of Commutative Regular Expressions as Solutions of Systems of Linear Diophantine Equations

<i>Ricardo Almeida, Blair Archibald, Basile Pesin, and Michele Sevegnani</i>	7:1–7:20
--	----------

Lean Formalization of Generalization Error Bound by Rademacher Complexity and Dudley's Entropy Integral

<i>Sho Sonoda, Kazumi Kasaura, Yuma Mizuno, Kei Tsukamoto, and Naoto Onda</i> ..	8:1–8:17
--	----------

Functional Correctness of an Optimized Modular Inversion Algorithm

<i>Assia Mahboubi, Guillaume Melquiond, Pierre-Yves Strub, and Tomás Vallejos Parada</i>	9:1–9:19
--	----------

Automated Verification of Robot Software Models with Assume-Guarantee Reasoning in Isabelle/HOL

<i>Fang Yan, Benoît Ballenghien, Simon Foster, Ana Cavalcanti, James Baxter, and Burkhart Wolff</i>	10:1–10:21
---	------------

Formalization of a Realistic Verification-Condition Generator for an Intermediate Verification Language

<i>Vladimir Gladstein and K. Rustan M. Leino</i>	11:1–11:19
--	------------

TableauxRocq: A Deep Embedding of Free-Variable Tableaux in Rocq

<i>Johann Rosain and Julie Cailler</i>	12:1–12:22
--	------------

17th International Conference on Interactive Theorem Proving (ITP 2026).

Editors: Ekaterina Komendantskaya and Tobias Nipkow



Leibniz International Proceedings in Informatics

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

Verification of the Garsia–Wachs Algorithm <i>Makoto Kanazawa</i>	13:1–13:19
Certified Infinite Descent Criteria in Isabelle/HOL <i>Jamie Wright, Liron Cohen, Reuben N. S. Rowe, and Andrei Popescu</i>	14:1–14:18
Formalizing a Hoare Calculus for Choreographic Programming <i>Luís Cruz-Filipe and Thomas Wulff Heissel</i>	15:1–15:18
Don’t Sweat Interaction Trees: Proof-Guided Local Variable Lifting for Interaction Trees <i>Yiming Lin, Ian Kariniemi, and Yao Li</i>	16:1–16:21
Panbench: A Comparative Benchmarking Tool for Dependently-Typed Languages <i>Reed Mullanix and Jacques Carette</i>	17:1–17:18
Apply2Isar: Automatically Converting Isabelle/HOL Apply-Style Proofs to Structured Isar <i>Sage Binder, Hanna Lachnitt, and Katherine Kosaian</i>	18:1–18:20
Formalizing the Bruck–Ryser–Chowla Theorem: Combinatorial Design Theory in Lean <i>Eric Jonathan Wang and Elif Uskuplu</i>	19:1–19:19
Completing Almost Fair Simulations <i>Arthur Correnson, Iona Kuhn, and Bernd Finkbeiner</i>	20:1–20:20
Formalizing Abstract Simplicial Complexes & Stellar Subdivisions in Lean <i>Garett Cunningham, Daniel Zach, and Stefan Friedl</i>	21:1–21:20
Feedback & Synthesis in LLM-Assisted Termination Proofs <i>Zeke Medley and Panagiotis Manolios</i>	22:1–22:19
From Weierstraß to Dedekind via Jacobi: Formalising Foundations of Modular Forms <i>Manuel Eberl, Wenda Li, and Lawrence C. Paulson</i>	23:1–23:19
PROOFWALA: A Framework for Multilingual Proof Data Synthesis and Theorem-Proving <i>Amitayush Thakur, George Tsoukalas, Greg Durrett, and Swarat Chaudhuri</i>	24:1–24:21
LeanArchitect: Automating Blueprint Generation for Humans and AI <i>Thomas Zhu, Pietro Monticone, Sean Welleck, and Jeremy Avigad</i>	25:1–25:16
An End-To-End Verification of Keller’s Conjecture <i>James Gallicchio, Cayden Codel, Jeremy Avigad, and Marijn J. H. Heule</i>	26:1–26:20
Fractional Separation Logic in Isabelle LLVM <i>Peter Lammich</i>	27:1–27:18
String Diagrams for Monoidal Categories, in Rocq <i>Damien Pous</i>	28:1–28:20
Securing the Foundations of an Intermediate Language for Probabilistic Program Verification <i>Oliver Bøving and Christoph Matheja</i>	29:1–29:21

Bidirectional Interpolation for the λ -Calculus: Revisiting and Formalising
Craig-Čubrić Interpolation

Meven Lennon-Bertrand and Alexis Saurin 30:1–30:21

Short Papers

130k Lines of Formal Topology in Two Weeks: Simple and Cheap
Autoformalization for Everyone?

Josef Urban 31:1–31:9

Faster Verified Real Root Isolation with Descartes' Rule of Signs

Aeacus Sheng, Wenda Li, and Paul B. Jackson 32:1–32:10

Formal Primal-Dual Algorithm Analysis

Mohammad Abdulaziz, Thomas Ammer, and Christoph Madlener 33:1–33:9

Three Roads to de Finetti's Theorem in Lean 4

Cameron Freer 34:1–34:9

A Lean Tactic for Normalizing Expressions in an Algebra over a Ring

Arend Mellendijk 35:1–35:8

Lean on Vampire Proofs

*Jonas Bodingbauer, Márton Hajdu, Laura Kovács, Axel Polaczek, and
Michael Rawson* 36:1–36:9

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 started life with a HOL workshop in 1988 in Cambridge. It gradually widened its scope to include other higher-order systems and became the conference series TPHOLs in 1996. In 2010, the scope was widened once more to interactive theorem provers generally and it became the current conference series ITP. This year's conference takes place in Lisbon in Portugal and is part of the Federated Logic Conference (FLoC).

This year's conference attracted a total of 130 submissions. Each paper was systematically reviewed by at least three program committee members or appointed external reviewers and 34 papers were finally selected for presentation at the conference (28 regular papers and 6 short papers). We thank all authors for their submissions and the programme committee members and the external reviewers for their invaluable work.

As well as all the selected papers, we are very pleased to have invited keynote talks by Domimic Mulligan (Automated Reasoning Group, Amazon Web Services) and Dominique Unruh (RWTH Aachen and University of Tartu). The present volume collects all the invited and accepted papers contributed to the conference. We thank the LIPICs team at Dagstuhl for their usual efficient production of the proceedings.

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

Ekaterina Komendantskaya and Tobias Nipkow

Organization

FLoC Organization Committee

Rajeev Alur	University of Pennsylvania, USA
Nuno P. Lopes	University of Lisbon, Portugal
Alexandra Silva	Cornell University, USA
Aws Albarghouthi	UW-Madison, USA
Loris D'Antoni	UC San Diego, USA
José Fragoso Santos	University of Lisbon, Portugal
Alessandro Gianola	University of Lisbon, Portugal
Bernd Finkbeiner	CISPA Helmholtz Center for Information Security, Germany
Caterina Urban	INRIA and ENS, France

Programme Committee Chairs

Ekaterina Komendantskaya	University of Southampton and Heriot-Watt University, UK
Tobias Nipkow	Technical University of Munich, Germany

Programme Committee

Mohammad Abdulaziz	Reynald Affeldt	Guillaume Allais
Robert Atkey	Jeremy Avigad	Jasmin Blanchette
Sandrine Blazy	Sylvie Boldo	Edwin Brady
Alessandro Bruni	Swarat Chaudhuri	Matthew Daggitt
Sander Dahmen	María Inés de Frutos-Fernández	Manuel Eberl
Amy Felty	Jacques Fleuriot	Yannick Forster
Ralf Jung	Ambrus Kaposi	Yonghyun Kim
Katherine Kosaian	Robert Lewis	Assia Mahboubi
William Mansky	Micaela Mayero	Magnus Myreen
Grant Passmore	Andrei Popescu	François Pottier
Talia Ringer	Christine Rizkallah	Rustan Leino
Nikhil Swamy	Nicolas Tabareau	Yong Kiam Tan
Joseph Tassarotti	Enrico Tassi	Laura Titolo
Dmitriy Traytel	Floris van Doorn	Niccolò Veltri
Akihisa Yamada		



External Reviewers

Gianluca Amato	Jonathan Arnoult	Aurele Barriere
Marc Bezem	Sage Binder	Chris Birkbeck
Asta Halkjær Boserup	Mathis Bouverot-Dupuis	Guillaume Burel
Anne Baanen	Luca Campa	Mario Carneiro
Arthur Charguéraud	Alain Chavarri Villarello	Mark Chevallier
François Clément	Cyril Cohen	Alessio Coltellacci
Martin Desharnais-Schäfer	Jérémy Dubut	Thiago Felicissimo
Laouen Fernet	Mathias Fleury	Fabian Huch
Alex Hyman	Kim Jieung	Aditi Kabra
Antanas Kalkauskas	Kevin Kappelmann	Marie Kerjean
Dohan Kim	Yoonseung Kim	Michael Kirsten
Ramana Kumar	Vincent Lafeychine	Ambroise Lafont
Thomas Lamiaux	Peter Lammich	Andrea Laretto
David Ledvinka	Yann Leray	Paul Lezeau
Moritz Lichter	Andreas Löw	Luca Maio
Arend Mellendijk	Guillaume Melquiond	Christian Merten
Josué Moreau	Daniel Nezamabadi	Michael Norrish
Filippo Nuccio	Luca Padovani	Karl Palmskog
Andrei Paskevich	Christine Paulin	Lawrence C. Paulson
Clément Pit-Claudel	Josselin Poirer	Mathias Schack Rabing
Rhea Ranalter	Michael Rothgang	Arnab Roy
Takafumi Saikawa	Jonas Schöpf	Ian Shillito
Maximilian Shäffeler	Filip Smola	Derek Sorensen
Lukas Stevens	Toru Takisaka	René Thiemann
Balazs Toth	Niels van der Weide	Quentin Vermande
Cheng-Syuan Wan	Zili Wang	Théo Winterhalter
Burkhardt Wolff	James Wood	Johannes Åman Pohjola

■ List of Authors

Mohammad Abdulaziz  (33)
King's College London, UK

Ricardo Almeida  (7)
School of Computing Science, University of
Glasgow, UK

Thomas Ammer  (33)
King's College London, UK

Blair Archibald  (7)
School of Computing Science, University of
Glasgow, UK

Jeremy Avigad  (25, 26)
Carnegie Mellon University, Pittsburgh, PA,
USA

Benoît Ballenghien  (10)
Université Paris-Saclay, CNRS, ENS
Paris-Saclay, LMF, France

James Baxter  (10)
University of York, UK

Hanno Becker  (1)
Automated Reasoning Group, Amazon Web
Services, Cambridge, UK

Sage Binder  (18)
University of Iowa, Iowa City, IA, USA

Jonas Bodingbauer  (36)
TU Wien, Austria

Oliver Bøving  (29)
Technical University of Denmark, Lyngby,
Denmark

José Manuel Rodríguez Caballero  (3)
Mathématiques et statistique - Faculté des
sciences et de génie - Université Laval, Québec,
Canada

Julie Cailler  (12)
University of Lorraine, CNRS, Inria, LORIA,
Nancy, France

Jacques Carette  (17)
Department of Computing and Software,
McMaster University, Hamilton, Canada

Ana Cavalcanti  (10)
University of York, UK

Swarat Chaudhuri  (24)
University of Texas, Austin, TX, USA

Nathan Chong  (1)
Automated Reasoning Group, Amazon Web
Services, FL, USA

Jesper Cockx  (5)
Delft University of Technology, The Netherlands

Cayden Codel  (26)
Carnegie Mellon University, Pittsburgh, PA,
USA

Liron Cohen  (14)
Ben-Gurion University of the Negev, Be'er
Sheva, Israel

Arthur Correnson  (20)
CISPA Helmholtz Center for Information
Security, Saarbrücken, Germany

Luís Cruz-Filipe  (15)
IT University Copenhagen, Denmark

Garett Cunningham  (21)
University of Connecticut, Storrs, CT, USA

Robert Dockins  (1)
Automated Reasoning Group, Amazon Web
Services, Portland, OR, USA

Greg Durrett  (24)
University of Texas, Austin, TX, USA

Manuel Eberl  (23)
University of Innsbruck, Austria

Bernd Finkbeiner  (20)
CISPA Helmholtz Center for Information
Security, Saarbrücken, Germany

Simon Foster  (10)
University of York, UK

Cameron Freer  (34)
Massachusetts Institute of Technology,
Cambridge, MA, USA

Stefan Friedl  (21)
Universität Regensburg, Germany

James Gallicchio  (26)
Carnegie Mellon University, Pittsburgh, PA,
USA

Vladimir Gladshstein  (6, 11)
School of Computing, National University of
Singapore, Singapore

17th International Conference on Interactive Theorem Proving (ITP 2026).

Editors: Ekaterina Komendantskaya and Tobias Nipkow



Leibniz International Proceedings in Informatics

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

- Jim Grundy  (1)
Automated Reasoning Group, Amazon Web Services, Austin, TX, USA
- Márton Hajdu  (36)
TU Wien, Austria
- Thomas Wulff Heissel (15)
Department of Computer Science, University of Southern Denmark, Odense, Denmark
- Marijn J. H. Heule  (26)
Carnegie Mellon University, Pittsburgh, PA, USA
- Jason Hu  (1)
Automated Reasoning Group, Amazon Web Services, Seattle, WA, USA
- Paul B. Jackson  (32)
University of Edinburgh, UK
- Sára Juhošová  (5)
Delft University of Technology, The Netherlands
- Makoto Kanazawa  (13)
Department of Advanced Sciences, Faculty of Science and Engineering, Hosei University, Tokyo, Japan
- Ian Kariniemi  (16)
Portland State University, OR, USA
- Kazumi Kasaura  (8)
OMRON SINIC X Corporation, Tokyo, Japan
- Omer Keskin  (4)
University of Edinburgh, UK
- Maria Khakimova  (5)
Delft University of Technology, The Netherlands
- Katherine Kosaian  (18)
University of Iowa, Iowa City, IA, USA
- Laura Kovács  (36)
TU Wien, Austria
- Iona Kuhn  (20)
CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
- Hanna Lachnitt  (18)
Stanford University, Stanford, CA, USA
- Peter Lammich  (27)
University of Twente, Enschede, The Netherlands
- K. Rustan M. Leino  (11)
Amazon Web Services, Seattle, WA, USA
- Meven Lennon-Bertrand  (30)
Université Paris Cité, INRIA, CNRS, IRIF, F-75013 Paris, France
- Wenda Li  (23, 32)
University of Edinburgh, UK
- Yao Li  (16)
Portland State University, OR, USA
- Yiming Lin  (16)
Portland State University, OR, USA
- Christoph Madlener  (33)
Technische Universität München, Germany
- Assia Mahboubi  (9)
Nantes Université, École Centrale Nantes, CNRS, INRIA, LS2N, UMR 6004, France; Vrije Universiteit Amsterdam, The Netherlands
- Panagiotis Manolios  (22)
Khoury College of Computer Sciences, Northeastern University, Boston, MA, USA
- Christoph Matheja  (29)
University of Oldenburg, Germany; Technical University of Denmark, Lyngby, Denmark
- Zeke Medley (22)
Khoury College of Computer Sciences, Northeastern University, Boston, MA, USA
- Arend Mellendijk  (35)
University of Bonn, Germany
- Guillaume Melquiond  (9)
Inria, ENS de Lyon, CNRS, Université Lyon 1, LIP, UMR 5668, Lyon, France
- Valentin Mikhalechuk  (6)
School of Computing, National University of Singapore, Singapore
- Yuma Mizuno  (8)
University College Cork, Ireland
- Pietro Monticone  (25)
University of Trento, Italy
- Ike Mulder  (1)
Automated Reasoning Group, Amazon Web Services, Cambridge, UK
- Reed Mullanix  (17)
Department of Computing and Software, McMaster University, Hamilton, Canada
- Dominic P. Mulligan  (1)
Automated Reasoning Group, Amazon Web Services, Cambridge, UK

Paul Mure  (1)
Massachusetts Institute of Technology,
Cambridge, MA, USA

Naoto Onda  (8)
OMRON SINIC X Corporation, Tokyo, Japan

Bryan Parno  (1)
Automated Reasoning Group, Amazon Web
Services, PA, USA

Lawrence C. Paulson  (1, 23)
Automated Reasoning Group, Amazon Web
Services, Cambridge, UK

Basile Pesin  (7)
Fédération ENAC ISAE-SUPAERO ONERA,
Université de Toulouse, France

Axel Polaczek  (36)
TU Wien, Austria

Andrei Popescu  (14)
University of Sheffield, UK

Damien Pous  (28)
Plume team, CNRS, LIP, ENS de Lyon, UMR
5668, France

Michael Rawson  (36)
University of Southampton, UK

Jaro Reinders  (5)
Delft University of Technology, The Netherlands

Johann Rosain  (12)
ENS de Lyon, Lyon, France

Reuben N. S. Rowe  (14)
Royal Holloway University of London, Egham,
UK

Alexis Saurin  (30)
Université Paris Cité, CNRS, INRIA, IRIF,
F-75013 Paris, France

Ilya Sergey  (6)
School of Computing, National University of
Singapore, Singapore

Michele Sevegnani  (7)
School of Computing Science, University of
Glasgow, UK

Aeacus Sheng  (32)
University of Edinburgh, UK

Konrad Slind  (1)
Unaffiliated, Minneapolis, MN, USA

Sho Sonoda  (8)
RIKEN AIP, Tokyo, Japan; CyberAgent Inc.,
Tokyo, Japan

Pierre-Yves Strub  (9)
PQShield, Paris, France

Amitayush Thakur  (24)
University of Texas, Austin, TX, USA

George Tsoukalas  (24)
University of Texas, Austin, TX, USA

Kei Tsukamoto  (8)
The University of Tokyo, Japan

Dominique Unruh  (2, 3)
RWTH Aachen, Germany; University of Tartu,
Estonia

Josef Urban  (31)
AI4REASON, Prague, Czech Republic;
University of Gothenburg, Sweden; Chalmers
University of Technology, Gothenburg, Sweden

Elif Uskuplu  (19)
Indiana University, Bloomington, IN, USA

Tomás Vallejos Parada  (9)
Nantes Université, École Centrale Nantes,
CNRS, INRIA, LS2N, UMR 6004, France

Rob van Glabbeek  (4)
University of Edinburgh, UK; School of
Computer Science and Engineering, University
of New South Wales, Sydney, Australia

Eric Jonathan Wang  (19)
Carnegie Mellon University, Pittsburgh, PA,
USA

Sean Welleck  (25)
Carnegie Mellon University, Pittsburgh, PA,
USA

Burkhart Wolff  (10)
Université Paris-Saclay, CNRS, ENS
Paris-Saclay, LMF, France

Jamie Wright  (14)
University of Sheffield, UK

Fang Yan  (10)
University of York, UK

Nobuko Yoshida  (4)
University of Oxford, UK

Daniel Zach  (21)
Universität Regensburg, Germany

Thomas Zhu  (25)
Carnegie Mellon University, Pittsburgh, PA,
USA

