

Mauricio Ayala-Rincón · César A. Muñoz (Eds.)

# Interactive Theorem Proving

8th International Conference, ITP 2017  
Brasília, Brazil, September 26–29, 2017  
Proceedings

# Contents

Automated Theory Exploration for Interactive Theorem Proving: An Introduction to the Hipster System . . . . .	1
<i>Moa Johansson</i>	
Automating Formalization by Statistical and Semantic Parsing of Mathematics . . . . .	12
<i>Cezary Kaliszyk, Josef Urban, and Jiří Vyskočil</i>	
A Formalization of Convex Polyhedra Based on the Simplex Method . . . . .	28
<i>Xavier Allamigeon and Ricardo D. Katz</i>	
A Formal Proof of the Expressiveness of Deep Learning . . . . .	46
<i>Alexander Bentkamp, Jasmin Christian Blanchette, and Dietrich Klakow</i>	
Formalization of the Lindemann-Weierstrass Theorem . . . . .	65
<i>Sophie Bernard</i>	
CompCertS: A Memory-Aware Verified C Compiler Using Pointer as Integer Semantics . . . . .	81
<i>Frédéric Besson, Sandrine Blazy, and Pierre Wilke</i>	
Formal Verification of a Floating-Point Expansion Renormalization Algorithm. . . . .	98
<i>Sylvie Boldo, Mioara Joldes, Jean-Michel Muller, and Valentina Popescu</i>	
How to Simulate It in Isabelle: Towards Formal Proof for Secure Multi-Party Computation . . . . .	114
<i>David Butler, David Aspinall, and Adrià Gascón</i>	
FoCaLiZe and Dedukti to the Rescue for Proof Interoperability . . . . .	131
<i>Raphaël Cauderlier and Catherine Dubois</i>	
A Formal Proof in Coq of LaSalle’s Invariance Principle . . . . .	148
<i>Cyril Cohen and Damien Rouhling</i>	
How to Get More Out of Your Oracles . . . . .	164
<i>Luís Cruz-Filipe, Kim S. Larsen, and Peter Schneider-Kamp</i>	
Certifying Standard and Stratified Datalog Inference Engines in SSReflect . . .	171
<i>Véronique Benzaken, Évelyne Contejean, and Stefania Dumbrava</i>	

Weak Call-by-Value Lambda Calculus as a Model of Computation in Coq . . . . .	189
<i>Yannick Forster and Gert Smolka</i>	
Bellerophon: Tactical Theorem Proving for Hybrid Systems . . . . .	207
<i>Nathan Fulton, Stefan Mitsch, Brandon Bohrer, and André Platzer</i>	
Formalizing Basic Quaternionic Analysis . . . . .	225
<i>Andrea Gabrielli and Marco Maggesi</i>	
A Formalized General Theory of Syntax with Bindings . . . . .	241
<i>Lorenzo Gheri and Andrei Popescu</i>	
Proof Certificates in PVS . . . . .	262
<i>Frédéric Gilbert</i>	
Efficient, Verified Checking of Propositional Proofs . . . . .	269
<i>Marijn Heule, Warren Hunt Jr., Matt Kaufmann, and Nathan Wetzler</i>	
Proof Tactics for Assertions in Separation Logic . . . . .	285
<i>Zhé Hóu, David Sanán, Alwen Tiu, and Yang Liu</i>	
Categoricity Results for Second-Order ZF in Dependent Type Theory . . . . .	304
<i>Dominik Kirst and Gert Smolka</i>	
Making PVS Accessible to Generic Services by Interpretation in a Universal Format . . . . .	319
<i>Michael Kohlhase, Dennis Müller, Sam Owre, and Florian Rabe</i>	
Formally Verified Safe Vertical Maneuvers for Non-deterministic, Accelerating Aircraft Dynamics . . . . .	336
<i>Yanni Kouskoulas, Daniel Genin, Aurora Schmidt, and Jean-Baptiste Jeannin</i>	
Using Abstract Stobjs in ACL2 to Compute Matrix Normal Forms . . . . .	354
<i>Laureano Lambán, Francisco J. Martín-Mateos, Julio Rubio, and José-Luis Ruiz-Reina</i>	
Typing Total Recursive Functions in Coq . . . . .	371
<i>Dominique Larchey-Wendling</i>	
Effect Polymorphism in Higher-Order Logic (Proof Pearl) . . . . .	389
<i>Andreas Lochbihler</i>	
Schulze Voting as Evidence Carrying Computation . . . . .	410
<i>Dirk Pattinson and Mukesh Tiwari</i>	
Verified Spilling and Translation Validation with Repair . . . . .	427
<i>Julian Rosemann, Sigurd Schneider, and Sebastian Hack</i>	

A Verified Generational Garbage Collector for CakeML . . . . .	444
<i>Adam Sandberg Ericsson, Magnus O. Myreen, and Johannes Aman Pohjola</i>	
A Formalisation of Consistent Consequence for Boolean Equation Systems . . .	462
<i>Myrthe van Delft, Herman Geuvers, and Tim A.C. Willemse</i>	
Homotopy Type Theory in Lean . . . . .	479
<i>Floris van Doorn, Jakob von Raumer, and Ulrik Buchholtz</i>	
Verifying a Concurrent Garbage Collector Using a Rely-Guarantee Methodology . . . . .	496
<i>Yannick Zakowski, David Cachera, Delphine Demange, Gustavo Petri, David Pichardie, Suresh Jagannathan, and Jan Vitek</i>	
Formalization of the Fundamental Group in Untyped Set Theory Using Auto2. . . . .	514
<i>Bohua Zhan</i>	
<b>Author Index</b> . . . . .	531