CPP’16

Proceedings of the 5th ACM SIGPLAN Conference on

Certified Programs and Proofs

Edited by:
Jeremy Avigad and Adam Chlipala

Sponsored by:
ACM SIGPLAN, in-coop with ACM SIGLOG

Co-located with:
POPL’16
Message from the Chairs

This collection includes the papers presented at CPP 2016, the 5th ACM SIGPLAN Conference on Certified Programs and Proofs, held in cooperation with ACM SIGLOG. The meeting was held in Saint Petersburg, Florida, USA, January 18-19, 2016.

CPP is an international forum on theoretical and practical topics in all areas that consider certification as an essential paradigm for their work, including computer science, mathematics, and education. Certification here means formal, mechanized verification of some sort, preferably with production of independently checkable certificates.

The first four CPP meetings were held in December 2011 in Taipei, in December 2012 in Kyoto, in December 2013 in Melbourne, and in January 2015 in Mumbai. For the second year in a row, the meeting was colocated with POPL, the Symposium on Principles of Programming Languages. We are deeply grateful to ACM SIGPLAN for sponsoring CPP 2016, to ACM SIGLOG for conferring “in-cooperation-with” status, and to the POPL 2016 general chair and local organizers for hosting the meeting.

We are pleased that Leonardo de Moura (Microsoft Research, Redmond) and Harvey Friedman (Ohio State University) accepted our invitations to be invited speakers. Abstracts of their presentations are included in the proceedings.

The program committee for CPP 2016 was composed of 20 researchers from 7 countries. We received a total of 37 submissions, and the committee selected 18 papers for presentation and inclusion in the proceedings. Every submission was reviewed by at least three program-committee members and their selected subreviewers. The committee’s deliberations were conducted using the EasyChair conference-management system.

We would like to thank the program-committee members and the reviewers for their efforts in evaluating the submissions. The discussions were thoughtful and stimulating. Finally, we especially wish to thank the authors of submitted papers and the conference participants for their support of CPP.

Jeremy Avigad and Adam Chlipala
CPP 2016 Co-chairs
CPP 2016 Organization

Organizing Committee

Program Co-Chairs
Jeremy Avigad Carnegie Mellon University, USA
Adam Chlipala MIT, USA

POPL’16 General Chair
Rastislav Bodik University of Washington, USA

Steering Committee Chair
Zhong Shao Yale University, USA

Steering Committee
Andrew Appel Princeton University, USA
Nikolaj Bjørner Microsoft Research Redmond, USA
Georges Gonthier Microsoft Research Cambridge, UK
John Harrison Intel Corporation, USA
Chris Hawblitzel Microsoft Research Redmond, USA
Gerwin Klein NICTA, Australia
Xavier Leroy Inria, France
Dale Miller Inria, France
Tobias Nipkow Technische Universität München, Germany
Michael Norrish NICTA, Australia
Zhong Shao Yale University, USA
Alwen Tiu Nanyang Technological University, Singapore

Sponsor: SIGPLAN, in cooperation with SIGLOG

Colocated with:
Program Committee

Sandrine Blazy  
Université de Rennes 1, France

Thierry Coquand  
Chalmers University of Technology, Sweden

John Harrison  
Intel, USA

Chris Hawblitzel  
Microsoft Research, Redmond, USA

Cătălin Hrițcu  
Inria Paris-Rocquencourt, France

Brian Huffman  
Galois, Inc., USA

Laura Kovács  
Chalmers University of Technology, Sweden

Peter Lammich  
Technische Universität München, Germany

Hongjin Liang  
University of Science and Technology of China, China

Dan Licata  
Wesleyan University, USA

Panagiotis Manolios  
Northeastern University, USA

Dale Miller  
Inria Saclay and LIX, France

Dominic Mulligan  
Cambridge University, UK

Lawrence Paulson  
Cambridge University, UK

Andrei Popescu  
Middlesex University London, UK

Claudio Sacerdoti Coen  
University of Bologna, Italy

Zachary Tatlock  
University of Washington, USA

Cesare Tinelli  
University of Iowa, USA

Additional Reviewers

Arthur Azevedo de Amorim  
Andrea Asperti  
Frédéric Besson

Jasmin Blanchette  
Jaap Boender  
Thomas Braibant

Taus Brock-Nannestad  
Richard Bubel  
Kaustuv Chaudhuri

Zakaria Chihani  
Cornelius Diekmann  
Lorenzo Gheri

Nick Giannarakis  
Yu Guo  
Mitesh Jain

Maximilian Jaroschek  
Chantal Keller  
Evgenii Kotelnikov

Ramana Kumar  
Wenda Li  
Zhaojui Luo

Zoe Paraskevopoulou  
Matthias Puech  
Giles Reger

Viorica Sofronie-Stokkermans  
Artem Starostin  
Enrico Tassi

Dmitriy Traytel  
Makarius Wenzel  
Colin Zwanziger
## Contents

### Frontmatter

**Message from the Chairs** .......................................................... iii

### Keynotes

**Perspectives on Formal Verification (Invited Talk)**  
Harvey M. Friedman — **Ohio State University, USA** .............................................. 1

**Dependent Type Practice (Invited Talk)**  
Leonardo de Moura — **Microsoft Research, USA** .................................................. 2

### Verifying Imperative Programs

**Higher-Order Representation Predicates in Separation Logic**  
Arthur Charguéraud — **Inria, France** ................................................................. 3

**A Unified Coq Framework for Verifying C Programs with Floating-Point Computations**  
Tahina Ramananandro, Paul Mountcastle, Benoît Meister, and Richard Lethin — **Reservoir Labs, USA** .................................................. 15

**Refinement Based Verification of Imperative Data Structures**  
Peter Lammich — **TU München, Germany** .......................................................... 27

### Design and Implementation of Theorem Provers

**The Vampire and the FOOL**  
Evgenii Kotelnikov, Laura Kovács, Giles Rege, and Andrei Voronkov — **Chalmers University of Technology, Sweden; University of Manchester, UK** .................................................. 37

**Improving Automation in Interactive Theorem Provers by Efficient Encoding of Lambda-Abstractions**  
Łukasz Czajka — **University of Innsbruck, Austria** .................................................. 49

**Towards a Mizar Environment for Isabelle: Foundations and Language**  
Cezary Kaliszyk, Karol Pąk, and Josef Urban — **University of Innsbruck, Austria; University of Bialystok, Poland; Czech Technical University in Prague, Czech Republic** .................................................. 58

### Mathematics

**A Modular, Efficient Formalisation of Real Algebraic Numbers**  
Wenda Li and Lawrence C. Paulson — **University of Cambridge, UK** .................................................. 66

**Formal Proofs of Transcendence for e and pi as an Application of Multivariate and Symmetric Polynomials**  
Sophie Bernard, Yves Bertot, Laurence Rideau, and Pierre-Yves Strub — **Inria, France; IMDEA Software Institute, Spain** .................................................. 76

**Formalizing Jordan Normal Forms in Isabelle/HOL**  
René Thiemann and Akihisa Yamada — **University of Innsbruck, Austria** .................................................. 88

**Formalization of a Newton Series Representation of Polynomials**  
Cyril Cohen and Boris Djalal — **Inria, France** .................................................. 100

### Foundations

**A Logic of Proofs for Differential Dynamic Logic: Toward Independently Checkable Proof Certificates for Dynamic Logics**  
Nathan Fulton and André Platzer — **Carnegie Mellon University, USA** .................................................. 110

**Constructing the Propositional Truncation using Non-recursive HITs**  
Floris van Doorn — **Carnegie Mellon University, USA** .................................................. 122

**A Nominal Exploration of Intuitionism**  
Vincent Rahli and Mark Bickford — **University of Luxembourg, Luxembourg; Cornell University, USA** .................................................. 130
Verification for Concurrent and Distributed Systems

Bisimulation Up-To Techniques for Psi-Calculi
Johannes Åman Pohjola and Joachim Parrow — Uppsala University, Sweden ........................................... 142

Planning for Change in a Formal Verification of the Raft Consensus Protocol
Doug Woos, James R. Wilcox, Steve Anton, Zachary Tatlock, Michael D. Ernst, and Thomas Anderson — University of Washington, USA ................................................................. 154

A Verified Algorithm for Detecting Conflicts in XACML Access Control Rules
Michel St-Martin and Amy P. Felty — University of Ottawa, Canada .............................................................. 166

Compiler Verification

Formal Verification of Control-Flow Graph Flattening
Sandrine Blazy and Alix Trieu — IRISA, France ......................................................................................... 176

Axiomatic Semantics for Compiler Verification
Steven Schäfer, Sigurd Schneider, and Gert Smolka — Saarland University, Germany .................................. 188

Author Index ................................................................................................................................................. 197