



**Association for  
Computing Machinery**

*Advancing Computing as a Science & Profession*

January 18–19, 2016  
St. Petersburg, FL, USA



# 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**

The Association for Computing Machinery, Inc.  
2 Penn Plaza, Suite 701  
New York, NY 10121-0701

Copyright © 2016 by the Association for Computing Machinery, Inc (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted.

To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from: Publications Dept. ACM, Inc.  
Fax +1-212-869-0481 or E-mail [permissions@acm.org](mailto:permissions@acm.org).

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

**Notice to Past Authors of ACM-Published Articles**

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that was previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform [permissions@acm.org](mailto:permissions@acm.org), stating the title of the work, the author(s), and where and when published.

ACM ISBN: 978-1-4503-4127-1

Additional copies may be ordered prepaid from:

|                         |                                                              |
|-------------------------|--------------------------------------------------------------|
| ACM Order Department    | Phone: 1-800-342-6626                                        |
| P.O. BOX 11405          | (U.S.A. and Canada)                                          |
| Church Street Station   | +1-212-626-0500                                              |
| New York, NY 10286-1405 | (All other countries)                                        |
|                         | Fax: +1-212-944-1318                                         |
|                         | E-mail: <a href="mailto:acmhelp@acm.org">acmhelp@acm.org</a> |

Cover photo by John O'Neill / Licensed under CC-BY-SA-3.0 / Cropped from original at  
[https://commons.wikimedia.org/wiki/File:Downtown\\_St.\\_Petersburg\\_Florida\\_from\\_Marina.png](https://commons.wikimedia.org/wiki/File:Downtown_St._Petersburg_Florida_from_Marina.png)

**Production:** Conference Publishing Consulting  
D-94034 Passau, Germany, [info@conference-publishing.com](mailto:info@conference-publishing.com)

## 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  
Adam Chlipala

Carnegie Mellon University, USA  
MIT, USA

### POPL'16 General Chair

Rastislav Bodik

University of Washington, USA

### Steering Committee Chair

Zhong Shao

Yale University, USA

## Steering Committee

Andrew Appel  
Nikolaj Bjørner  
Georges Gonthier  
John Harrison  
Chris Hawblitzel  
Gerwin Klein  
Xavier Leroy  
Dale Miller  
Tobias Nipkow  
Michael Norrish  
Zhong Shao  
Alwen Tiu

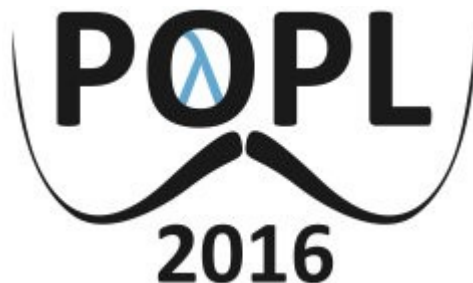
Princeton University, USA  
Microsoft Research Redmond, USA  
Microsoft Research Cambridge, UK  
Intel Corporation, USA  
Microsoft Research Redmond, USA  
NICTA, Australia  
Inria, France  
Inria, France  
Technische Universität München, Germany  
NICTA, Australia  
Yale University, USA  
Nanyang Technological 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           | Zhaohui 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 — <i>Ohio State University, USA</i> . . . . . | 1 |
|------------------------------------------------------------------|---|

### Dependent Type Practice (Invited Talk)

|                                                              |   |
|--------------------------------------------------------------|---|
| Leonardo de Moura — <i>Microsoft Research, USA</i> . . . . . | 2 |
|--------------------------------------------------------------|---|

## Verifying Imperative Programs

### Higher-Order Representation Predicates in Separation Logic

|                                                     |   |
|-----------------------------------------------------|---|
| Arthur Charguéraud — <i>Inria, France</i> . . . . . | 3 |
|-----------------------------------------------------|---|

### A Unified Coq Framework for Verifying C Programs with Floating-Point Computations

|                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------|----|
| Tahina Ramananandro, Paul Mountcastle, Benoît Meister, and Richard Lethin — <i>Reservoir Labs, USA</i> . . . . . | 15 |
|------------------------------------------------------------------------------------------------------------------|----|

### Refinement Based Verification of Imperative Data Structures

|                                                      |    |
|------------------------------------------------------|----|
| Peter Lammich — <i>TU München, Germany</i> . . . . . | 27 |
|------------------------------------------------------|----|

## Design and Implementation of Theorem Provers

### The Vampire and the FOOL

|                                                                                                                                                               |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Evgenii Kotelnikov, Laura Kovács, Giles Reger, and Andrei Voronkov — <i>Chalmers University of Technology, Sweden; University of Manchester, UK</i> . . . . . | 37 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----|

### Improving Automation in Interactive Theorem Provers by Efficient Encoding of Lambda-Abstractions

|                                                                   |    |
|-------------------------------------------------------------------|----|
| Łukasz Czajka — <i>University of Innsbruck, Austria</i> . . . . . | 49 |
|-------------------------------------------------------------------|----|

### Towards a Mizar Environment for Isabelle: Foundations and Language

|                                                                                                                                                                                        |    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Cezary Kaliszyk, Karol Pąk, and Josef Urban — <i>University of Innsbruck, Austria; University of Białystok, Poland; Czech Technical University in Prague, Czech Republic</i> . . . . . | 58 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|

## Mathematics

### A Modular, Efficient Formalisation of Real Algebraic Numbers

|                                                                                 |    |
|---------------------------------------------------------------------------------|----|
| Wenda Li and Lawrence C. Paulson — <i>University of Cambridge, UK</i> . . . . . | 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 — <i>Inria, France; IMDEA Software Institute, Spain</i> . . . . . | 76 |
|---------------------------------------------------------------------------------------------------------------------------------------|----|

### Formalizing Jordan Normal Forms in Isabelle/HOL

|                                                                                      |    |
|--------------------------------------------------------------------------------------|----|
| René Thiemann and Akihisa Yamada — <i>University of Innsbruck, Austria</i> . . . . . | 88 |
|--------------------------------------------------------------------------------------|----|

### Formalization of a Newton Series Representation of Polynomials

|                                                               |     |
|---------------------------------------------------------------|-----|
| Cyril Cohen and Boris Djalal — <i>Inria, France</i> . . . . . | 100 |
|---------------------------------------------------------------|-----|

## Foundations

### A Logic of Proofs for Differential Dynamic Logic: Toward Independently Checkable Proof Certificates for Dynamic Logics

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| Nathan Fulton and André Platzer — <i>Carnegie Mellon University, USA</i> . . . . . | 110 |
|------------------------------------------------------------------------------------|-----|

### Constructing the Propositional Truncation using Non-recursive HITs

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| Floris van Doorn — <i>Carnegie Mellon University, USA</i> . . . . . | 122 |
|---------------------------------------------------------------------|-----|

### A Nominal Exploration of Intuitionism

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| Vincent Rahli and Mark Bickford — <i>University of Luxembourg, Luxembourg; Cornell University, USA</i> . . . . . | 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