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

Association for
Computing Machinery

Advancing Computing as a Science & Profession

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

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, 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:

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

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`

Production: Conference Publishing Consulting
D-94034 Passau, Germany, 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	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 Hriţcu	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

Keynotes

Verifying Imperative Programs

Design and Implementation of Theorem Provers

Mathematics

Foundations

Verification for Concurrent and Distributed Systems

Compiler Verification