

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Alfred Kobsa

*University of California, Irvine, CA, USA*

Friedemann Mattern

*ETH Zurich, Switzerland*

John C. Mitchell

*Stanford University, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz

*University of Bern, Switzerland*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Germany*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbruecken, Germany*

Chris Hawblitzel Dale Miller (Eds.)

# Certified Programs and Proofs

Second International Conference, CPP 2012  
Kyoto, Japan, December 13-15, 2012  
Proceedings



Springer

Volume Editors

Chris Hawblitzel

Microsoft Research Redmond, WA, USA

E-mail: [chris.hawblitzel@microsoft.com](mailto:chris.hawblitzel@microsoft.com)

Dale Miller

INRIA Saclay and LIX, Ecole Polytechnique, Palaiseau Cedex, France

E-mail: [dale@lix.polytechnique.fr](mailto:dale@lix.polytechnique.fr)

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-35307-9

e-ISBN 978-3-642-35308-6

DOI 10.1007/978-3-642-35308-6

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: Applied for

CR Subject Classification (1998): F.3.1, F.4.1, D.3.3, I.2.3, D.2.4, D.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media ([www.springer.com](http://www.springer.com))

# Preface

This volume contains the proceedings of the 2nd International Conference on Certified Programs and Proofs (CPP 2012) held during 13–15 December 2012 in Kyoto, Japan.

The CPP series of meetings aims to cover those topics in computer science and mathematics in which certification via formal techniques is crucial. This year's edition of CPP was co-located with APLAS 2012 (Asian Symposium on Programming Languages and Systems); similarly, CPP 2011 and APLAS 2011 were co-located in Taiwan. Both CPP 2011 and CPP 2012 took place in Asia in order to provide a focus point for the work on certification that is occurring there. The plan is to eventually locate CPP in Europe and North America as well as in Asia. A manifesto for CPP, written by Jean-Pierre Jouannaud and Zhong Shao, appears in the proceedings of CPP 2011 (LNCS 7086).

We are pleased that Gilles Barthe and Naoki Kobayashi accepted our invitation to be invited speakers for CPP 2012 and that Xavier Leroy and Greg Morrisett accepted to be keynote speakers addressing both APLAS 2012 and CPP 2012.

The program committee for CPP 2012 was composed of 18 researchers from 12 countries. We received a total of 37 submissions and eventually accepted 18 papers. Every submission was reviewed by at least 4 program committee members and their selected reviewers.

We wish to thank the program committee members and their reviewers for their efforts in helping to evaluate the submissions: it was a privilege to work with them. The EasyChair conference management system helped us to deal with all aspects of putting together our program. It was a pleasure to work with Jacques Garrigue, the General Chair for CPP 2012, and with Atsushi Igarashi and Ranjit Jhala who were, respectively, the General Chair and the Program Committee Chair for APLAS 2012. We also wish to thank the invited speakers, the authors of submitted papers, and the reviewers for their interest and strong support of this new conference series. Finally, we thank Nagoya University Graduate School of Mathematics for institutional sponsorship of this meeting.

October 2012

Chris Hawblitzel  
Dale Miller

# Organization

## Organizing Committee

Jacques Garrigue  
Atsushi Igarashi

Nagoya University, Japan  
Kyoto University, Japan

## CPP Steering Committee

Andrew Appel  
Nikolaj Bjørner  
Georges Gonthier  
John Harrison  
Jean-Pierre Jouannaud  
(Co-chair)  
Gerwin Klein  
Tobias Nipkow  
Zhong Shao (Co-chair)

Princeton University, USA  
Microsoft Research Redmond, USA  
Microsoft Research Cambridge, UK  
Intel Corporation, USA  
INRIA, France and Tsinghua University, China  
NICTA, Australia  
Technische Universität München, Germany  
Yale University, USA

## Program Committee

Stefan Berghofer  
Wei-Ngan Chin  
Adam Chlipala  
Mike Dodds  
Amy Felty  
Xinyu Feng  
Herman Geuvers

Secunet Security Networks AG, Germany  
National Univ. of Singapore, Singapore  
MIT, USA  
University of Cambridge, UK  
University of Ottawa, Canada  
Toyota Technological Institute at Chicago, USA  
Radboud University Nijmegen,  
The Netherlands

Robert Harper  
Chris Hawblitzel  
Gerwin Klein  
Laura Kovacs  
Rupak Majumdar  
Dale Miller  
Lawrence Paulson  
Frank Piessens  
Randy Pollack  
Bow-Yaw Wang  
Santiago Zanella Béguelin

Carnegie Mellon University, USA  
Microsoft Research Redmond, USA  
NICTA and UNSW, Australia  
TU Vienna, Austria  
UCLA, USA  
INRIA, France  
University of Cambridge, UK  
Katholieke Universiteit Leuven, Belgium  
University of Edinburgh, UK  
Academia Sinica, Taiwan  
IMDEA Software Institute, Spain

## Additional Reviewers

Avigad, Jeremy  
Bourke, Timothy  
Brotherston, James  
Bulwahn, Lukas  
Campbell, Brian  
Capretta, Venanzio  
Chang, Bor-Yuh Evan  
Charguéraud, Arthur  
Chaudhuri, Kaustuv  
Costea, Andreea  
David, Cristina  
Dixon, Lucas  
Ellison, Chucky  
Gherghina, Cristian  
Hoefner, Peter  
Hölzl, Johannes  
Jackson, Paul  
Kloos, Johannes  
Kozen, Dexter  
Krebbers, Robbert  
Le, Quang Loc  
Le, Ton-Chanh  
Mahboubi, Assia  
Matichuk, Daniel  
McKinna, James  
Memarian, Kayvan

Merz, Stephan  
Moskal, Michał  
Muehlberg, Jan Tobias  
Murray, Toby  
Nakata, Keiko  
Nigam, Vivek  
Norrish, Michael  
O'Connor, Russell  
Pichardie, David  
Platzer, André  
Schmidt, Renate  
Scott, Owens  
Sergey, Ilya  
Sewell, Thomas  
Smans, Jan  
Stampoulis, Antonis  
Starostin, Artem  
Ta, Quang-Trung  
Tahar, Sofiene  
Théry, Laurent  
Tiu, Alwen  
Tuerk, Thomas  
van der Weegen, Eelis  
Vogels, Frederic  
Wickerson, John  
Wiedijk, Freek

# Table of Contents

Scalable Formal Machine Models . . . . .	1
<i>Greg Morrisett</i>	
Mechanized Semantics for Compiler Verification . . . . .	4
<i>Xavier Leroy</i>	
Automation in Computer-Aided Cryptography: Proofs, Attacks and Designs . . . . .	7
<i>Gilles Barthe, Benjamin Grégoire, César Kunz, Yassine Lakhnech, and Santiago Zanella Béguelin</i>	
Program Certification by Higher-Order Model Checking . . . . .	9
<i>Naoki Kobayashi</i>	
A Formally-Verified Alias Analysis . . . . .	11
<i>Valentin Robert and Xavier Leroy</i>	
Mechanized Verification of Computing Dominators for Formalizing Compilers . . . . .	27
<i>Jianzhou Zhao and Steve Zdancewic</i>	
On the Correctness of an Optimising Assembler for the Intel MCS-51 Microprocessor . . . . .	43
<i>Dominic P. Mulligan and Claudio Sacerdoti Coen</i>	
An Executable Semantics for CompCert C . . . . .	60
<i>Brian Campbell</i>	
Producing Certified Functional Code from Inductive Specifications . . . . .	76
<i>Pierre-Nicolas Tollitte, David Delahaye, and Catherine Dubois</i>	
The New Quickcheck for Isabelle: Random, Exhaustive and Symbolic Testing under One Roof . . . . .	92
<i>Lukas Bulwahn</i>	
Proving Concurrent Noninterference . . . . .	109
<i>Andrei Popescu, Johannes Hölzl, and Tobias Nipkow</i>	
Noninterference for Operating System Kernels . . . . .	126
<i>Toby Murray, Daniel Matichuk, Matthew Brassil, Peter Gammie, and Gerwin Klein</i>	
Compositional Verification of a Baby Virtual Memory Manager . . . . .	143
<i>Alexander Vaynberg and Zhong Shao</i>	

Shall We Juggle, Coinductively? .....	160
<i>Keisuke Nakano</i>	
Proof Pearl: Abella Formalization of $\lambda$ -Calculus Cube Property .....	173
<i>Beniamino Accattoli</i>	
A String of Pearls: Proofs of Fermat’s Little Theorem .....	188
<i>Hing-Lun Chan and Michael Norrish</i>	
Compact Proof Certificates for Linear Logic .....	208
<i>Kaustuv Chaudhuri</i>	
Constructive Completeness for Modal Logic with Transitive Closure ....	224
<i>Christian Doczkal and Gert Smolka</i>	
Rating Disambiguation Errors .....	240
<i>Andrea Asperti and Wilmer Ricciotti</i>	
A Formal Proof of Square Root and Division Elimination in Embedded Programs .....	256
<i>Pierre Neron</i>	
Coherent and Strongly Discrete Rings in Type Theory .....	273
<i>Thierry Coquand, Anders Mörberg, and Vincent Siles</i>	
Improving Real Analysis in Coq: A User-Friendly Approach to Integrals and Derivatives .....	289
<i>Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond</i>	
<b>Author Index</b> .....	<b>305</b>