

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

Rajeev Joshi Peter Müller
Andreas Podelski (Eds.)

Verified Software: Theories, Tools, Experiments

4th International Conference, VSTTE 2012
Philadelphia, PA, USA, January 28-29, 2012
Proceedings

Volume Editors

Rajeev Joshi
MS 301-285
4800 Oak Grove Drive, Pasadena, CA 91109, USA
E-mail: rajeev.joshi@jpl.nasa.gov

Peter Müller
ETH Zürich
Universitätstr. 6, 8092 Zürich, Switzerland
E-mail: peter.mueller@inf.ethz.ch

Andreas Podelski
University of Freiburg
Department of Computer Science
Georges-Köhler-Allee 52, 79110 Freiburg, Germany
E-mail: podelski@informatik.uni-freiburg.de

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27704-7 e-ISBN 978-3-642-27705-4
DOI 10.1007/978-3-642-27705-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011944848

CR Subject Classification (1998): D.2, F.3, D.3, D.1, C.2, F.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© 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)

Preface

This volume contains the papers presented at the 4th International Conference on Verified Software: Theories, Tool and Experiments (VSTTE), which was held in Philadelphia, USA, during January 28–29, 2012. Historically, the conference originated from the Verified Software Initiative (VSI), a cooperative, international initiative directed at the scientific challenges of large-scale software verification. The inaugural VSTTE conference was held at ETH Zurich in October 2005. Starting in 2008, the conference became a biennial event: VSTTE 2008 was held in Toronto, and VSTTE 2010 was held in Edinburgh.

The goal of the VSTTE conference is to advance the state of the art through the interaction of theory development, tool evolution, and experimental validation. Topics of interest include:

- Specification and verification techniques
- Tool support for specification languages
- Tool for various design methodologies
- Tool integration and plug-ins
- Automation in formal verification
- Tool comparisons and benchmark repositories
- Combination of tools and techniques (e.g., formal vs. semiformal, software specification vs. engineering techniques)
- Customizing tools for particular applications
- Challenge problems
- Refinement methodologies
- Requirements modeling
- Specification languages
- Specification/verification case studies
- Software design methods
- Program logic

The conference received 54 submissions, of which 20 were accepted after a rigorous review process, for an acceptance rate of 37%.

The conference included two invited talks, by Rupak Majumdar (Max Planck Institute for Software Systems) and Wolfgang Paul (Saarland University), and two tutorials, by Rustan Leino (Microsoft Research) and Francesco Logozzo (Microsoft Research).

A software verification competition was also held in advance of the main conference. This competition consisted of five independent programs, which had to be verified using automated verification tools. The competition was held online, November 8–10, 2011, and was a great success, with 29 participating teams, comprising 79 individuals, and 22 verification tools. Competition results were announced on December 5, 2011.

We would like to thank the invited speakers, all submitting authors, the organizers of the verification competition, the Steering Committee, the General Chair, the external reviewers, and especially the Program Committee, who put in a lot of hard work into reviewing and selecting the papers that appear in this volume.

November 2011

Rajeev Joshi
Peter Müller
Andreas Podelski

Organization

Program Committee

Clark Barrett	New York University, USA
Lars Birkedal	IT University of Copenhagen, Denmark
Patrick Cousot	Courant Institute - New York University and École normale supérieure, USA and France
Leonardo De Moura	Microsoft Research, USA
Jean-Christophe Filliatre	CNRS, France
John Hatcliff	Kansas State University, USA
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Ranjit Jhala	UC San Diego, USA
Rajeev Joshi	Laboratory for Reliable Software, Jet Propulsion Laboratory, USA
Gerwin Klein	NICTA and UNSW, Australia
Viktor Kuncak	EPFL, Switzerland
Gary T. Leavens	University of Central Florida, USA
Rustan Leino	Microsoft Research, USA
Panagiotis Manolios	Northeastern University, USA
Peter Müller	ETH Zurich, Switzerland
Tobias Nipkow	TU Munich, Germany
Matthew Parkinson	Microsoft Research, UK
Corina Pasareanu	CMU/NASA Ames Research Center, USA
Wolfgang Paul	Saarland University, Germany
Andreas Podelski	University of Freiburg, Germany
Natasha Sharygina	Università della Svizzera Italiana, Switzerland
Willem Visser	Stellenbosch University, South Africa
Thomas Wies	IST Austria

Additional Reviewers

Alberti, Francesco	Chlipala, Adam
Andronick, June	Daum, Matthias
Apel, Sven	Dinsdale-Young, Thomas
Bagherzadeh, Mehdi	Dross, Claire
Bengtson, Jesper	Fedyukovich, Grigory
Blanchet, Bruno	Feret, Jérôme
Boyton, Andrew	Goldberg, Eugene
Brim, Lubos	Greenaway, David
Butterfield, Andrew	Gvero, Tihomir
Chamarthi, Harsh Raju	Hadarean, Liana

VIII Organization

Haddad, Ghaith
Hansen, Michael R.
Hildebrandt, Thomas
Hobor, Aquinas
Hojjat, Hossein
Hussain, Faraz
Jacobs, Swen
Jain, Mitesh
Jeong, Mina
Jovanovic, Dejan
King, Tim
Kolanski, Rafal
Lahiri, Shuvendu
Laviron, Vincent
Losa, Giuliano
Martel, Matthieu
Massé, Damien
Mauborgne, Laurent
Mery, Dominique
Milicevic, Aleksandar
Miné, Antoine

Murray, Toby
Neis, Georg
Norrish, Michael
Ouaknine, Joel
Owens, Scott
Papavasileiou, Vasilis
Paskevich, Andrei
Pichardie, David
Rollini, Simone Fulvio
Rozier, Kristin Yvonne
Sery, Ondrej
Smans, Jan
Suter, Philippe
Svendsen, Kasper
Tkachuk, Oksana
Tsitovich, Aliaksei
Vogels, Frédéric
Vujosevic-Janicic, Milena
Wang, Wei
Wickerson, John
Zufferey, Damien

Table of Contents

Cyber War, Formal Verification and Certified Infrastructure	1
<i>Wolfgang Paul</i>	
A Certified Multi-prover Verification Condition Generator	2
<i>Paolo Herms, Claude Marché, and Benjamin Monate</i>	
Integrated Semantics of Intermediate-Language C and Macro-Assembler for Pervasive Formal Verification of Operating Systems and Hypervisors from VerisoftXT	18
<i>Sabine Schmaltz and Andrey Shadrin</i>	
The Location Linking Concept: A Basis for Verification of Code Using Pointers	34
<i>Gregory Kulczycki, Hampton Smith, Heather Harton, Murali Sitaraman, William F. Ogden, and Joseph E. Hollingsworth</i>	
Verifying Implementations of Security Protocols by Refinement	50
<i>Nadia Polikarpova and Michał Moskal</i>	
Deciding Functional Lists with Sublist Sets	66
<i>Thomas Wies, Marco Muñoz, and Viktor Kuncak</i>	
Developing Verified Programs with Dafny	82
<i>K. Rustan M. Leino</i>	
Verifying Two Lines of C with Why3: An Exercise in Program Verification	83
<i>Jean-Christophe Filliâtre</i>	
Development and Evaluation of LAV: An SMT-Based Error Finding Platform	98
<i>Milena Vujošević-Janičić and Viktor Kuncak</i>	
A Lightweight Technique for Distributed and Incremental Program Verification	114
<i>Martin Brain and Florian Schanda</i>	
A Comparison of Intermediate Verification Languages: Boogie and Sireum/Pilar	130
<i>Loren Segal and Patrice Chalin</i>	
LLBMC: Bounded Model Checking of C and C++ Programs Using a Compiler IR	146
<i>Florian Merz, Stephan Falke, and Carsten Sinz</i>	

The Marriage of Exploration and Deduction	162
<i>Rupak Majumdar</i>	
Modeling and Validating the Train Fare Calculation and Adjustment System Using VDM++	163
<i>Nguyen Van Tang, Daisuke Souma, Goro Hatayama, and Hitoshi Ohsaki</i>	
Formalized Verification of Snapshotable Trees: Separation and Sharing	179
<i>Hannes Mehnert, Filip Sieczkowski, Lars Birkedal, and Peter Sestoft</i>	
Comparing Verification Condition Generation with Symbolic Execution: An Experience Report	196
<i>Ioannis T. Kassios, Peter Müller, and Malte Schwerhoff</i>	
Verification of TLB Virtualization Implemented in C	209
<i>Eyad Alkassar, Ernie Cohen, Mikhail Kovalev, and Wolfgang J. Paul</i>	
Formalization and Analysis of Real-Time Requirements: A Feasibility Study at BOSCH	225
<i>Amalinda Post and Jochen Hoenicke</i>	
Our Experience with the CodeContracts Static Checker (Invited Tutorial)	241
<i>Francesco Logozzo</i>	
Isabelle/ <i>Circus</i> : A Process Specification and Verification Environment	243
<i>Abderrahmane Feliachi, Marie-Claude Gaudel, and Burkhart Wolff</i>	
Termination Analysis of Imperative Programs Using Bitvector Arithmetic	261
<i>Stephan Falke, Deepak Kapur, and Carsten Sinz</i>	
Specifying and Verifying the Correctness of Dynamic Software Updates	278
<i>Christopher M. Hayden, Stephen Magill, Michael Hicks, Nate Foster, and Jeffrey S. Foster</i>	
Symbolic Execution Enhanced System Testing	294
<i>Misty Davies, Corina S. Păsăreanu, and Vishwanath Raman</i>	
Infeasible Code Detection	310
<i>Cristiano Bertolini, Martin Schäff, and Pascal Schweitzer</i>	
Author Index	327