Lecture Notes in Computer Science 2937

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Hong Kong
London
Milan
Paris
Tokyo

Bernhard Steffen Giorgio Levi (Eds.)

Verification, Model Checking, and Abstract Interpretation

5th International Conference, VMCAI 2004
Venice, Italy, January 11-13, 2004
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Bernhard Steffen
Universität Dortmund, LS V
Baroper Str. 301, 44221 Dortmund, Germany
E-mail: steffen@cs.uni-dortmund.de

Giorgio Levi
Università di Pisa, Dipartimento di Informatica
Via Buonarroti, 2, 56100 Pisa, Italy
E-mail: levi@di.unipi.it

Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): F.3.1-2, D.3.1, D.2.4

ISSN 0302-9743
ISBN 3-540-20803-8 Springer-Verlag Berlin Heidelberg New York

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10975695 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the 5th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2004), held in Venice, January 11–13, 2004, in conjunction with POPL 2004, the 31st Annual Symposium on Principles of Programming Languages, January 14–16, 2004. The purpose of VMCAI is to provide a forum for researchers from three communities—verification, model checking, and abstract interpretation—which will facilitate interaction, cross-fertilization, and the advance of hybrid methods that combine the three areas. With the growing need for formal tools to reason about complex, infinite-state, and embedded systems, such hybrid methods are bound to be of great importance.

Topics covered by VMCAI include program verification, static analysis techniques, model checking, program certification, type systems, abstract domains, debugging techniques, compiler optimization, embedded systems, and formal analysis of security protocols.

This year's meeting follows the four previous events in Port Jefferson (1997), Pisa (1998), Venice (2002), LNCS 2294 and New York (2003), LNCS 2575. In particular, we thank VMCAI 2003's sponsor, the Courant Institute at New York University, for allowing us to apply a monetary surplus from the 2003 meeting to this one.

The program committee selected 22 papers out of 68 on the basis of three reviews. The principal criteria were relevance and quality. The program of VMCAI 2004 included, in addition to the research papers,

- a keynote speech by David Harel (Weizmann Institute, Israel) on *A Grand Challenge for Computing: Full Reactive Modeling of a Multicellular Animal*,
- an invited talk by Dawson Engler (Stanford University, USA) on *Static Analysis Versus Software Model Checking for Bug Finding*,
- an invited talk by Mooly Sagiv (Tel Aviv University, Israel) called *On the Expressive Power of Canonical Abstraction*, and
- a tutorial by Joshua D. Guttman (Mitre, USA) on *Security, Protocols, and Trust*.

We would like to thank the Program Committee members and the reviewers, without whose dedicated effort the conference would not have been possible. Our thanks go also to the Steering Committee members for helpful advice, to Agostino Cortesi, the Local Arrangements Chair, who also handled the conference's Web site, and to David Schmidt, whose expertise and support was invaluable for the budgeting. Special thanks are due to Martin Karusseit for installing, managing, and taking care of the METAFrame Online Conference Service, and to Claudia Herbers, who, together with Alfred Hofmann and his team at Springer-Verlag, collected the final versions and prepared the proceedings.

Special thanks are due to the institution that helped sponsor this event, the Department of Computer Science of Ca' Foscari University, and to the professional organizations that support the event: VMCAI 2004 is held in cooperation with ACM and is sponsored by EAPLS.

January 2004 Bernhard Steffen

Steering Committee

Agostino Cortesi (Italy)
E. Allen Emerson (USA)
Giorgio Levi (Italy)
Andreas Podelski (Germany)
Thomas W. Reps (USA)
David A. Schmidt (USA)
Lenore Zuck (USA)

Program Committee

Chairs: Giorgio Levi (University of Pisa)
Bernhard Steffen (Dortmund University)

Ralph Back (Åbo Akademi University, Finland)
Agostino Cortesi (Università Ca' Foscari di Venezia, Italy)
Radhia Cousot (CNRS and École Polytechnique, France)
Susanne Graf (VERIMAG Grenoble, France)
Radu Grosu (SUNY at Stony Brook, USA)
Orna Grumberg (Technion, Israel)
Gerhard Holzmann (Bell Laboratories, USA)
Yassine Lakhnech (Université Joseph Fourier, France)
Jim Larus (Microsoft Reseach, USA)
Markus Müller-Olm (FernUniversität in Hagen, Germany)
Hanne Riis Nielson (Technical University of Denmark, Denmark)
David A. Schmidt (Kansas State University, USA)
Lenore Zuck (New York University, USA)

Reviewers

Rajeev Alur
Roberto Bagnara
Ittai Balaban
Rudolf Berghammer
Chiara Bodei
Victor Bos
Dragan Bosnacki
Marius Bozga
Liana Bozga
Chiara Braghin
Roberto Bruni
Glenn Bruns
Sagar Chaki
Patrick Cousot
Silvia Crafa
Pierpaolo Degano
Benet Devereux
Agostino Dovier
Christian Ene
Javier Esparza
Jérôme Feret
Jean-Claude Fernandez
Gianluigi Ferrari
Riccardo Focardi
Martin Fränzle
John Gallagher
Roberto Giacobazzi
Arie Gurfinkel
Rene Rydhof Hansen
Jonathan Herzog
Patricia Hill
Frank Huch
Radu Iosif
Romain Janvier
Salvatore La Torre
Flavio Lerda
Francesca Levi
Flaminia Luccio
Jens Knoop
Daniel Kroening
Damiano Macedonio
Monika Maidl
Oded Maler
Damien Massé
Laurent Mauborgne
Fred Mesnard
Antoine Miné
Jean-François Monin
David Monniaux
Laurent Mounier
Kedar Namjoshi
Flemming Nielson
Sinha Nishant
Iulian Ober
Joël Ouaknine
Carla Piazza
Amir Pnueli
Cory Plock
Shaz Qadeer
Sriram Rajamani
Xavier Rival
Sabina Rossi
Grigore Rosu
Oliver Rüthing
Nicoletta Sabadini
Ursula Scheben
Axel Simon
Eli Singerman
Francesca Scozzari
Margaret H. Smith
Muralidhar Talupur
Simone Tini
Tayssir Touili
Stavros Tripakis
Enrico Tronci
Helmut Veith
Andreas Wolf
Ben Worrell
James Worrell
Aleksandr Zaks

Table of Contents

Formal Methods II

Software Checking

Invited Talk

Software Checking

Liveness and Completeness

Formal Methods III

Key Note

Preface

This volume contains the proceedings of the 5th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2004), held in Venice, January 11–13, 2004, in conjunction with POPL 2004, the 31st Annual Symposium on Principles of Programming Languages, January 14–16, 2004. The purpose of VMCAI is to provide a forum for researchers from three communities—verification, model checking, and abstract interpretation—which will facilitate interaction, cross-fertilization, and the advance of hybrid methods that combine the three areas. With the growing need for formal tools to reason about complex, infinite-state, and embedded systems, such hybrid methods are bound to be of great importance.

Topics covered by VMCAI include program verification, static analysis techniques, model checking, program certification, type systems, abstract domains, debugging techniques, compiler optimization, embedded systems, and formal analysis of security protocols.

This year's meeting follows the four previous events in Port Jefferson (1997), Pisa (1998), Venice (2002), LNCS 2294 and New York (2003), LNCS 2575. In particular, we thank VMCAI 2003's sponsor, the Courant Institute at New York University, for allowing us to apply a monetary surplus from the 2003 meeting to this one.

The program committee selected 22 papers out of 68 on the basis of three reviews. The principal criteria were relevance and quality. The program of VMCAI 2004 included, in addition to the research papers,

- a keynote speech by David Harel (Weizmann Institute, Israel) on *A Grand Challenge for Computing: Full Reactive Modeling of a Multicellular Animal*,
- an invited talk by Dawson Engler (Stanford University, USA) on *Static Analysis Versus Software Model Checking for Bug Finding*,
- an invited talk by Mooly Sagiv (Tel Aviv University, Israel) called *On the Expressive Power of Canonical Abstraction*, and
- a tutorial by Joshua D. Guttman (Mitre, USA) on *Security, Protocols, and Trust*.

We would like to thank the Program Committee members and the reviewers, without whose dedicated effort the conference would not have been possible. Our thanks go also to the Steering Committee members for helpful advice, to Agostino Cortesi, the Local Arrangements Chair, who also handled the conference's Web site, and to David Schmidt, whose expertise and support was invaluable for the budgeting. Special thanks are due to Martin Karusseit for installing, managing, and taking care of the METAFrame Online Conference Service, and to Claudia Herbers, who, together with Alfred Hofmann and his team at Springer-Verlag, collected the final versions and prepared the proceedings.

Special thanks are due to the institution that helped sponsor this event, the Department of Computer Science of Ca' Foscari University, and to the professional organizations that support the event: VMCAI 2004 is held in cooperation with ACM and is sponsored by EAPLS.

January 2004 Bernhard Steffen

Steering Committee

Agostino Cortesi (Italy)
E. Allen Emerson (USA)
Giorgio Levi (Italy)
Andreas Podelski (Germany)
Thomas W. Reps (USA)
David A. Schmidt (USA)
Lenore Zuck (USA)

Program Committee

Chairs: Giorgio Levi (University of Pisa)
Bernhard Steffen (Dortmund University)

Ralph Back (Åbo Akademi University, Finland)
Agostino Cortesi (Università Ca' Foscari di Venezia, Italy)
Radhia Cousot (CNRS and École Polytechnique, France)
Susanne Graf (VERIMAG Grenoble, France)
Radu Grosu (SUNY at Stony Brook, USA)
Orna Grumberg (Technion, Israel)
Gerhard Holzmann (Bell Laboratories, USA)
Yassine Lakhnech (Université Joseph Fourier, France)
Jim Larus (Microsoft Reseach, USA)
Markus Müller-Olm (FernUniversität in Hagen, Germany)
Hanne Riis Nielson (Technical University of Denmark, Denmark)
David A. Schmidt (Kansas State University, USA)
Lenore Zuck (New York University, USA)

Reviewers

Rajeev Alur
Roberto Bagnara
Ittai Balaban
Rudolf Berghammer
Chiara Bodei
Victor Bos
Dragan Bosnacki
Marius Bozga
Liana Bozga
Chiara Braghin
Roberto Bruni
Glenn Bruns
Sagar Chaki
Patrick Cousot
Silvia Crafa
Pierpaolo Degano
Benet Devereux
Agostino Dovier
Christian Ene
Javier Esparza
Jérôme Feret
Jean-Claude Fernandez
Gianluigi Ferrari
Riccardo Focardi
Martin Fränzle
John Gallagher
Roberto Giacobazzi
Arie Gurfinkel
Rene Rydhof Hansen
Jonathan Herzog
Patricia Hill
Frank Huch
Radu Iosif
Romain Janvier
Salvatore La Torre
Flavio Lerda
Francesca Levi
Flaminia Luccio
Jens Knoop
Daniel Kroening
Damiano Macedonio
Monika Maidl
Oded Maler
Damien Massé
Laurent Mauborgne
Fred Mesnard
Antoine Miné
Jean-François Monin
David Monniaux
Laurent Mounier
Kedar Namjoshi
Flemming Nielson
Sinha Nishant
Iulian Ober
Joël Ouaknine
Carla Piazza
Amir Pnueli
Cory Plock
Shaz Qadeer
Sriram Rajamani
Xavier Rival
Sabina Rossi
Grigore Rosu
Oliver Rüthing
Nicoletta Sabadini
Ursula Scheben
Axel Simon
Eli Singerman
Francesca Scozzari
Margaret H. Smith
Muralidhar Talupur
Simone Tini
Tayssir Touili
Stavros Tripakis
Enrico Tronci
Helmut Veith
Andreas Wolf
Ben Worrell
James Worrell
Aleksandr Zaks

Table of Contents

Formal Methods II

Software Checking

Invited Talk

Software Checking

Liveness and Completeness

Formal Methods III

Key Note