Lecture Notes in Computer Science 2575

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

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

Lenore D. Zuck
Paul C. Attie
Agostino Cortesi
Supratik Mukhopadhyay (Eds.)

Verification, Model Checking, and Abstract Interpretation

4th International Conference, VMCAI 2003
New York, NY, USA, January 9-11, 2003
Proceedings

Springer

Volume Editor

Lenore D. Zuck
Department of Computer Science, New York University
715 Broadway (7th floor), New York, NY 10003, USA
E-mail: zuck@cs.nyu.edu

Paul C. Attie
Northeastern University, College of Computer Science
360 Huntington Ave., Boston, MA 02115, USA
E-mail: attie@ccs.neu.edu

Agostino Cortesi
Venice University C'Foscari, Computer Science Department
Via Torino 155, 30170 Mestre-Venezia, Italy
E-mail: cortesi@dsi.unive.it

Supratik Mukhopadhyay
West Virginia University, Department of Computer Science and
Electrical Engineering, Morgantown, WV 26505, USA
E-mail: supratik@saul.cis.upenn.edu

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 3-540-00348-7 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP Berlin, Stefan Sossna e. K.
Printed on acid-free paper SPIN: 10872328 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the 4th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI 2003), held in New York city, January 9–11, 2003. The purpose of VMCAI was to provide a forum for researchers from three communities—Verification, Model Checking, and Abstract Interpretation—that 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.

VMCAI 2003 was the fourth VMCAI meeting. The previous three were held as workshops (Port Jefferson 1997, Pisa 1998, and Venice 2002). It is the success of the last meeting, and the wide response it generated, that made it clear the time had come to make it an annual conference.

The program committee selected 20 papers out of 43 submitted, on the basis of at least four reviews. The principal criteria were relevance and quality. The program of VMCAI 2003 included, in addition to the research papers, two invited talks, by Amir Pnueli (Weizmann and NYU) on *Model-Checking and Abstraction to the Aid of Parameterized Systems*, and Andreas Podelski (MPI) on *Software Model Checking with Abstraction Refinement*, and three tutorials, by Patrick Cousot (ENS) on *Automatic Verification by Abstract Interpretation,* A. Prasad Sistla (UIC) on *Symmetry Reductions in Model-Checking*, and Bernhard Steffen (Dortmund) on *Behaviour-Based Model Construction.* 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 also to the Steering Committee members for helpful advice. Thanks to Radu Grosu, the local arrangement chair. Special thanks are due to Ittai Balaban for installing, managing, and taking care of the START software and to Yi Fang for handling the website. Alfred Hofmann and his team at Springer-Verlag were very helpful in preparing the proceedings. We remain extremely grateful to Supratik Mukhopadhyay for help in the initial stages of this conference, and to Paul Attie and Agostino Cortesi for assistance in editing this volume.

Special thanks are due to the institutions that helped sponsor this event: the National Science Foundation (NSF), the Office of Naval Research (ONR), New York University, Ca'Foscari University of Venice, the Max Planck Institute, and the State University of New York at Stony Brook. We would like to thank Marcia Saito Eckel, Lourdes Santana, and Daisy Calderon for their administrative assistance.

January 2003 Lenore Zuck

Organization

Conference Chair

Lenore D. Zuck (New York University)

Program Committee

Rajeev Alur (University of Pennsylvania)
Paul C. Attie (Northeastern University)
Annalisa Bossi (Università Ca' Foscari di Venezia)
Agostino Cortesi (Università Ca' Foscari di Venezia)
Radhia Cousot (École Polytechnique)
Javier Esparza (University of Edinburgh)
Andrew D. Gordon (Microsoft Research Cambridge)
Radu Grosu (SUNY Stony Brook)
Joshua D. Guttman (Mitre)
Barbara König (Technische Universität München)
Salvatore LaTorre (Università di Salerno)
Giorgio Levi (Università di Pisa)
Michael Lowry (NASA Ames)
Supratik Mukhopadhyay (University of West Virginia)
Doron A. Peled (University of Warwick)
Colin P. Sterling (University of Edinburgh)
Lenore D. Zuck (New York University)

Local Arrangement Chair

Radu Grosu (SUNY Stony Brook)

Steering Committee

Agostino Cortesi (Università Ca' Foscari di Venezia)
Allen E. Emerson (University of Texas at Austin)
Giorgio Levi (Università di Pisa)
Andreas Podelski (Max-Planck-Institut für Informatik)
Thomas W. Reps (University of Wisconsin-Madison)
David A. Schmidt (Kansas State University)

Reviewers

Tuomas Aura
Roberto Barbuti
Clark Barrett
Massimo Benerecetti
Stefan Berghofer
Bruno Blanchet
Chiara Bodei
Chiara Braghin
Luca Cardelli
Witold Charatonik
Stelvio Cimato
Patrick Cousot
Bojan Cukic
Thao Dang
Roberto De Prisco
Pierpaolo Degano
Giorgio Delzanno
Catalin Dima
Allen Emerson
Kousha Etessami
Marco Faella
Yi Fang
Jérôme Feret
Gianluigi Ferrari
Gilberto Filé
Riccardo Focardi
Cédric Fournet
Roberto Giacobazzi
Roberta Gori
David Harel
Sara Kalvala
Ruggero Lanotte
Martin Lange
Ranko Lazik
Martin Leucker
Francesca Levi
Annie Liu
Monika Maidl
Rupak Majumdar
Matthieu Martel
Moreno Marzolla
Andrea Masini
Damien Masse
Barbara Masucci
Laurent Mauborgne
Antoine Miné
David Monniaux
Aniello Murano
Jan Obdrzalek
Paritosh Pandya
Carla Piazza
Amir Pnueli
Antonino Salibra
Francesco Tapparo
C.R. Ramakrishnan
Jean-Francois Raskin
Stefan Roemer
Alessandro Roncato
Sabina Rossi
Abhik Roychoudhury
Stefan Schwoon
Scott Stoller
Enea Zaffanella

Sponsoring Institutions

National Science Foundation (NSF)
Office of Naval Research (ONR)
New York University (NYU)
Università Ca' Foscari di Venezia
Max Planck Institute (MPI)
State University of New York at Stony Brook

Table of Contents

Invited Talks

Invited Tutorials

Static Analysis

Dynamic Systems

Abstract Interpretation

Model Checking I

Security Protocols

Formal Methods

Model Checking II