

Lecture Notes in Computer Science  
Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2575

**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

## Series Editors

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

## 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

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

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2003  
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.

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

## 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

Software Model Checking with Abstraction Refinement . . . . .	1
<i>Andreas Podelski</i>	
Model-Checking and Abstraction to the Aid of Parameterized Systems . . . . .	4
<i>Amir Pnueli, Lenore Zuck</i>	

## Invited Tutorials

Behavior-Based Model Construction . . . . .	5
<i>Bernhard Steffen, Hardi Hungar</i>	
Automatic Verification by Abstract Interpretation . . . . .	20
<i>Patrick Cousot</i>	
Symmetry Reductions in Model-Checking . . . . .	25
<i>Aravinda Prasad Sistla</i>	

## Static Analysis

CHASE: A Static Checker for JML's <i>Assignable</i> Clause . . . . .	26
<i>Néstor Cataño, Marieke Huisman</i>	
Abstract Interpretation-Based Certification of Assembly Code . . . . .	41
<i>Xavier Rival</i>	
Property Checking Driven Abstract Interpretation-Based Static Analysis . . . . .	56
<i>Damien Massé</i>	
Optimized Live Heap Bound Analysis . . . . .	70
<i>Leena Unnikrishnan, Scott D. Stoller, Yanhong A. Liu</i>	

## Dynamic Systems

Complexity of Nesting Analysis in Mobile Ambients . . . . .	86
<i>Chiara Braghin, Agostino Cortesi, Riccardo Focardi, Flaminia L. Luccio, Carla Piazza</i>	
Types for Evolving Communication in Safe Ambients . . . . .	102
<i>Francesca Levi</i>	



A Logical Encoding of the $\pi$ -Calculus: Model Checking Mobile Processes Using Tabled Resolution . . . . .	116
<i>Ping Yang, C.R. Ramakrishnan, Scott A. Smolka</i>	

## Abstract Interpretation

Properties of a Type Abstract Interpreter . . . . .	132
<i>Roberta Gori, Giorgio Levi</i>	
Domain Compression for Complete Abstractions . . . . .	146
<i>Roberto Giacobazzi, Isabella Mastroeni</i>	
Abstraction of Expectation Functions Using Gaussian Distributions . . . . .	161
<i>David Monniaux</i>	

## Model Checking I

Lifting Temporal Proofs through Abstractions . . . . .	174
<i>Kedar S. Namjoshi</i>	
Efficient Verification of Timed Automata with BDD-Like Data-Structures . . . . .	189
<i>Farn Wang</i>	
On the Expressiveness of 3-Valued Models . . . . .	206
<i>Patrice Godefroid, Radha Jagadeesan</i>	

## Security Protocols

Bisimulation and Unwinding for Verifying Possibilistic Security Properties . . . . .	223
<i>Annalisa Bossi, Riccardo Focardi, Carla Piazza, Sabina Rossi</i>	
Formal Verification of the Horn-Preneel Micropayment Protocol . . . . .	238
<i>Kazuhiro Ogata, Kokichi Futatsugi</i>	

## Formal Methods

Action Refinement from a Logical Point of View . . . . .	253
<i>Mila Majster-Cederbaum, Naijun Zhan, Harald Fecher</i>	
Reasoning about Layered Message Passing Systems . . . . .	268
<i>B. Meenakshi, R. Ramanujam</i>	
Using Simulated Execution in Verifying Distributed Algorithms . . . . .	283
<i>Toh Ne Win, Michael D. Ernst, Stephen J. Garland, Dilsun Kirlı, Nancy A. Lynch</i>	

**Model Checking II**

Efficient Computation of Recurrence Diameters .....	298
<i>Daniel Kroening, Ofer Strichman</i>	
Shape Analysis through Predicate Abstraction and Model Checking .....	310
<i>Dennis Dams, Kedar S. Namjoshi</i>	
<b>Author Index</b> .....	325