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

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 Lazic
Martin Leucker
Francesca Levi
Annie Liu
Monika Mäidl
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-François 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
Software Model Checking with Abstraction Refinement .......... 1
  Andreas Podelski
Model-Checking and Abstraction to the Aid of Parameterized Systems ... 4
  Amir Pnueli, Lenore Zuck

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

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

Dynamic Systems
Complexity of Nesting Analysis in Mobile Ambients ................ 86
  Chiara Braghin, Agostino Cortesi, Riccardo Focardi,
  Flaminia L. Luccio, Carla Piazza
Types for Evolving Communication in Safe Ambients ............. 102
  Francesca Levi
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Logical Encoding of the $\pi$-Calculus: Model Checking Mobile</td>
<td>116</td>
</tr>
<tr>
<td>Ping Yang, C.R. Ramakrishnan, Scott A. Smolka</td>
<td></td>
</tr>
<tr>
<td><strong>Abstract Interpretation</strong></td>
<td></td>
</tr>
<tr>
<td>Properties of a Type Abstract Interpreter</td>
<td>132</td>
</tr>
<tr>
<td>Roberta Gori, Giorgio Levi</td>
<td></td>
</tr>
<tr>
<td>Domain Compression for Complete Abstractions</td>
<td>146</td>
</tr>
<tr>
<td>Roberto Giacobazzi, Isabella Mastroeni</td>
<td></td>
</tr>
<tr>
<td>Abstraction of Expectation Functions Using Gaussian Distributions</td>
<td>161</td>
</tr>
<tr>
<td>David Monniaux</td>
<td></td>
</tr>
<tr>
<td><strong>Model Checking I</strong></td>
<td></td>
</tr>
<tr>
<td>Lifting Temporal Proofs through Abstractions</td>
<td>174</td>
</tr>
<tr>
<td>Kedar S. Namjoshi</td>
<td></td>
</tr>
<tr>
<td>Efficient Verification of Timed Automata with BDD-Like Data-Structures</td>
<td>189</td>
</tr>
<tr>
<td>Farn Wang</td>
<td></td>
</tr>
<tr>
<td>On the Expressiveness of 3-Valued Models</td>
<td>206</td>
</tr>
<tr>
<td>Patrice Godefroid, Radha Jagadeesan</td>
<td></td>
</tr>
<tr>
<td><strong>Security Protocols</strong></td>
<td></td>
</tr>
<tr>
<td>Bisimulation and Unwinding for Verifying Possibilistic Security</td>
<td>223</td>
</tr>
<tr>
<td>Properties</td>
<td></td>
</tr>
<tr>
<td>Annalisa Bossi, Riccardo Focardi, Carla Piazza, Sabina Rossi</td>
<td></td>
</tr>
<tr>
<td>Formal Verification of the Horn-Preneel Micropayment Protocol</td>
<td>238</td>
</tr>
<tr>
<td>Kazuhiro Ogata, Kokichi Futatsugi</td>
<td></td>
</tr>
<tr>
<td><strong>Formal Methods</strong></td>
<td></td>
</tr>
<tr>
<td>Action Refinement from a Logical Point of View</td>
<td>253</td>
</tr>
<tr>
<td>Mila Majster-Cederbaum, Naijun Zhan, Harald Fecher</td>
<td></td>
</tr>
<tr>
<td>Reasoning about Layered Message Passing Systems</td>
<td>268</td>
</tr>
<tr>
<td>B. Meenakshi, R. Ramanujam</td>
<td></td>
</tr>
<tr>
<td>Using Simulated Execution in Verifying Distributed Algorithms</td>
<td>283</td>
</tr>
<tr>
<td>Toh Ne Win, Michael D. Ernst, Stephen J. Garland, Dilsun Kırål, Nancy A. Lynch</td>
<td></td>
</tr>
</tbody>
</table>
Model Checking II

Efficient Computation of Recurrence Diameters ......................... 298
   Daniel Kroening, Ofer Strichman

Shape Analysis through Predicate Abstraction and Model Checking ...... 310
   Dennis Dams, Kedar S. Namjoshi

Author Index .......................................................... 325