

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Byron Cook Andreas Podelski (Eds.)

Verification, Model Checking, and Abstract Interpretation

8th International Conference, VMCAI 2007
Nice, France, January 14-16, 2007
Proceedings

Volume Editors

Byron Cook
Microsoft Research
Roger Needham Building
JJ Thomson Avenue
CB3 0FB, Cambridge, United Kingdom
E-mail: bycook@microsoft.com

Andreas Podelski
University of Freiburg
79110 Freiburg, Germany
E-mail: podelski@informatik.uni-freiburg.de

Library of Congress Control Number: 2006939351

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

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743
ISBN-10 3-540-69735-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-69735-0 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11973966 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers presented at VMCAI 2007: Verification, Model Checking and Abstract Interpretation held January 14–16, 2007 in Nice. VMCAI provides a forum for researchers from the communities of verification, model checking, and abstract interpretation, facilitating interaction, cross-fertilization, and advancement of hybrid methods that combine the three areas. This years VMCAI was held in conjunction with POPL, allowing further cross-fertilization between programming language research and the areas covered by VMCAI.

There were 85 submissions to VMCAI 2007. Each submission was reviewed by at least three Program Committee members. The committee decided to accept 21 papers. The program also includes invited talks by Tom Reps, Moshe Vardi, and Hongseok Yang and tutorials by Ken McMillan, Madhusudan Parthasarathy, and Peter Revesz.

We would like to acknowledge the financial support from Microsoft Research and Andrei Voronkov for assistance with the EasyChair conference system.

November 2006

Byron Cook
Andreas Podelski

External Reviewers

Eugene Asarin
James Avery
Ittai Balaban
Laurent Van Begin
Josh Berdine
Julien Bertrane
Ahmed Bouajjani
Marius Bozga
Thomas Brihaye
Véronique Bruyère
Peter Buchholz
Thierry Cachat
Gianfranco Ciardo
Christopher Conway
Dennis Dams
Dino Distefanno
Laurent Doyen
Bruno Dufour
Stefan Edelkamp
Jérôme Feret
Limor Fix
Martin Fränzle
Maria-del-Mar Gallardo
Yuan Gan
Pierre Ganty
Gilles Geeraerts
Naghme Ghafari
Mihaela Gheorghiu
Alex Groce
Arie Gurfinkel
Peter Habermehl
Nicolas Halbwachs
Rene Rydhof Hansen
Reinhold Heckmann
Jason Hickey
Micheal Huth
Radu Iosif
Neil Jones
Rajeev Joshi
Stefan Kiefer
Viktor Kuncak
Yassine Lakhnech
Julia Lawall

Etienne Lozes
Michael Luttenberger
Thierry Massart
Damien Massé
Antoine Miné
Torben Mogensen
David Monniaux
Madan Musuvathi
Shiva Nejati
Tobias Nipkow
Thomas Noll
Paritosh Pandya
Matthew Parkinson
Doron Peled
C.R. Ramakrishnan
Francesco Ranzato
Jakob Rehof
Xavier Rival
Oliver Rüthing
Andrey Rybalchenko
Marko Samer
Sriram Sankaranarayanan
Stefan Schwoon
Olivier Serre
Frédéric Servais
Mihaela Sighireanu
Jocelyn Simmonds
Jakob Grue Simonsen
Élodie-Jane Sims
Nishant Sinha
Viorica Sofronie
Sylvain Soliman
Fausto Spoto
Jan Strejcek
Dejvuth Suwimonteerabuth
Todd Veldhuizen
Tomas Vojnar
Ou Wei
Martin De Wulf
Hongseok Yang
Lenore Zuck

Table of Contents

Invited Talk

DIVINE: DIScovering Variables IN Executables	1
<i>Gogul Balakrishnan and Thomas Reps</i>	

Session 1

Verifying Compensating Transactions	29
<i>Michael Emmi and Rupak Majumdar</i>	
Model Checking Nonblocking MPI Programs	44
<i>Stephen F. Siegel</i>	
Model Checking Via FCFA	59
<i>Matthew Might, Benjamin Chambers, and Olin Shivers</i>	
Using First-Order Theorem Provers in the Jahob Data Structure Verification System	74
<i>Charles Bouillaguet, Viktor Kuncak, Thomas Wies, Karen Zee, and Martin Rinard</i>	

Invited Tutorial

Interpolants and Symbolic Model Checking	89
<i>K.L. McMillan</i>	

Session 2

Shape Analysis of Single-Parent Heaps	91
<i>Ittai Balaban, Amir Pnueli, and Lenore D. Zuck</i>	
An Inference-Rule-Based Decision Procedure for Verification of Heap-Manipulating Programs with Mutable Data and Cyclic Data Structures	106
<i>Zvonimir Rakamarić, Jesse Bingham, and Alan J. Hu</i>	
On Flat Programs with Lists	122
<i>Marius Bozga and Radu Iosif</i>	

Invited Talk

Automata-Theoretic Model Checking Revisited	137
<i>Moshe Y. Vardi</i>	

Session 3

Language-Based Abstraction Refinement for Hybrid System Verification 151
Felix Klaedtke, Stefan Ratschan, and Zhikun She

More Precise Partition Abstractions 167
Harald Fecher and Michael Huth

The Spotlight Principle 182
Björn Wachter and Bernd Westphal

Lattice Automata 199
Orna Kupferman and Yoad Lustig

Invited Tutorial

Learning Algorithms and Formal Verification 214
P. Madhusudan

Session 4

Constructing Specialized Shape Analyses for Uniform Change 215
Tal Lev-Ami, Mooly Sagiv, Neil Immerman, and Thomas Reps

Maintaining Doubly-Linked List Invariants in Shape Analysis with Local Reasoning 234
Sigmund Cheren and Radu Rugina

Automated Verification of Shape and Size Properties Via Separation Logic 251
Huu Hai Nguyen, Cristina David, Shengchao Qin, and Wei-Ngan Chin

Invited Talk

Towards Shape Analysis for Device Drivers 267
Hongseok Yang

Session 5

An Abstract Domain Extending Difference-Bound Matrices with Disequality Constraints 268
Mathias Péron and Nicolas Halbwachs

Cibai: An Abstract Interpretation-Based Static Analyzer for Modular Analysis and Verification of Java Classes 283
Francesco Logozzo

Symmetry and Completeness in the Analysis of Parameterized Systems	299
<i>Kedar S. Namjoshi</i>	
Better Under-Approximation of Programs by Hiding Variables	314
<i>Thomas Ball and Orna Kupferman</i>	
Invited Tutorial	
The Constraint Database Approach to Software Verification	329
<i>Peter Revesz</i>	
Session 6	
Constraint Solving for Interpolation	346
<i>Andrey Rybalchenko and Viorica Sofronie-Stokkermans</i>	
Assertion Checking Unified	363
<i>Sumit Gulwani and Ashish Tiwari</i>	
Invariant Synthesis for Combined Theories	378
<i>Dirk Beyer, Thomas A. Henzinger, Rupak Majumdar, and Andrey Rybalchenko</i>	
Author Index	395