

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

New York University, NY, 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

Radhia Cousot (Ed.)

Verification, Model Checking, and Abstract Interpretation

6th International Conference, VMCAI 2005
Paris, France, January 17-19, 2005
Proceedings

Volume Editor

Radhia Cousot

École Polytechnique, 91128 Palaiseau cedex, France

E-mail: Radhia.Cousot@polytechnique.fr

Library of Congress Control Number: 2004117275

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

ISSN 0302-9743

ISBN 3-540-24297-X 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

springeronline.com

© Springer-Verlag Berlin Heidelberg 2005

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik

Printed on acid-free paper SPIN: 11375739 06/3142 5 4 3 2 1 0

Preface

This volume contains the papers accepted for presentation at the 6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2005), which was held January 17–19, 2005 in Paris, France.

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. With the growing need for formal methods to reason about complex, infinite-state, and embedded systems, such hybrid methods are bound to be of great importance.

VMCAI 2005 received 92 submissions. Each paper was carefully reviewed, being judged according to scientific quality, originality, and relevance to the symposium topics. Following online discussions, the program committee met in Paris, France, at the École Normale Supérieure on October 30, 2004, and selected 27 papers.

In addition to the contributed papers, this volume includes contributions by outstanding invited speakers:

- Patrick Cousot (École Normale Supérieure, Paris), *Proving Program Invariance and Termination by Parametric Abstraction, Lagrangian Relaxation and Semidefinite Programming*;
- C.A.R. Hoare (Microsoft Research, Cambridge), *The Verifying Compiler, a Grand Challenge for Computing Research*;
- Amir Pnueli (New York University and Weizmann Institute of Science), *Abstraction for Liveness*.

The VMCAI 2005 program included an invited tutorial by Sriram K. Rajamani (Microsoft Research, Redmond) on *Model Checking, Abstraction and Symbolic Execution for Software*.

VMCAI 2005 was followed by workshops on Automatic Tools for Verification, Abstract Interpretation of Object-Oriented Languages, and Numerical & Symbolic Abstract Domains.

On behalf of the Program Committee, the Program Chair would like to thank the authors of the submitted papers, and the external referees, who provided timely and significant reviews. We owe special thanks to Jacques Beigbeder from the École Normale Supérieure for managing the submission site and the developers of CyberChair for the use of their software.

VMCAI 2005 was held in cooperation with the Association for Computing Machinery (ACM) and the European Association for Programming Languages and Systems (EAPLS).

Sponsoring Organizations

The 6th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2005) was held in cooperation with the Association for Computing Machinery (ACM) and the European Association for Programming Languages and Systems (EAPLS).

Program Committee

Agostino Cortesi	Università Ca' Foscari di Venezia, Italy
Radhia Cousot (Chair)	CNRS/École Polytechnique, France
E. Allen Emerson	University of Texas at Austin, USA
Roberto Giacobazzi	Università degli Studi di Verona, Italy
Chris Hankin	Imperial College London, UK
Warren A. Hunt, Jr.	University of Texas at Austin, USA
Ken McMillan	Cadence Berkeley, USA
David Monniaux	CNRS/École Normale Supérieure, France
Amir Pnueli	New York University, USA and Weizmann Institute of Science, Israel
Andreas Podelski	Max-Planck-Institut für Informatik, Germany
Francesco Ranzato	Università di Padova, Italy
Hanne Riis Nielson	Technical University of Denmark, Denmark
Shmuel Sagiv	TelAviv University, Israel
Bernhard Steffen	Universität Dortmund, Germany
Reinhard Wilhelm	Universität des Saarlandes, Germany

Steering Committee

Agostino Cortesi	Università Ca' Foscari di Venezia, Italy
E. Allen Emerson	University of Texas at Austin, USA
Giorgio Levi	Università di Pisa, Italy
Thomas W. Reps	University of Wisconsin-Madison, USA
Andreas Podelski	Max-Planck-Institut für Informatik, Germany
David A. Schmidt	Kansas State University, USA
Lenore Zuck	University of Illinois at Chicago, USA

Organizing Committee

General Chair	Radhia Cousot, CNRS/École Polytechnique
Submission Website	Jacques Beigbeder, École Normale Supérieure
Local Arrangements	Radhia Cousot, CNRS/École Polytechnique David Monniaux, CNRS/École Normale Supérieure Élodie-Jane Sims, CNRS/École Polytechnique

Referees

Nina Amla	Walid Ghandour	Jan Reineke
Egon Börger	Ursula Goltz	Tamara Rezk
Christel Baier	Sumit Gulwani	Noam Rinetzky
Clark Barrett	Jörg Hoffmann	Eike Ritter
Jörg Bauer	Hardi Hungar	Xavier Rival
Bernd Becker	Michael Huth	Grigore Rosu
Gerd Behrmann	Charles Hymans	Harald Ruess
Sergey Berezin	François Irigoin	Andrey Rybalchenko
Bruno Blanchet	Shahid Jabbar	Rene Rydhof Hansen
Thomas Bolander	Bertrand Jeannet	Antonino Salibra
Ahmed Bouajjani	Thomas Jensen	Sven Schewe
Chiara Braghin	Robert Krug	Francesca Scozzari
Mikael Buchholz	Marta Kwiatkowska	Roberto Segala
Feng Chen	Ruggero Lanotte	Helmut Seidl
Horatiu Cirstea	Fabrice le Fessant	Ohad Shacham
Nicoletta Cocco	Stefan Leue	Vitaly Shmatikov
Livio Colussi	Hanbing Liu	Élodie-Jane Sims
Scott Cotton	Francesco Logozzo	Fausto Spoto
Patrick Cousot	Markus Müller-Olm	Jean-Pierre Talpin
William D. Young	Rupak Majumdar	Francesco Tapparo
Mila Dalla Preda	Oded Maler	Stephan Thesing
Sayaki Das	Roman Manevich	Sarah Thompson
Jared Davis	Shawn Manley	Terkel Tolstrup
Jyotirmoy Deshmukh	Jacopo Mantovani	Shmuel Tyszberowicz
Agostino Dovier	Damien Massé	Antti Valmari
Klaus Dräger	Isabella Mastroeni	Tullio Vardanega
Stefan Edelkamp	Laurent Mauborgne	Arnaud Venet
Cindy Eisner	Tilman Mehler	Vinod Viswanath
Alessandro Fantechi	Flemming Nielson	Hubert Wagner
Jérôme Feret	Gethin Norman	Thomas Wahl
Gilberto Filé	Peter O'Hearn	Bernd Westphal
Jean-Christophe Filliâtre	Peter Padawitz	Thomas Wies
David Fink	Carla Piazza	Kirsten Winter
Bernd Finkbeiner	Michele Pinna	Enea Zaffanella
Riccardo Focardi	Anne Proetzsch	Damiano Zanardini
Martin Fraenzle	Oliver Rüthing	Hormoz Zarnani
Han Gao	David Rager	Qiang Zhang
Angelo Gargantini	Sandip Ray	Lenore Zuck
Samir Genaim	Erik Reeber	

Table of Contents

Invited Paper

Proving Program Invariance and Termination by Parametric Abstraction, Lagrangian Relaxation and Semidefinite Programming	1
<i>Patrick Cousot</i>	

Numerical Abstraction

Scalable Analysis of Linear Systems Using Mathematical Programming . .	25
<i>Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna</i>	
The Arithmetic-Geometric Progression Abstract Domain	42
<i>Jérôme Feret</i>	
An Overview of Semantics for the Validation of Numerical Programs	59
<i>Matthieu Martel</i>	

Invited Talk

The Verifying Compiler, a Grand Challenge for Computing Research	78
<i>C.A.R. Hoare</i>	

Verification I

Checking Herbrand Equalities and Beyond	79
<i>Markus Müller-Olm, Oliver Rüthing, and Helmut Seidl</i>	
Static Analysis by Abstract Interpretation of the Quasi-synchronous Composition of Synchronous Programs	97
<i>Julien Bertrane</i>	
Termination of Polynomial Programs	113
<i>Aaron R. Bradley, Zohar Manna, and Henny B. Sipma</i>	
Verifying Safety of a Token Coherence Implementation by Parametric Compositional Refinement	130
<i>Sebastian Burckhardt, Rajeev Alur, and Milo M.K. Martin</i>	

Invited Talk

Abstraction for Liveness	146
<i>Amir Pnueli</i>	

Heap and Shape Analysis

Abstract Interpretation with Alien Expressions and Heap Structures	147
<i>Bor-Yuh Evan Chang and K. Rustan M. Leino</i>	
Shape Analysis by Predicate Abstraction	164
<i>Ittai Balaban, Amir Pnueli, and Lenore D. Zuck</i>	
Predicate Abstraction and Canonical Abstraction for Singly-Linked Lists . .	181
<i>Roman Manevich, E. Yahav, G. Ramalingam, and Mooly Sagiv</i>	
Purity and Side Effect Analysis for Java Programs	199
<i>Alexandru Sălcianu and Martin Rinard</i>	

Abstract Model Checking

Automata as Abstractions	216
<i>Dennis Dams and Kedar S. Namjoshi</i>	
<i>Don't Know</i> in the μ -Calculus	233
<i>Orna Grumberg, Martin Lange, Martin Leucker, and Sharon Shoham</i>	
Model Checking of Systems Employing Commutative Functions	250
<i>A. Prasad Sistla, Min Zhou, and Xiaodong Wang</i>	

Model Checking

Weak Automata for the Linear Time μ -Calculus	267
<i>Martin Lange</i>	
Model Checking for Process Rewrite Systems and a Class of Action-Based Regular Properties	282
<i>Laura Bozzelli</i>	
Minimizing Counterexample with Unit Core Extraction and Incremental SAT	298
<i>ShengYu Shen, Ying Qin, and SiKun Li</i>	
I/O Efficient Directed Model Checking	313
<i>Shahid Jabbar and Stefan Edelkamp</i>	

Applied Abstract Interpretation

Verification of an Error Correcting Code by Abstract Interpretation	330
<i>Charles Hymans</i>	
Information Flow Analysis for Java Bytecode	346
<i>Samir Genaim and Fausto Spoto</i>	
Cryptographic Protocol Analysis on Real C Code	363
<i>Jean Goubault-Larrecq and Fabrice Parrennes</i>	

Bounded Model Checking

Simple Is Better: Efficient Bounded Model Checking for Past LTL 380
Timo Latvala, Armin Biere, Keijo Heljanko, and Tommi Junttila

Optimizing Bounded Model Checking for Linear Hybrid Systems 396
Erika Ábrahám, Bernd Becker, Felix Klaedtke, and Martin Steffen

Verification II

Efficient Verification of Halting Properties for MPI Programs
 with Wildcard Receives 413
Stephen F. Siegel

Generalized Typestate Checking for Data Structure Consistency 430
Patrick Lam, Viktor Kuncak, and Martin Rinard

On the Complexity of Error Explanation 448
Nirman Kumar, Viraj Kumar, and Mahesh Viswanathan

Efficiently Verifiable Conditions for Deadlock-Freedom
 of Large Concurrent Programs 465
Paul C. Attie and Hana Chockler

Author Index 483