

Lecture Notes in Computer Science

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

2694

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Radhia Cousot (Ed.)

Static Analysis

10th International Symposium, SAS 2003
San Diego, CA, USA, June 11-13, 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

Radhia Cousot
École Polytechnique, STIX
91128 Palaiseau cedex, France
E-mail: radhia.cousot@polytechnique.fr

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 Nationalbibliographie;
detailed bibliographic data is available in the Internet at <http://dnb.ddb.de>.

CR Subject Classification (1998): D.3.2-3, F.3.1-2, D.2.8, F.4.2, D.1

ISSN 0302-9743

ISBN 3-540-40325-6 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 Christian Grosche, Hamburg
Printed on acid-free paper SPIN: 10927960 06/3142 5 4 3 2 1 0

Preface

Static analysis is a research area aimed at developing principles and tools for verification and semantics-based manipulation of programs and high-performance implementations of programming languages. The series of Static Analysis symposia has served as the primary venue for presentation and discussion of theoretical, practical, and application advances in the area.

This volume contains the papers accepted for presentation at the 10th International Static Analysis Symposium (SAS 2003), which was held June 11–13, 2003 in San Diego, California, USA.

Firmly established as a leading forum in the static analysis area, SAS 2003 received 82 high-quality submissions. Each paper was carefully reviewed, being judged according to scientific quality, originality, and relevance to the symposium topics.

Following on-line discussions, the program committee met in Paris, France, at the École Normale Supérieure on March 15, 2003, and selected 25 papers. In addition to the contributed papers, this volume includes an invited paper by Manuel Hermenegildo (Technical University of Madrid and University of New Mexico) and the abstract of an invited talk by Ken McMillan (Cadence Berkeley Laboratories).

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

On this occasion, SAS was sponsored by the Association for Computing Machinery (ACM) and was held as part of the Federated Computing Research Conference (FCRC 2003). I would like to thank all organizing committee members for all their tremendous work.

Organization and Sponsor

The 10th International Static Analysis Symposium (SAS 2003) was sponsored by the Association for Computing Machinery (ACM) and was held as part of the Federated Computing Research Conference (FCRC 2003).

FCRC 2003 Organizing Committee

General Chair	Barbara Ryder, Rutgers University
Keynote Speaker Chair	Stuart Feldman, International Business Machines
Website Coordinator	Jack Davidson, University of Virginia
Support Travel Chair	Kathleen Fisher, AT&T Research
Past FCRC General Chair	David Johnson, AT&T Research
Student Activities Chair	John Karro, Oberlin College
ACM FCRC Coordinator	Donna Baglio, Association for Computing Machinery

Program Committee

Alex Aiken	University of California, Berkeley, USA
Radhia Cousot (Chair)	CNRS/École Polytechnique, France
Luddy Harrison	Intel Corporation, USA
Susan Horwitz	University of Wisconsin-Madison, USA
Andy King	University of Kent, UK
Giorgio Levi	University of Pisa, Italy
Michael Lowry	NASA Ames Research Center, USA
Laurent Mauborgne	École Normale Supérieure, France
Alan Mycroft	Cambridge University, UK
Germán Puebla	Technical University of Madrid, Spain
Francesco Ranzato	University of Padova, Italy
Shmuel Sagiv	Tel Aviv University, Israel
David Sands	Chalmers University of Technology and University of Göteborg, Sweden
Helmut Seidl	University of Trier, Germany
Mary Lou Soffa	University of Pittsburgh, USA
Harald Søndergard	University of Melbourne, Australia

Executive Committee

General Chair	Peter Lee, Carnegie Mellon University
Program Chair	Radhia Cousot, CNRS/École Polytechnique
Submission Website	Jacques Beigbeder, École Normale Supérieure
Website	Radhia Cousot, CNRS/École Polytechnique

Steering Committee

Patrick Cousot	École Normale Supérieure
Gilberto Filé	Università di Padova
David Schmidt	Kansas State University

Referees

Nava Aizikowitz
 Krzysztof Apt
 Alessandro Armando
 Roberto Bagnara
 Bruno Blanchet
 Chiara Bodei
 Howard Bowman
 Andrea Bracciali
 Guillaume Brat
 Francisco Bueno
 Peter Bunus
 Daniel Cabeza
 Manuel Carro
 Livio Colussi
 Jesus Correias
 Agostino Cortesi
 Patrick Cousot
 Ferruccio Damiani
 Marco Danelutto
 Anuj Dawar
 Bjorn De Sutter
 Saumya K. Debray
 Pierpaolo Degano
 Giorgio Delzanno
 Amer Diwan
 Nurit Dor
 Stephen A. Edwards
 Rob Ennals
 Peter Faber
 Christian Ferdinand
 Jérôme Feret
 Gilberto Filé
 Simon Frankau
 Roberto Giacobazzi
 Robert Glück
 Jose M. Gomez-Perez
 Roberta Gori
 Susanne Graf
 Jörgen Gustavsson
 Jurriaan Hage
 Les Hatton
 Bastiaan Heeren
 Nevin Heintze
 Fergus Henderson

Angel Herranz-Nieva
 Pat Hill
 Michael Hind
 Jacob Howe
 Charles Hymans
 Radha Jagadeesan
 Bertrand Jeannet
 Ranjit Jhala
 Neil Johnson
 Stefan Kahrs
 Volker Klotz
 Jens Knoop
 John Kodumal
 Francesco Logozzo
 Alan C. Lawrence
 Marina Lenisa
 Francesca Levi
 Donglin Liang
 Sandra Loosemore
 Pedro Lopez-Garcia
 Lunjin Lu
 Antoine Mineé
 Andrea Maggiolo Schettini
 Rupak Majumdar
 Roman Manevich
 Julio Mariño
 Damien Massé
 Isabella Mastroeni
 Fred Mesnard
 David Monniaux
 Jose F. Morales
 Markus Müller-Olm
 Lee Naish
 Härmel Nestra
 Nicholas Nethercote
 Karol Ostrovsky
 Linda Pagli
 Justin Pearson
 Susanna Pelagatti
 Andreas Podelski
 Corrado Priami
 Ganesan Ramalingam
 Laura Ricci
 Martin Rinard

Xavier Rival
Alexandru Salcianu
Peter Schachte
Sybille Schupp
Francesca Scozzari
Cotton Seed
Clara Segura
Peter Sestoft
Ran Shaham
Richard Sharp
Ilya Shlyakhter
Simon Frankau
Jeremy Singer
Fausto Spoto
Peter Stuckey

Zhendong Su
Martin Sulzmann
Josef Svenningsson
Walid Taha
Francesco Tapparo
Eben Upton
Arnaud Venet
Eelco Visser
Keith Wansbrough
Joe Wells
Herbert Wiklicky
Reinhard Wilhelm
Eran Yahav
Greta Yorsh
Min Zhao

Table of Contents

Static Analysis of Object-Oriented Languages

Precise Analysis of String Expressions.....	1
<i>Aske Simon Christensen, Anders Møller, and Michael I. Schwartzbach (BRICS, Department of Computer Science, University of Aarhus)</i>	
Modular Class Analysis with DATALOG.....	19
<i>Frédéric Besson and Thomas Jensen (Irisa)</i>	
Class-Level Modular Analysis for Object Oriented Languages	37
<i>Francesco Logozzo (STIX - École Polytechnique)</i>	

Static Analysis of Concurrent Languages

Checking Interference with Fractional Permissions	55
<i>John Boyland (University of Wisconsin-Milwaukee)</i>	
Message Analysis for Concurrent Languages	73
<i>Richard Carlsson, Konstantinos Sagonas, and Jesper Wilhelmsson (Computing Science Department, Uppsala University, Sweden)</i>	
Instantaneous Termination in Pure Esterel.....	91
<i>Olivier Tardieu and Robert de Simone (INRIA)</i>	
Stack Size Analysis for Interrupt-Driven Programs.....	109
<i>Krishnendu Chatterjee (University of California, Berkeley), Di Ma (Purdue University), Rupak Majumdar (University of California, Berkeley), Tian Zhao (University of Wisconsin, Milwaukee), Thomas A. Henzinger (University of California, Berkeley), and Jens Palsberg (Purdue University)</i>	

Invited Paper

Program Development Using Abstract Interpretation (And the Ciao System Preprocessor).....	127
<i>Manuel V. Hermenegildo (Technical University of Madrid and University of New Mexico), Germán Puebla, Francisco Bueno, and Pedro López-García (Technical University of Madrid)</i>	

Static Analysis of Functional Languages

Selective Tail Call Elimination	153
<i>Yasuhiko Minamide (University of Tsukuba and PRESTO, JST)</i>	
Inserting Safe Memory Reuse Commands into ML-Like Programs	171
<i>Oukseh Lee, Hongseok Yang, and Kwangkeun Yi</i> <i>(Korea Advanced Institute of Science and Technology)</i>	

Static Analysis of Procedural Languages

Weighted Pushdown Systems and Their Application to Interprocedural Dataflow Analysis	189
<i>Thomas Reps (University of Wisconsin),</i> <i>Stefan Schwoon (Universität Stuttgart), and</i> <i>Somesh Jha (University of Wisconsin)</i>	
Client-Driven Pointer Analysis	214
<i>Samuel Z. Guyer and Calvin Lin (The University of Texas at</i> <i>Austin)</i>	
Abstract Interpretation of Programs as Markov Decision Processes	237
<i>David Monniaux (CNRS/École normale supérieure)</i>	

Static Data Analysis

A Logic for Analyzing Abstractions of Graph Transformation Systems	255
<i>Paolo Baldan (Dipartimento di Informatica, Università Ca' Foscari</i> <i>Venezia, Italy),</i> <i>Barbara König (Institut für Informatik, Technische Universität</i> <i>München, Germany), and</i> <i>Bernhard König (Department of Mathematics, University of</i> <i>California, Irvine, USA)</i>	
Type Systems for Distributed Data Sharing	273
<i>Ben Liblit, Alex Aiken, and Katherine Yelick (UC Berkeley)</i>	
Z-Ranking: Using Statistical Analysis to Counter the Impact of Static Analysis Approximations	295
<i>Ted Kremenek and Dawson Engler (Stanford University)</i>	
Computer-Assisted Verification of a Protocol for Certified Email	316
<i>Martín Abadi (University of California, Santa Cruz) and</i> <i>Bruno Blanchet (École Normale Supérieure, Paris and</i> <i>Max-Planck-Institut für Informatik, Saarbrücken)</i>	

Invited Talk

Craig Interpolation and Reachability Analysis	336
<i>Ken L. McMillan (Cadence Berkeley Laboratories)</i>	

Static Linear Relation Analysis

Precise Widening Operators for Convex Polyhedra	337
<i>Roberto Bagnara (Department of Mathematics, University of Parma, Italy),</i>	
<i>Patricia M. Hill (School of Computing, University of Leeds, UK),</i>	
<i>Elisa Ricci, and Enea Zaffanella (Department of Mathematics, University of Parma, Italy)</i>	
Cartesian Factoring of Polyhedra in Linear Relation Analysis	355
<i>Nicolas Halbwachs (Verimag/CNRS),</i>	
<i>David Merchat (Verimag), and</i>	
<i>Catherine Parent-Vigouroux (Verimag/UJF)</i>	

Static Analysis Based Program Transformation

Continuation-Based Partial Evaluation without Continuations	366
<i>Peter Thiemann (Universität Freiburg)</i>	
Loop Transformations for Reducing Data Space Requirements of Resource-Constrained Applications	383
<i>Priya Unnikrishnan, Guangyu Chen, Mahmut Kandemir</i>	
<i>(Penn State Univ),</i>	
<i>Mustafa Karakoy (Imperial College, London), and</i>	
<i>Ibrahim Kolcu (UMIST, UK)</i>	
Code Compaction of Matching Single-Entry Multiple-Exit Regions	401
<i>Wen-Ke Chen, Bengu Li, and Rajiv Gupta (University of Arizona)</i>	

Static Heap Analysis

Existential Heap Abstraction Entailment Is Undecidable	418
<i>Viktor Kuncak and Martin Rinard (MIT Laboratory for Computer Science)</i>	
Typestate Verification: Abstraction Techniques and Complexity Results...	439
<i>John Field, Deepak Goyal, G. Ramalingam</i>	
<i>(IBM T.J. Watson Research Center), and</i>	
<i>Eran Yahav (Tel Aviv University)</i>	

Static Analysis of Accessed Regions in Recursive Data Structures 463
Stephen Chong and Radu Rugina (Cornell University)

Establishing Local Temporal Heap Safety Properties with Applications to
Compile-Time Memory Management..... 483
*Ran Shaham (Tel-Aviv University and IBM Haifa Research
Laboratory),
Eran Yahav (Tel-Aviv University),
Elliot Kolodner (IBM Haifa Research Laboratory),, and
Mooly Sagiv (Tel-Aviv University)*

Author Index505