

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

Roberto Giacobazzi (Ed.)

Static Analysis

11th International Symposium, SAS 2004
Verona, Italy, August 26-28, 2004
Proceedings

Volume Editor

Roberto Giacobazzi

Università degli Studi di Verona, Dipartimento di Informatica

Strada Le Grazie 15, 37134 Verona, Italy

E-mail: roberto.giacobazzi@univr.it

Library of Congress Control Number: 2004109776

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

ISSN 0302-9743

ISBN 3-540-22791-1 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 2004

Printed in Germany

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

Printed on acid-free paper SPIN: 11310426 06/3142 5 4 3 2 1 0

Preface

Static analysis is a research area aimed at developing principles and tools for verification, certification, semantics-based manipulation, and high-performance implementation of programming languages and systems. 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 11th International Static Analysis Symposium (SAS 2004), which was held August 26–28 in Verona, Italy. In response to the call for papers, 63 contributions were submitted from 20 different countries. Following on-line discussions, the Program Committee met in Verona on May 06, and selected 23 papers, basing this choice on their scientific quality, originality, and relevance to the symposium. Each paper was reviewed by at least 3 PC members or external referees. In addition to the contributed papers, this volume includes contributions by outstanding invited speakers: a full invited paper by Thomas Henzinger (University of California at Berkeley), and abstracts of the talks given by the other invited speakers, Sheila McIlraith (University of Toronto), Ehud Shapiro (Weizmann Institute) and Yannis Smaragdakis (Georgia Institute of Technology).

On the behalf of the Program Committee, the Program Chair would like to thank all the authors who submitted papers and all external referees for their careful work in the reviewing process. The Program Chair would like to thank in particular Samir Genaim, who did an invaluable, excellent job in organizing the Program Committee meeting and the structure of this volume. We would like to express our gratitude to the *Dipartimento di Informatica* and to the *Università degli Studi di Verona*, in particular to Prof. Elio Mosele (president of the university), who handled the logistical arrangements and provided financial support for organizing this event.

SAS 2004 was held concurrently with *LOPSTR 2004, International Symposium on Logic-Based Program Synthesis and Transformation*; *PEPM 2004, ACM SIGPLAN Symposium on Partial Evaluation and Program Manipulation*; and *PPDP 2004, ACM SIGPLAN International Conference on Principles and Practice of Declarative Programming*. There were also several workshops in the area of programming languages. We would like to thank Sandro Etalle (LOPSTR PC Chair), Nevin Heintze and Peter Sestoft (PEPM PC Chairs), Eugenio Moggi (PPDP General Chair), Fausto Spoto (Organizing Chair), and David Warren (PPDP PC Chair) for their help in the organization aspects. Special thanks to all the members of the Organizing Committee who worked with enthusiasm in order to make this event possible and to ENDES, specifically to Anna Chiara Caputo, for the great job she did in the local organization.

Organization

Program Committee

Thomas Ball	Microsoft, USA
Radhia Cousot	École Polytechnique, France
Roberto Giacobazzi (Chair)	Università di Verona, Italy
Chris Hankin	Imperial College London, UK
Thomas Jensen	IRISA, France
Jens Knoop	Technische Universität Wien, Austria
Giorgio Levi	Università di Pisa, Italy
Laurent Mauborgne	École Normale Supérieure, France
Andreas Podelski	Max-Planck-Institut für Informatik, Germany
German Puebla	Technical University of Madrid, Spain
Ganesan Ramalingam	IBM, USA
Francesco Ranzato	Università di Padova, Italy
Martin Rinard	Massachusetts Institute of Technology, USA
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Mary Lou Soffa	University of Pittsburgh, USA
Harald Søndergaard	University of Melbourne, Australia
Reinhard Wilhelm	Universität des Saarlandes, Germany

Steering Committee

Patrick Cousot	École Normale Supérieure, France
Gilberto Filé	Università di Padova, Italy
David Schmidt	Kansas State University, USA

Organizing Committee

Mila Dalla Preda
Samir Genaim
Isabella Mastroeni
Massimo Merro
Giovanni Scardoni
Fausto Spoto
Damiano Zanardini

Referees

Elvira Albert
M. Anton Ertl
Roberto Bagnara
Roberto Barbuti
Joerg Bauer
Michele Bugliesi
V.C. Sreedhar
Paul Caspi
Patrick Cousot
Alexandru D. Salcianu
Mila Dalla Preda
Ferruccio Damiani
Bjorn De Sutter
Bjoern Decker
Pierpaolo Degano
Nurit Dor
Manuel Fahndrich
Jérôme Feret
Gilberto Filé
Steve Fink
Bernd Finkbeiner
Cormac Flanagan
Maurizio Gabbrielli
Samir Genaim
Roberta Gori
David Grove
Daniel Hedin
Dan Hirsch
Charles Hymans
Daniel Kaestner
John Kodumal
Andreas Krall
Viktor Kuncak
Kung-Kiu Lau
Francesca Levi
Donglin Liang
Andrea Maggiolo Schettini
Isabella Mastroeni
Ken McMillan

Massimo Merro
Antoine Miné
Anders Moller
David Monniaux
Carlo Montangero
Damen Mssé
Markus Müller-Olm
Ulrich Neumerkel
Jens Palsberg
Filippo Portera
Franz Puntigam
Xavier Rival
Enric Rodríguez-Carbonell
Sabina Rossi
Salvatore Ruggieri
Andrey Rybalchenko
Rene Rydhof Hansen
Oliver Rüthing
Mooly Sagiv
Giovanni Scardoni
Dave Schmidt
Bernhard Scholz
Markus Schordan
Francesca Scozzari
Clara Segura
Helmut Seidl
Alexander Serebrenik
Vincent Simonet
Fabio Somenzi
Fausto Spoto
Zhendong Su
Francesco Tapparo
Ashish Tiwari
Thomas Wies
Sebastian Winkel
Zhe Yang
Enea Zaffanella
Damiano Zanardini
Andreas Zeller

Table of Contents

Invited Talks

Injecting Life with Computers	1
<i>Ehud Shapiro</i>	
The BLAST Query Language for Software Verification.....	2
<i>Dirk Beyer, Adam J. Chlipala, Thomas A. Henzinger, Ranjit Jhala, and Rupak Majumdar</i>	
Program Generators and the Tools to Make Them	19
<i>Yannis Smaragdakis</i>	
Towards Declarative Programming for Web Services	21
<i>Sheila McIlraith</i>	

Program and System Verification

Closed and Logical Relations for Over- and Under-Approximation of Powersets	22
<i>David A. Schmidt</i>	
Completeness Refinement in Abstract Symbolic Trajectory Evaluation	38
<i>Mila Dalla Preda</i>	
Constraint-Based Linear-Relations Analysis	53
<i>Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna</i>	
Spatial Analysis of BioAmbients	69
<i>Hanne Riis Nielson, Flemming Nielson, and Henrik Pilegaard</i>	

Security and Safety

Modular and Constraint-Based Information Flow Inference for an Object-Oriented Language	84
<i>Qi Sun, Anindya Banerjee, and David A. Naumann</i>	
Information Flow Analysis in Logical Form	100
<i>Torben Amtoft and Anindya Banerjee</i>	
Type Inference Against Races	116
<i>Cormac Flanagan and Stephen N. Freund</i>	

Pointer Analysis

Pointer-Range Analysis	133
<i>Suan Hsi Yong and Susan Horwitz</i>	
A Scalable Nonuniform Pointer Analysis for Embedded Programs	149
<i>Arnaud Venet</i>	
Bottom-Up and Top-Down Context-Sensitive Summary-Based Pointer Analysis	165
<i>Erik M. Nystrom, Hong-Seok Kim, and Wen-mei W. Hwu</i>	

Abstract Interpretation and Algorithms

Abstract Interpretation of Combinational Asynchronous Circuits	181
<i>Sarah Thompson and Alan Mycroft</i>	
Static Analysis of Gated Data Dependence Graphs	197
<i>Charles Hymans and Eben Upton</i>	
A Polynomial-Time Algorithm for Global Value Numbering	212
<i>Sumit Gulwani and George C. Necula</i>	

Shape Analysis

Quantitative Shape Analysis	228
<i>Radu Rugina</i>	
A Relational Approach to Interprocedural Shape Analysis	246
<i>Bertrand Jeannet, Alexey Loginov, Thomas Reps, and Mooly Sagiv</i>	
Partially Disjunctive Heap Abstraction	265
<i>Roman Manevich, Mooly Sagiv, Ganesan Ramalingam, and John Field</i>	

Abstract Domain and Data Structures

An Abstract Interpretation Approach for Automatic Generation of Polynomial Invariants	280
<i>Enric Rodríguez-Carbonell and Deepak Kapur</i>	
Approximating the Algebraic Relational Semantics of Imperative Programs	296
<i>Michael A. Colón</i>	
The Octahedron Abstract Domain	312
<i>Robert Clarisó and Jordi Cortadella</i>	

Path-Sensitive Analysis for Linear Arithmetic and Uninterpreted Functions	328
<i>Sumit Gulwani and George C. Necula</i>	

Shape Analysis and Logic

On Logics of Aliasing	344
<i>Marius Bozga, Radu Iosif, and Yassine Lakhnech</i>	
Generalized Records and Spatial Conjunction in Role Logic	361
<i>Viktor Kuncak and Martin Rinard</i>	

Termination Analysis

Non-termination Inference for Constraint Logic Programs	377
<i>Etienne Payet and Fred Mesnard</i>	

Author Index	393
---------------------------	-----