

Lecture Notes in Computer Science

2477

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Manuel V. Hermenegildo Germán Puebla (Eds.)

Static Analysis

9th International Symposium, SAS 2002
Madrid, Spain, September 17-20, 2002
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Manuel V. Hermenegildo
Germán Puebla
Technical University of Madrid, Department of Computer Science
Facultad de Informática, Campus de Montegancedo
28660 Boadilla del Monte, Madrid, Spain
E-mail: {herme, german}@fi.upm.es

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Static analysis : 9th international symposium ; proceedings / SAS 2002, Madrid, Spain, September 17 - 20, 2002. Manuel V. Hermenegildo ; German Puebla (ed.). - Berlin ; Heidelberg ; New York ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2477)
ISBN 3-540-44235-9

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

ISSN 0302-9743

ISBN 3-540-44235-9 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 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Stefan Sossna e.K.
Printed on acid-free paper SPIN: 10871380 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 implementation of programming languages. The series of Static Analysis Symposia is a forum for the presentation and discussion of advances in the area.

This volume contains the papers accepted for presentation at the Ninth International Static Analysis Symposium (SAS 2002), which was held September 17-20, 2002 in Madrid, Spain. Previous SAS symposia were held in Paris, France (LNCS 2126), Santa Barbara, CA, USA (LNCS 1824), Venice, Italy (LNCS 1694), Pisa, Italy (LNCS 1503), Paris, France (LNCS 1302), Aachen, Germany (LNCS 1145), Glasgow, UK (LNCS 983), Namur, Belgium (LNCS 864), following the international workshop WSA in Padova, Italy (LNCS 724), Bordeaux, France (Bigre Vol. 81-82) and JTASPEFL/WSA, Bordeaux, France (Bigre Vol. 74).

In response to the call for papers, 86 contributions were submitted from 12 different countries. Following on-line discussions, the Program Committee met in Madrid on June 22, 2002, and selected 32 papers, basing this choice on their scientific quality and relevance to the symposium. Each paper was reviewed by at least three Program Committee members or external referees. In addition to the contributed papers, this volume includes abstracts of invited talks by Thomas Reps (University of Wisconsin, USA), Robert Hall (AT&T Labs Research, USA), and Javier Esparza (University of Edinburgh, United Kingdom).

On behalf of the Program Committee, the Program Chairs would like to thank all the authors who submitted papers and all the external referees for their careful work in the reviewing process. The support of the several funding agencies, listed later in the volume, which provided part of the funds for the organization of the conference is also gratefully acknowledged.

On this occasion, SAS was held concurrently with the 2002 International Workshop on Logic-Based Program Development and Transformation and the 2002 APPIA-GULP-PRODE Joint Conference on Declarative Programming as well as several workshops. We would like to express our gratitude to the members of the Local Organizing Committees of all the conferences co-located with SAS 2002 and the members of the organizing departments and institutions involved for the invaluable help and enthusiasm provided throughout the preparation and organization of the joint event.

July 2002

Manuel Hermenegildo
Germán Puebla

Organization

Program Committee

Manuel Hermenegildo (Chair)	Technical University of Madrid, Spain
Germán Puebla (Co-chair)	Technical University of Madrid, Spain
Radhia Cousot	École Polytechnique, France
Saumya Debray	The University of Arizona, USA
Manuel Fahndrich	Microsoft Research, USA
Roberto Giacobazzi	University of Verona, Italy
Chris Hankin	Imperial College, UK
Giorgio Levi	University of Pisa, Italy
Kim Marriott	Monash University, Australia
Alan Mycroft	Cambridge University, United Kingdom
Ganesan Ramalingam	IBM T.J. Watson Research Center, USA
Martin Rinard	Massachusetts Institute of Technology, USA
Shmuel Sagiv	Tel-Aviv University, Israel
Reinhard Wilhelm	Universität des Saarlandes, Germany

Organizing Committee

SAS 2002 was organized by the following members of the School of Computer Science of the Technical University of Madrid:

Germán Puebla (Local Chair)	Jose Manuel Gómez
Manuel Hermenegildo (Local Co-chair)	Pedro López
Astrid Beascoa	José Morales
Francisco Bueno	Oscar Portela
Jesús Correas	Claudio Vaucheret

Referees

Scott Armenian	Jesús Correas
Roberto Bagnara	Patrick Cousot
Roberto Barbuti	Pierpaolo Degano
Jörg Bauer	Stephan Diehl
Bruno Blanchet	Alessandra Di Pierro
Bard Bloom	Nurit Dor
Chiara Bodei	Robert Ennals
Daniel Cabeza	Jérôme Feret
Manuel Carro	Gian L. Ferrari
Michael Codish	Gilberto Filé

Alessandro Fin
Steve Fink
Riccardo Focardi
Jeffrey S. Foster
Simon Frankau
Maurizio Gabbrielli
John Gallagher
María García de la Banda
Samir Genaim
Deepak Goyal
Roberta Gori
Dave Grove
Orna Grumberg
René R. Hansen
Nevin Heintze
Pat M. Hill
Mike Hind
Yoram Hirshfeld
Charles Hymans
Gerda Janssens
Bertrand Jeannot
Neil Johnson
Andy King
Uday Khedker
Peeter Laud
Michael Leuschel
Francesca Levi
Annie Liu
Francesco Logozzo
Pedro López-García
Andrea Maggiolo-Schettini
Roman Manevich
Julio Mariño
Damien Massé
Isabella Mastroeni
Laurent Mauborgne
Nancy Mazur
Fred Mesnard
Massimo Merro
Antoine Miné

David Monniaux
Susana Muñoz-Hernández
Nicholas Nethercote
Joachim Niehren
Hans de Nivelle
Robert O'Callahan
Andreas Podelski
Christian Probst
Francesco Ranzato
Xavier Rival
David Sands
Peter Schachte
David Scott
Francesca Scozzari
Helmut Seidl
Peter Sewell
Ran Shaham
Richard Sharp
Roberto Segala
Jeremy Singer
Harald Søndergaard
Fausto Spoto
Vugranam. C. Sreedhar
Martin Sulzmann
Peter Stuckey
Henrik Theiling
Stephan Thesing
Eben Upton
Pawel Urzyczyn
Wim Vanhoof
Claudio Vaucheret
Sven Verdoolaege
Herbert Wiklicky
Sebastian Winkel
Jessie Xu
Eran Yahav
Enea Zaffanella
Lenore Zuck

Sponsoring Institutions

The SAS 2002 conference was supported by the following organizations:

- Spanish Ministry of Science and Technology.
- Technical University of Madrid (UPM).
- Department of Computer Science, UPM.
- Department of Industrial Engineering, UPM.
- European Commission – Information Society Technologies Programme.
- CoLogNet, the European Network of Excellence in Computational Logic.

The SAS 2002 conference was organized in cooperation with the European Association for Programming Languages and Systems (EAPLS).

Table of Contents

Static Program Analysis via 3-Valued Logic	1
<i>Thomas Reps</i>	
Open Modeling in Multi-stakeholder Distributed Systems: Research and Tool Challenges	2
<i>Robert J. Hall</i>	
An Algebraic Approach to the Static Analysis of Concurrent Software	3
<i>Javier Esparza</i>	
Polynomial Constants Are Decidable	4
<i>Markus Müller-Olm, Helmut Seidl</i>	
Normalizable Horn Clauses, Strongly Recognizable Relations, and Spi	20
<i>Flemming Nielson, Hanne Riis Nielson, Helmut Seidl</i>	
Nonuniform Alias Analysis of Recursive Data Structures and Arrays	36
<i>Arnaud Venet</i>	
Representing and Approximating Transfer Functions in Abstract Interpretation of Heterogeneous Datatypes	52
<i>B. Jeannot</i>	
Automated Verification of Concurrent Linked Lists with Counters	69
<i>Tuba Yavuz-Kahveci, Tevfik Bultan</i>	
Backward Type Inference Generalises Type Checking	85
<i>Lunjin Lu, Andy King</i>	
More Precise Yet Efficient Type Inference for Logic Programs	102
<i>Claudio Vaucheret, Francisco Bueno</i>	
A Few Graph-Based Relational Numerical Abstract Domains	117
<i>Antoine Miné</i>	
Static Analysis of the Numerical Stability of Loops	133
<i>Mathieu Martel</i>	
On Termination of Logic Programs with Floating Point Computations	151
<i>Alexander Serebrenik, Danny De Schreye</i>	

Modular Control Flow Analysis for Libraries	165
<i>Christian W. Probst</i>	
An Efficient Inclusion-Based Points-To Analysis for Strictly-Typed Languages	180
<i>John Whaley, Monica S. Lam</i>	
Compactly Representing First-Order Structures for Static Analysis	196
<i>R. Manevich, G. Ramalingam, J. Field, D. Goyal, M. Sagiv</i>	
Possibly Not Closed Convex Polyhedra and the Parma Polyhedra Library	213
<i>Roberto Bagnara, Elisa Ricci, Enea Zaffanella, Patricia M. Hill</i>	
Speeding Up Dataflow Analysis Using Flow-Insensitive Pointer Analysis	230
<i>Stephen Adams, Thomas Ball, Manuvir Das, Sorin Lerner, Sriram K. Rajamani, Mark Seigle, Westley Weimer</i>	
Improving the Precision of Equality-Based Dataflow Analyses	247
<i>Erik Ruf</i>	
Guaranteed Optimization: Proving Nullspace Properties of Compilers.....	263
<i>Todd L. Veldhuizen, Andrew Lumsdaine</i>	
Representation Analysis for Coercion Placement	278
<i>Karl-Filip Faxén</i>	
Pipeline Modeling for Timing Analysis.....	294
<i>Marc Langenbach, Stephan Thesing, Reinhold Heckmann</i>	
Analysing Approximate Confinement under Uniform Attacks	310
<i>Alessandra Di Pierro, Chris Hankin, Herbert Wiklicky</i>	
An Improved Constraint-Based System for the Verification of Security Protocols.....	326
<i>Ricardo Corin, Sandro Etalle</i>	
From Secrecy to Authenticity in Security Protocols	342
<i>Bruno Blanchet</i>	
Security Typings by Abstract Interpretation	360
<i>Mirko Zanotti</i>	
Static Confidentiality Enforcement for Distributed Programs	376
<i>Andrei Sabelfeld, Heiko Mantel</i>	
Refinement of LTL Formulas for Abstract Model Checking	395
<i>María del Mar Gallardo, Pedro Merino, Ernesto Pimentel</i>	

Making Abstract Model Checking Strongly Preserving	411
<i>Francesco Ranzato, Francesco Tapparo</i>	
Semantics for Abstract Interpretation-Based Static Analyzes of Temporal Properties	428
<i>Damien Massé</i>	
Checking Safety Properties of Behavioral VHDL Descriptions by Abstract Interpretation	444
<i>Charles Hymans</i>	
States vs. Traces in Model Checking by Abstract Interpretation	461
<i>Roberto Giacobazzi, Francesco Ranzato</i>	
Reuse of Results in Termination Analysis of Typed Logic Programs	477
<i>Maurice Bruynooghe, Michael Codish, Samir Genaim, Wim Vanhoof</i>	
Finiteness Analysis in Polynomial Time	493
<i>Chin Soon Lee</i>	
Detecting Optimal Termination Conditions of Logic Programs	509
<i>Fred Mesnard, Etienne Payet, Ulrich Neumerkel</i>	
Author Index	527