

# Lecture Notes in Computer Science

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

1694

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

Agostino Cortesi Gilberto Filé (Eds.)

# Static Analysis

6th International Symposium, SAS'99  
Venice, Italy, September 22-24, 1999  
Proceedings



Springer

## Series Editors

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

## Volume Editors

Agostino Cortesi  
Dipartimento di Informatica, Università Ca'Foscari di Venezia  
via Torino 155, I-30170 Mestre-Venezia, Italy  
E-mail: cortesi@dsi.unive.it

Gilberto Filé  
Dipartimento di Matematica Pura ed Applicata, Università di Padova  
via Belzoni 7, I-35131 Padova, Italy  
E-mail: gilberto@math.unipd.it

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Static analysis** : 6th international symposium ; proceedings / SAS '99, Venice, Italy, September 22 - 24, 1999. Agostino Cortesi ; Gilberto Filé (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1999

(Lecture notes in computer science ; Vol. 1694)  
ISBN 3-540-66459-9

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

ISSN 0302-9743

ISBN 0-543-66459-9 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 1999  
Printed in Germany

Typesetting: Camera-ready by author

SPIN 10704494 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

# Preface

Static analysis is increasingly recognized as a fundamental research area aimed at studying and developing tools for high performance implementations and verification systems for all programming language paradigms. The last two decades have witnessed substantial developments in this field, ranging from theoretical frameworks to design, implementation, and application of analyzers in optimizing compilers.

Since 1994, SAS has been the annual conference and forum for researchers in all aspects of static analysis. This volume contains the proceedings of the 6th International Symposium on Static Analysis (SAS'99) which was held in Venice, Italy, on 22–24 September 1999. The previous SAS conferences were held in Namur (Belgium), Glasgow (UK), Aachen (Germany), Paris (France), and Pisa (Italy).

The program committee selected 18 papers out of 42 submissions on the basis of at least three reviews. The resulting volume offers to the reader a complete landscape of the research in this area. The papers contribute to the following topics: foundations of static analysis, abstract domain design, and applications of static analysis to different programming paradigms (concurrent, synchronous, imperative, object oriented, logical, and functional). In particular, several papers use static analysis for obtaining state space reduction in concurrent systems. New application fields are also addressed, such as the problems of security and secrecy.

In addition to these high quality technical papers, SAS'99 included in its program several outstanding invited speakers. Daniel Weise, Dennis Volpano, David MacAllester, Don Sannella, David Schmidt, Mary Lou Soffa, and Craig Chambers accepted our invitation to give invited talks or tutorials. Their contributions are also included in this volume.

In general, it is clear to us that the role of static analysis is bound to become more and more important in the future due to the enormous popularity of the Internet. For the latter requires the construction of increasingly complex software systems for which efficiency but also security are crucial issues.

The staff of the department of computer science at Ca' Foscari University and that of the department of mathematics at Padova University were extremely helpful in handling all aspects of the symposium.

Special thanks are also due to the institutions that sponsored the event: EAPLS, ALP, CNR, Compulog, Ca' Foscari University, and Padova University.

## Program Committee

Craig Chambers	(University of Washington, USA)
Agostino Cortesi	(Università Ca' Foscari, Venice, Italy )
Patrick Cousot	(LIENS, Paris, France)
Gilberto Filé	(Università di Padova, Italy)
Roberto Giacobazzi	(Università di Verona, Italy)
Gopal Gupta	(New Mexico University, USA)
Alan Mycroft	(Cambridge University, UK)
Flemming Nielson	(University of Aarhus, DK)
Jens Palsberg	(Purdue University, USA)
Andreas Podelski	(Max Plank Institute, Germany)
Mooly Sagiv	(Tel Aviv University, Israel)
David Schmidt	(Kansas State University, USA)
Mary Lou Soffa	(University of Pittsburgh, USA)
Harald Søndergaard	(University of Melbourne, Australia)
Pascal Van Hentenryck	(Université Catholique de Louvain, Belgium)

## List of Referees

Roberto Bagnara	Nurit Dor	Lawrence C Paulson
Roberto Barbuti	Agostino Dovier	Alberto Pettorossi
Bruno Blanchet	Sandro Etalle	Enrico Pontelli
Rastislav Bodik	Moreno Falaschi	Francesco Ranzato
Michele Bugliesi	Riccardo Focardi	David Sands
Nadia Busi	Maurizio Gabbrielli	Peter Schachte
Giuseppe Castagna	Patrice Godefroid	Francesca Scozzari
Satish Chandra	Michael Hanus	Helmut Seidl
Witold Charatonik	Reinhold Heckmann	Olin Shivers
Nicoletta Cocco	Tom Henzinger	Zoltan Somogyi
Michael Codish	Clara Jaramillo	Peter Stuckey
Livio Colussi	Giorgio Levi	Peter Thiemann
Priami Corrado	Lunjin Lu	Arnaud Venet
Vitor Santos Costa	Laurent Mauborgne	Eran Yahav
Ferruccio Damiani	David Melski	Xin Yuan
Arie van Deursen	Atif M. Memon	
Alain Deutsch	Hanne Riis Nielson	

# Table of Contents

## Synchronization in JAVA Programs

A Formal Study of Slicing for Multi-threaded Programs with JVM Concurrency Primitives .....	1
<i>John Hatchliff, James Corbett, Matthew Dwyer, Stefan Sokolowski, Hongjun Zheng</i>	
Static Analyses for Eliminating Unnecessary Synchronization from Java Programs .....	19
<i>Jonathan Aldrich, Craig Chambers, Emin Gun Sirer, and Susan Eggers</i>	

## Synchronous Languages

Dynamic Partitioning in Analyses of Numerical Properties .....	39
<i>Bertrand Jeannot, Nicolas Halbwachs, Pascal Raymond</i>	
Polyhedral Analysis for Synchronous Languages.....	51
<i>Frédéric Besson, Thomas Jensen, Jean-Pierre Talpin</i>	

## Abstract Domains

Decomposing Non-Redundant Sharing by Complementation .....	69
<i>Enea Zaffanella, Patricia M. Hill, Roberto Bagnara</i>	
Freeness Analysis Through Linear Refinement .....	85
<i>Patricia Hill, Fausto Spoto</i>	
Binary Decision Graphs.....	101
<i>Laurent Mauborgne</i>	
Binding-Time Analysis for Both Static and Dynamic Expressions .....	117
<i>Kenichi Asai</i>	

## Concurrency

Abstract Interpretation of Mobile Ambients .....	134
<i>René Rydhof Hansen, Jacob Grydholt Jensen, Flemming Nielson, Hanne Riis Nielson</i>	
Abstracting Cryptographic Protocols with Tree Automata .....	149
<i>David Monniaux</i>	
State Space Reduction based on Live Variables Analysis .....	164
<i>Marius Bozga, Jean-Claude Fernandez, Lucian Ghirvu</i>	

## Static Single Assignment

Partial Dead Code Elimination Using Extended Value Graph . . . . .	179
<i>Munehiro Takimoto, Kenichi Harada</i>	
Translating out of Single Assignment Form . . . . .	194
<i>Vugranam C. Sreedhar, Roy Dz-Ching Ju, David M. Gillies, Vatsa Santhanam</i>	

## Optimizations

Eliminating Dead Code on Recursive Data . . . . .	211
<i>Yanhong A. Liu, Scott D. Stoller</i>	
Detecting Equalities of Variables: Combining Efficiency with Precision . . . .	232
<i>Oliver Rüthing, Jens Knoop, Bernhard Steffen</i>	

## Foundations

A New Class of Functions for Abstract Interpretation . . . . .	248
<i>Jörg Köller, Markus Mohnen</i>	
Equational Semantics . . . . .	264
<i>Loïc Correnson, Etienne Duris, Didier Parigot, Gilles Roussel</i>	
Abstract Animator for Temporal Specifications: Application to TLA . . . . .	284
<i>Dominique Cansell, Dominique Méry</i>	

## Invited Talks and Tutorials

Static Analysis of Mega-Programs . . . . .	300
<i>Daniel Weise</i>	
Safety versus Secrecy . . . . .	303
<i>Dennis Volpano</i>	
On the Complexity Analysis of Static Analyses . . . . .	312
<i>David McAllester</i>	
Model-Checking: A Tutorial Introduction . . . . .	330
<i>Markus Müller-Olm, David Schmidt, Bernhard Steffen</i>	
Tutorial: Techniques to Improve the Scalability and Precision of Data Flow Analysis . . . . .	355
<i>Mary Lou Soffa</i>	

<b>Author Index</b> . . . . .	357
-------------------------------	-----