

*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*

Chris Hankin Igor Siveroni (Eds.)

# Static Analysis

12th International Symposium, SAS 2005  
London, UK, September 7-9, 2005  
Proceedings

Volume Editors

Chris Hankin  
Igor Siveroni  
Imperial College London, Department of Computing  
180 Queen's Gate, London SW7 2BZ, UK  
E-mail: {clh,siveroni}@doc.ic.ac.uk

Library of Congress Control Number: 2005931559

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

ISSN 0302-9743  
ISBN-10 3-540-28584-9 Springer Berlin Heidelberg New York  
ISBN-13 978-3-540-28584-7 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](http://springeronline.com)

© Springer-Verlag Berlin Heidelberg 2005  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 11547662 06/3142 5 4 3 2 1 0

# Preface

Static analysis allows us to determine aspects of the dynamic behavior of programs and systems without actually executing them. Traditionally used in optimizing compilers, static analysis is now also used extensively in verification, software certification and semantics-based manipulation. The research community in static analysis covers a broad spectrum from foundational issues – new semantic models of programming languages and systems – through to practical tools. 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 12th International Static Analysis Symposium (SAS 2005) which was held 7–9 September 2005 at Imperial College London. A total of 66 papers were submitted; the Program Committee held an online discussion which led to the selection of 22 papers for presentation. The selection was based on scientific quality, originality and relevance to the scope of SAS. Every paper was reviewed by at least 3 PC members or external referees. This volume also includes abstracts of talks given by the two invited speakers: Samson Abramsky FRS (University of Oxford) and Andrew Gordon (Microsoft Research, Cambridge).

On behalf of the Program Committee, the Program Chair would like to thank all of the authors who submitted papers and all of the external referees for their careful work in the reviewing process. The Program Chair would also particularly like to thank Igor Siveroni who provided local support for the conference management system and who helped in organizing the structure of this volume. We would also like to express our gratitude to Herbert Wiklicky and Bridget Gundry who masterminded the local arrangements.

SAS 2005 was held concurrently with *LOPSTR 2005*, the *International Symposium on Logic-Based Program Synthesis and Transformation*. We would like to thank Pat Hill (LOPSTR PC Chair) for her help and advice on the organizational aspects.

London, June 2005

Chris Hankin

# Organization

## Program Committee

|                      |   |
|----------------------|---|
| Thomas Ball          | Microsoft, USA                              |
| Radhia Cousot        | CNRS/Ecole Polytechnique, France            |
| Alessandra Di Pierro | Università di Pisa, Italy                   |
| Gilberto Filé        | Università di Padova, Italy                 |
| Roberto Giacobazzi   | Università di Verona, Italy                 |
| Chris Hankin (Chair) | Imperial College London, UK                 |
| Thomas Jensen        | IRISA/CNRS Rennes, France                   |
| Andy King            | University of Kent, UK                      |
| Pasquale Malacaria   | Queen Mary College, UK                      |
| Laurent Mauborgne    | École Normale Supérieure, France            |
| Alan Mycroft         | University of Cambridge, UK                 |
| Andreas Podelski     | Max-Planck-Institut für Informatik, Germany |
| German Puebla        | Technical University of Madrid, Spain       |
| Ganesan Ramalingam   | IBM, USA                                    |
| Andrei Sabelfeld     | Chalmers University of Technology, Sweden   |
| Mooly Sagiv          | Tel Aviv University, Israel                 |
| Harald Søndergaard   | University of Melbourne, Australia          |
| Bernhard Steffen     | University of Dortmund, Germany             |

## Steering Committee

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

## Organizing Committee

Bridget Gundry  
Igor Siveroni  
Herbert Wiklicky

## Referees

|             |              |             |
|-------------|--------------|-------------|
| A. Askarov  | T. Harris    | X. Rival    |
| G. Barthe   | D. Hirsch    | F. Rossi    |
| J. Bean     | N. Kettle    | R. Rugina   |
| J. Berdine  | R. Komondoor | O. Rüdthing |
| S. Berezin  | A. Lawrence  | P. Schmitt  |
| J. Bertrane | O. Lee       | R. Segala   |

## VIII Organization

F. Besson  
B. Blanchet  
F. Bueno  
M. Carro  
P. Caspi  
O. Chitil  
S. Chong  
D. Clark  
D. Colazzo  
L. Colussi  
J. Correas  
S. Crafa  
N. Dur  
S. Edelkamp  
C. Faggian  
J. Feret  
J. Field  
A. Frisch  
M. Gil  
A. Gotlieb  
T. Griffin  
S. Gulwani  
N. Halbwachs  
R. Hansen

F. Levi  
X. Li  
F. Logozzo  
A. Lokhmotov  
R. Manevich  
P. Manghi  
J. Mariño  
D. Massé  
I. Mastreoni  
H. Melgratti  
A. Merlo  
A. Miné  
D. Monniaux  
M. Müller-Olm  
B. Nicolescu  
K. Ostrovsky  
L. Pareto  
M. Preda  
P. Pietrzak  
H. Raffelt  
F. Ranzato  
A. Rensink  
T. Rezk  
N. Rinetzky

C. Segura  
A. Simon  
J. Singer  
J.-G. Smaus  
F. Spoto  
M. Strout  
F. Tapparo  
R. Thrippleton  
S. Thompson  
E. Tuosto  
S. Valentini  
A. Venet  
L. Vigano  
P. Wadler  
H. Wiklicky  
D. Xu  
E. Yahav  
G. Yorsh  
S. Yong  
E. Zaffanella  
D. Zanardini  
R. Zunino

# Table of Contents

## Invited Talks

|  |   |
|--|---|
| Algorithmic Game Semantics and Static Analysis<br><i>Samson Abramsky</i> .....       | 1 |
| From Typed Process Calculi to Source-Based Security<br><i>Andrew D. Gordon</i> ..... | 2 |

## Contributed Papers

|   |     |
|---|-----|
| Widening Operators for Weakly-Relational Numeric Abstractions<br><i>Roberto Bagnara, Patricia M. Hill, Elena Mazzi, Enea Zaffanella</i> ....                  | 3   |
| Generation of Basic Semi-algebraic Invariants Using Convex Polyhedra<br><i>Roberto Bagnara, Enric Rodríguez-Carbonell, Enea Zaffanella</i> .....              | 19  |
| Inference of Well-Typings for Logic Programs with Application to Termination Analysis<br><i>Maurice Bruynooghe, John Gallagher, Wouter Van Humbeeck</i> ..... | 35  |
| Memory Space Conscious Loop Iteration Duplication for Reliable Execution<br><i>Guilin Chen, Mahmut Kandemir, Mustafa Karakoy</i> .....                        | 52  |
| Memory Usage Verification for OO Programs<br><i>Wei-Ngan Chin, Huu Hai Nguyen, Shengchao Qin, Martin Rinard</i> ...   | 70  |
| Abstraction Refinement for Termination<br><i>Byron Cook, Andreas Podelski, Andrey Rybalchenko</i> .....   | 87  |
| Data-Abstraction Refinement: A Game Semantic Approach<br><i>Aleksandar Dimovski, Dan R. Ghica, Ranko Lazić</i> .....  | 102 |
| Locality-Based Abstractions<br><i>Javier Esparza, Pierre Ganty, Stefan Schwoon</i> .....  | 118 |
| Type-Safe Optimisation of Plugin Architectures<br><i>Neal Glew, Jens Palsberg, Christian Grothoff</i> .....   | 135 |

|  |     |
|--|-----|
| Using Dependent Types to Certify the Safety of Assembly Code<br><i>Matthew Harren, George C. Necula</i> .....  | 155 |
| The PER Model of Abstract Non-interference<br><i>Sebastian Hunt, Isabella Mastroeni</i> .....  | 171 |
| A Relational Abstraction for Functions<br><i>Bertrand Jeannot, Denis Gopan, Thomas Reps</i> .....  | 186 |
| Taming False Alarms from a Domain-Unaware C Analyzer by a<br>Bayesian Statistical Post Analysis<br><i>Yunghum Jung, Jaehwang Kim, Jaeho Shin, Kwangkeun Yi</i> ..... | 203 |
| Banshee: A Scalable Constraint-Based Analysis Toolkit<br><i>John Kodumal, Alex Aiken</i> .....   | 218 |
| A Generic Framework for Interprocedural Analysis of Numerical<br>Properties<br><i>Markus Müller-Olm, Helmut Seidl</i> .....  | 235 |
| Finding Basic Block and Variable Correspondence<br><i>Iman Narasamdya, Andrei Voronkov</i> .....   | 251 |
| Boolean Heaps<br><i>Andreas Podelski, Thomas Wies</i> .....  | 268 |
| Interprocedural Shape Analysis for Cutpoint-Free Programs<br><i>Noam Rinetzky, Mooly Sagiv, Eran Yahav</i> .....   | 284 |
| Understanding the Origin of Alarms in ASTRÉE<br><i>Xavier Rival</i> .....  | 303 |
| Pair-Sharing Analysis of Object-Oriented Programs<br><i>Stefano Secci, Fausto Spoto</i> .....  | 320 |
| Exploiting Sparsity in Polyhedral Analysis<br><i>Axel Simon, Andy King</i> .....   | 336 |
| Secure Information Flow as a Safety Problem<br><i>Tachio Terauchi, Alex Aiken</i> .....  | 352 |
| <b>Author Index</b> .....  | 369 |