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
- Mooy 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. Komondoore  
  O. Rüthing
- S. Berezin  
  A. Lawrence  
  P. Schmitt
- J. Bertrane  
  O. Lee  
  R. Segala
## Table of Contents

### Invited Talks

Algorithmic Game Semantics and Static Analysis  
*Samson Abramsky* ............................................. 1  

From Typed Process Calculi to Source-Based Security  
*Andrew D. Gordon* ............................................. 2  

### Contributed Papers

Widening Operators for Weakly-Relational Numeric Abstractions  
*Roberto Bagnara, Patricia M. Hill, Elena Mazzi, Enea Zaffanella* .... 3  

Generation of Basic Semi-algebraic Invariants Using Convex Polyhedra  
*Roberto Bagnara, Enric Rodríguez-Carbonell, Enea Zaffanella* ......... 19  

Inference of Well-Typings for Logic Programs with Application to Termination Analysis  
*Maurice Bruynooghe, John Gallagher, Wouter Van Humbeeck* ....... 35  

Memory Space Conscious Loop Iteration Duplication for Reliable Execution  
*Guilin Chen, Mahmut Kandemir, Mustafa Karakoy* .................... 52  

Memory Usage Verification for OO Programs  
*Wei-Ngan Chin, Huu Hai Nguyen, Shengchao Qin, Martin Rinard* .... 70  

Abstraction Refinement for Termination  
*Byron Cook, Andreas Podelski, Andrey Rybalchenko* .................. 87  

Data-Abstraction Refinement: A Game Semantic Approach  
*Aleksandar Dimovski, Dan R. Ghica, Ranko Lazić* .................... 102  

Locality-Based Abstractions  
*Javier Esparza, Pierre Ganty, Stefan Schwoon* ....................... 118  

Type-Safe Optimisation of Plugin Architectures  
*Neal Glew, Jens Palsberg, Christian Grothoff* ....................... 135
Using Dependent Types to Certify the Safety of Assembly Code
Matthew Harren, George C. Necula .............................. 155

The PER Model of Abstract Non-interference
Sebastian Hunt, Isabella Mastroeni ............................... 171

A Relational Abstraction for Functions
Bertrand Jeannet, Denis Gopan, Thomas Reps .................. 186

Taming False Alarms from a Domain-Unaware C Analyzer by a
Bayesian Statistical Post Analysis
Yungbum Jung, Jaehwang Kim, Jaeho Shin, Kwangkeun Yi .... 203

Banshee: A Scalable Constraint-Based Analysis Toolkit
John Kodumal, Alex Aiken ........................................ 218

A Generic Framework for Interprocedural Analysis of Numerical
Properties
Markus Müller-Olm, Helmut Seidl ............................... 235

Finding Basic Block and Variable Correspondence
Iman Narasamdya, Andrei Voronkov .............................. 251

Boolean Heaps
Andreas Podelski, Thomas Wies .................................. 268

Interprocedural Shape Analysis for Cutpoint-Free Programs
Noam Rinetzky, Mooly Sagiv, Eran Yahav ...................... 284

Understanding the Origin of Alarms in ASTRÉE
Xavier Rival ..................................................... 303

Pair-Sharing Analysis of Object-Oriented Programs
Stefano Secci, Fausto Spoto .................................... 320

Exploiting Sparsity in Polyhedral Analysis
Axel Simon, Andy King ........................................ 336

Secure Information Flow as a Safety Problem
Tachio Terauchi, Alex Aiken .................................... 352

Author Index .................................................... 369