

*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

*University of California, Los Angeles, CA, 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*

Hanne Riis Nielson   Gilberto Filé (Eds.)

# Static Analysis

14th International Symposium, SAS 2007  
Kongens Lyngby, Denmark, August 22-24, 2007  
Proceedings

## Volume Editors

Hanne Riis Nielson

Technical University of Denmark, Informatics and Mathematical Modelling

Richard Petersens Plads, 2800 Kongens Lyngby, Denmark

E-mail: riis@imm.dtu.dk

Gilberto Filé

University of Padova, Department of Pure and Applied Mathematics

via Trieste 63, 35121 Padova, Italy

E-mail: gilberto@math.unipd.it

Library of Congress Control Number: 2007932181

CR Subject Classification (1998): D.3.2-3, F.3.1-2, I.2.2, F.4.2, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743

ISBN-10 3-540-74060-0 Springer Berlin Heidelberg New York

ISBN-13 978-3-540-74060-5 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

springer.com

© Springer-Verlag Berlin Heidelberg 2007

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper SPIN: 12103201 06/3180 5 4 3 2 1 0

# Preface

The aim of static analysis is to develop principles, techniques and tools for validating properties of programs, for designing semantics-based transformations of programs and for obtaining high-performance implementations of high-level programming languages. Over the years the series of static analysis symposia has served as the primary venue for presentation and discussion of theoretical, practical and innovative advances in the area.

This volume contains the papers accepted for presentation at the 14th International Static Analysis Symposium (SAS 2007). The meeting was held August, 22–24, 2007, at the Technical University of Denmark (DTU) in Kongens Lyngby, Denmark. In response to the call for papers, 85 submissions were received. Each submission was reviewed by at least 3 experts and, based on these reports, 26 papers were selected after a week of intense electronic discussion using the EasyChair conference system. In addition to these 26 papers, this volume also contains contributions by the two invited speakers: Frank Tip (IBM T. J. Watson Research Center, USA) and Alan Mycroft (Cambridge University, UK).

On the behalf of the Program Committee, the Program Chairs would like to thank all the authors who submitted their work to the conference and also all the external referees who have been indispensable for the selection process. Special thanks go to Terkel Tolstrup and Jörg Bauer, who helped in handling the submitted papers and in organizing the structure of this volume. We would also like to thank the members of the Organizing Committee at DTU for their great work. Finally we want to thank the PhD school ITMAN at DTU for financial support.

SAS 2007 was held concurrently with LOPSTR 2007, the International Symposium on Logic-Based Program Synthesis and Transformation.

June 2007

Hanne Riis Nielson  
Gilberto Filé

# Organization

## Program Chairs

|                    |                                          |
|--------------------|------------------------------------------|
| Gilberto Filé      | University of Padova, Italy              |
| Hanne Riis Nielson | Technical University of Denmark, Denmark |

## Program Committee

|                     |                                         |
|---------------------|-----------------------------------------|
| Agostino Cortesi    | University Ca' Foscari of Venice, Italy |
| Patrick Cousot      | École Normale Supérieure, France        |
| Manuel Fähndrich    | Microsoft Research, USA                 |
| Roberto Giacobazzi  | University of Verona, Italy             |
| Chris Hankin        | Imperial College, UK                    |
| Manuel Hermenegildo | Technical University of Madrid, Spain   |
| Jens Knoop          | Technical University of Vienna, Austria |
| Naoki Kobayashi     | Tohoku University, Japan                |
| Julia Lawall        | Copenhagen University, Denmark          |
| Andreas Podelski    | University of Freiburg, Germany         |
| Jakob Rehof         | University of Dortmund, Germany         |
| Radu Rugina         | Cornell University, USA                 |
| Mooly Sagiv         | Tel-Aviv University, Israel             |
| David Schmidt       | Kansas State University, USA            |
| Helmut Seidl        | Technical University of Munich, Germany |
| Harald Søndergaard  | University of Melbourne, Australia      |
| Kwangkeun Yi        | Seoul National University, Korea        |

## Steering Committee

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

## Organizing Committee

Christian W. Probst  
Sebastian Nanz  
Flemming Nielson  
Henrik Pilegaard  
Terkel K. Tolstrup  
Eva Bing  
Elsebeth Strøm

## Referees

|                    |                      |                     |
|--------------------|----------------------|---------------------|
| Luca de Alfaro     | Patricia Hill        | Franz Puntigam      |
| Rajeev Alur        | Yungbum Jung         | Shaz Qadeer         |
| Jesper Andersen    | Deepak Kapur         | Noam Rinetzky       |
| James Avery        | Deokhwan Kim         | Xavier Rival        |
| Domagoj Babic      | Andreas Krall        | Enric               |
| Roberto Bagnara    | Shuvendu Lahiri      | Rodriguez-Carbonell |
| Josh Berdine       | Akash Lal            | Francesca Rossi     |
| Julien Bertrane    | Michel Leconte       | Andrey Rybalchenko  |
| Sapan Bhatia       | Oukseh Lee           | Oliver Rüthing      |
| Bruno Blanchet     | Heejong Lee          | Cesar Sanchez       |
| Chiara Braghin     | Tal Lev-Ami          | Peter Schachte      |
| Bruno De Bus       | Francesco Logozzo    | Markus Schordan     |
| Cristiano Calgano  | Flaminia Luccio      | Stefan Schwoon      |
| Manuel Carro       | Matteo Maffei        | Roberto Segala      |
| Amadeo Casas       | Rupak Majumdar       | Sunae Seo           |
| Bor-Yuh Evan Chang | Roman Manevich       | Elodie-Jane Sims    |
| Byron Cook         | Mark Marron          | Zoltan Somogyi      |
| Silvia Crafa       | Matthieu Martel      | Fausto Spoto        |
| Hyunjun Eo         | Florian Martin       | Manu Sridharan      |
| M. Anton Ertl      | Isabella Mastroeni   | Bjarne Steensgaard  |
| Manuel Fahndrich   | Laurent Mauborgne    | Darko Stefanovic    |
| Xinyu Feng         | Richard Mayr         | Peter Stuckey       |
| Jerome Feret       | Mario Mendez-Lojo    | Kohei Suenaga       |
| Pietro Ferrara     | Alessio Merlo        | Yoshinori Tanabe    |
| Andrea Flexeder    | Yasuhiko Minamide    | Francesco Tapparo   |
| Lars-Ake Fredlund  | Antoine Mine         | Makoto Tatsuta      |
| Samir Gemaim       | David Monniaux       | Tachio Terauchi     |
| Thomas Gawlitza    | Sebastian Nanz       | Terkel Tolstrup     |
| Andy Gordon        | Jorge Navas          | Tullio Vardanega    |
| Alexey Gotsman     | Nicholas Nethercote  | Kumar Neeraj Verma  |
| Andreas Griesmayer | Flemming Nielson     | Uwe Waldmann        |
| Sumit Gulwani      | Hakjoo Oh            | Thomas Wies         |
| Masami Hagiya      | Daejun Park          | Herbert Wiklicky    |
| Hwansoo Han        | Sungwoo Park         | Eran Yahav          |
| Trevor Hansen      | Michael Petter       | Greta Yorsh         |
| Rene Rydhof Hansen | Alessandra Di Pierro | Enea Zaffanella     |
| Haifeng He         | Mila Dalla Preda     | Francesco Ranzato   |

# Table of Contents

## Invited Papers

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| Refactoring Using Type Constraints .....                                          | 1  |
| <i>Frank Tip</i>                                                                  |    |
| Programming Language Design and Analysis Motivated by Hardware<br>Evolution ..... | 18 |
| <i>Alan Mycroft</i>                                                               |    |

## Contributed Papers

|                                                                                                                        |     |
|------------------------------------------------------------------------------------------------------------------------|-----|
| A Compilation Model for Aspect-Oriented Polymorphically Typed<br>Functional Languages .....                            | 34  |
| <i>Kung Chen, Shu-Chun Weng, Meng Wang, Siau-Cheng Khoo, and<br/>Chung-Hsin Chen</i>                                   |     |
| Lattice Automata: A Representation for Languages on Infinite<br>Alphabets, and Some Applications to Verification ..... | 52  |
| <i>Tristan Le Gall and Bertrand Jeannet</i>                                                                            |     |
| Compositional Verification and 3-Valued Abstractions Join Forces .....                                                 | 69  |
| <i>Sharon Shoham and Orna Grumberg</i>                                                                                 |     |
| Formalised Inductive Reasoning in the Logic of Bunched Implications...                                                 | 87  |
| <i>James Brotherston</i>                                                                                               |     |
| Optimal Abstraction on Real-Valued Programs .....                                                                      | 104 |
| <i>David Monniaux</i>                                                                                                  |     |
| Taming the Wrapping of Integer Arithmetic .....                                                                        | 121 |
| <i>Axel Simon and Andy King</i>                                                                                        |     |
| Under-Approximations of Computations in Real Numbers Based on<br>Generalized Affine Arithmetic .....                   | 137 |
| <i>Eric Goubault and Sylvie Putot</i>                                                                                  |     |
| A Framework for End-to-End Verification and Evaluation of Register<br>Allocators .....                                 | 153 |
| <i>V. Krishna Nandivada, Fernando Magno Quintão Pereira, and<br/>Jens Palsberg</i>                                     |     |
| A New Algorithm for Identifying Loops in Decompilation .....                                                           | 170 |
| <i>Tao Wei, Jian Mao, Wei Zou, and Yu Chen</i>                                                                         |     |

|                                                                                    |     |
|------------------------------------------------------------------------------------|-----|
| Accelerated Data-Flow Analysis .....                                               | 184 |
| <i>Jérôme Leroux and Grégoire Sutre</i>                                            |     |
| Abstract Error Projection .....                                                    | 200 |
| <i>Akash Lal, Nicholas Kidd, Thomas Reps, and Tayssir Touili</i>                   |     |
| Precise Thread-Modular Verification .....                                          | 218 |
| <i>Alexander Malkis, Andreas Podelski, and Andrey Rybalchenko</i>                  |     |
| Modular Safety Checking for Fine-Grained Concurrency .....                         | 233 |
| <i>Cristiano Calcagno, Matthew Parkinson, and Viktor Vafeiadis</i>                 |     |
| Static Analysis of Dynamic Communication Systems by Partner<br>Abstraction .....   | 249 |
| <i>Jörg Bauer and Reinhard Wilhelm</i>                                             |     |
| Exploiting Pointer and Location Equivalence to Optimize Pointer<br>Analysis .....  | 265 |
| <i>Ben Hardekopf and Calvin Lin</i>                                                |     |
| Hierarchical Pointer Analysis for Distributed Programs .....                       | 281 |
| <i>Amir Kamil and Katherine Yelick</i>                                             |     |
| Semantics-Based Transformation of Arithmetic Expressions .....                     | 298 |
| <i>Matthieu Martel</i>                                                             |     |
| A Fast Implementation of the Octagon Abstract Domain on Graphics<br>Hardware ..... | 315 |
| <i>Francesco Banterle and Roberto Giacobazzi</i>                                   |     |
| Fixpoint-Guided Abstraction Refinements .....                                      | 333 |
| <i>Patrick Cousot, Pierre Ganty, and Jean-François Raskin</i>                      |     |
| Guided Static Analysis .....                                                       | 349 |
| <i>Denis Gopan and Thomas Reps</i>                                                 |     |
| Program Analysis Using Symbolic Ranges .....                                       | 366 |
| <i>Sriram Sankaranarayanan, Franjo Ivančić, and Aarti Gupta</i>                    |     |
| Shape Analysis with Structural Invariant Checkers .....                            | 384 |
| <i>Bor-Yuh Evan Chang, Xavier Rival, and George C. Necula</i>                      |     |
| Footprint Analysis: A Shape Analysis That Discovers Preconditions ....             | 402 |
| <i>Cristiano Calcagno, Dino Distefano, Peter W. O'Hearn, and<br/>Hongseok Yang</i> |     |
| Arithmetic Strengthening for Shape Analysis .....                                  | 419 |
| <i>Stephen Magill, Josh Berdine, Edmund Clarke, and Byron Cook</i>                 |     |
| Astrée: From Research to Industry .....                                            | 437 |
| <i>David Delmas and Jean Souyris</i>                                               |     |

Magic-Sets Transformation for the Analysis of Java Bytecode . . . . . 452  
    *Étienne Payet and Fausto Spoto*

**Author Index . . . . . 469**