

*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*

Alfred Kobsa

*University of California, Irvine, CA, 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

*Microsoft Research, Cambridge, MA, USA*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max-Planck Institute of Computer Science, Saarbruecken, Germany*

Jens Palsberg Zhendong Su (Eds.)

# Static Analysis

16th International Symposium, SAS 2009  
Los Angeles, CA, USA, August 9-11, 2009  
Proceedings

Volume Editors

Jens Palsberg

University of California, Department of Computer Science  
4531K Boelter Hall, Los Angeles, CA 90095-1596, USA  
E-mail: palsberg@cs.ucla.edu

Zhendong Su

University of California, Department of Computer Science  
1 Shields Avenue, Davis, CA 95616, USA  
E-mail: su@cs.ucdavis.edu

Library of Congress Control Number: 2009930752

CR Subject Classification (1998): D.3, F.3.1-2, I.2.2, F.4.2, B.8.1, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743  
ISBN-10 3-642-03236-2 Springer Berlin Heidelberg New York  
ISBN-13 978-3-642-03236-3 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.com

© Springer-Verlag Berlin Heidelberg 2009  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India  
Printed on acid-free paper SPIN: 12721160 06/3180 5 4 3 2 1 0

# Preface

Static analysis is increasingly recognized as a fundamental tool for program verification, bug detection, compiler optimization, program understanding, and software maintenance. The series of Static Analysis Symposia has served as the primary venue for presentation of theoretical, practical, and application advances in the area.

This volume contains the proceedings of the 16th International Static Analysis Symposium (SAS 2009), which was held August 9–11, 2009 at UCLA, University of California, Los Angeles, USA. The previous SAS conferences were held in Valencia, Spain (2008); Kongens Lyngby, Denmark (2007); Seoul, South Korea (2006); London, UK (2005); Verona, Italy (2004); San Diego, USA (2003); Madrid, Spain (2002); Paris, France (2001); Santa Barbara, USA (2000); Venice, Italy (1999); Pisa, Italy (1998); Paris, France (1997); Aachen, Germany (1996); Glasgow, UK (1995); and Namur, Belgium (1994).

In response to the call for papers, a total of 52 contributions were submitted to the symposium. After a five-week paper review period and a subsequent two-week online discussion, the Program Committee selected 21 papers for presentation at the symposium and inclusion in this volume. The selection was based on scientific quality, originality, and relevance to the symposium. Each submission was reviewed by four (or more) Program Committee members with the help of external reviewers.

In addition to the 21 accepted papers, this volume also contains abstracts of talks given by two invited speakers: Rastislav Bodik (University of California, Berkeley) and Shaz Qadeer (Microsoft).

SAS 2009 was co-located with LICS 2009, the 24th IEEE Symposium on Logic in Computer Science. SAS and LICS had a day with shared sessions, including an invited speaker: Edmund M. Clarke (Carnegie Mellon University, USA). Last time SAS and LICS were co-located was in 2000 in Santa Barbara, USA.

We would like to thank members of the Program Committee for their thorough reviews and dedicated involvement during the paper selection process. On behalf of the Program Committee, we would like to express our gratitude to all the authors who submitted papers and all the external reviewers for their invaluable contributions. We would also like to thank the Steering Committee for their help and advice, and Andrei Voronkov for making EasyChair available to us. Finally, we gratefully acknowledge the institution that sponsored this event: UCLA, University of California, Los Angeles, USA.

August 2009

Jens Palsberg  
Zhendong Su



## External Reviewers

Gogul Balakrishnan	Laurent Mauborgne
Demis Ballis	Jan Midtgaard
Gregory Batt	Yasuhiko Minamide
Ralph Becket	Antoine Miné
Julien Bertrane	Jorge Navas
Bruno Blanchet	Hakjoo Oh
Wei-Ngan Chin	Sungwoo Park
Duc Hiep Chu	Ruzica Piskac
Marco Comini	Bernie Pope
Vijay D'Silva	Shaz Qadeer
Julian Dolby	Sriram Rajamani
Santiago Escobar	G. Ramalingam
Jérôme Feret	Xavier Rival
Stephen Fink	Andrey Rybalchenko
Martin Fränzle	Andrew Santosa
Pierre Ganty	Ryosuke Sato
Matt Giuca	Peter Schachte
Trevor Hansen	Sharon Shoham
Martin Henz	Saurabh Srivastava
Jose Hernandez-Orallo	Peter Stuckey
Jose Iborra	Kohei Suenaga
Kazuhiro Inaba	Philippe Suter
Christophe Joubert	Carolyn Talcott
Siau-Cheng Khoo	Tachio Terauchi
William Klieber	Ashish Tiwari
Soonho Kong	Takeshi Tsukada
Laura Kovacs	Hiroshi Unno
Oukseh Lee	Kapil Vaswani
Zhenkai Liang	Martin Vechev
Yin Liu	Ramarathnam Venkatesan
Benjamin Livshits	Alicia Villanueva
Francesco Logozzo	Razvan Voicu
Salvador Lucas	Tanja Vos
Michael Maher	Thomas Wies
Roman Manevich	Hongseok Yang
Matthieu Martel	Greta Yorsh
Damien Massé	

## Sponsoring Institutions

University of California, Los Angeles, USA

# Table of Contents

## Invited Talks

Algorithmic Program Synthesis with Partial Programs and Decision Procedures . . . . .	1
<i>Rastislav Bodik</i>	
Algorithmic Verification of Systems Software Using SMT Solvers . . . . .	2
<i>Shaz Qadeer</i>	

## Contributed Papers

Abstraction Refinement for Quantified Array Assertions . . . . .	3
<i>Mohamed Nassim Seghir, Andreas Podelski, and Thomas Wies</i>	
Inferring Dataflow Properties of User Defined Table Processors . . . . .	19
<i>Songtao Xia, Manuel Fähndrich, and Francesco Logozzo</i>	
Polymorphic Fractional Capabilities . . . . .	36
<i>Hirotooshi Yasuoka and Tachio Terauchi</i>	
Automatic Parallelization and Optimization of Programs by Proof Rewriting . . . . .	52
<i>Clément Hurlin</i>	
Refinement of Trace Abstraction . . . . .	69
<i>Matthias Heizmann, Jochen Hoenicke, and Andreas Podelski</i>	
The Causal Graph Revisited for Directed Model Checking . . . . .	86
<i>Martin Wehrle and Malte Helmert</i>	
Proving the Correctness of the Implementation of a Control-Command Algorithm . . . . .	102
<i>Olivier Bouissou</i>	
Abstract Interpretation of FIFO Replacement . . . . .	120
<i>Daniel Grund and Jan Reineke</i>	
A Verifiable, Control Flow Aware Constraint Analyzer for Bounds Check Elimination . . . . .	137
<i>David Niedzielski, Jeffery von Ronne, Andreas Gampe, and Kleanthis Psarris</i>	
Increasing the Scope and Resolution of Interprocedural Static Single Assignment . . . . .	154
<i>Silvian Calman and Jianwen Zhu</i>	

Region Analysis for Race Detection .....	171
<i>Helmut Seidl and Vesal Vojdani</i>	
Bottom-Up Shape Analysis.....	188
<i>Bhargav S. Gulavani, Supratik Chakraborty,</i> <i>Ganesan Ramalingam, and Aditya V. Nori</i>	
The Complexity of Andersen’s Analysis in Practice .....	205
<i>Manu Sridharan and Stephen J. Fink</i>	
Optimizing Pointer Analysis Using Bisimilarity .....	222
<i>Luke Simon</i>	
Type Analysis for JavaScript .....	238
<i>Simon Holm Jensen, Anders Møller, and Peter Thiemann</i>	
Abstract Parsing: Static Analysis of Dynamically Generated String Output Using LR-Parsing Technology .....	256
<i>Kyung-Goo Doh, Hyunha Kim, and David A. Schmidt</i>	
Creating Transformations for Matrix Obfuscation .....	273
<i>Stephen Drape and Irina Voiculescu</i>	
Abstract Interpretation from a Topological Perspective .....	293
<i>David A. Schmidt</i>	
Interval Polyhedra: An Abstract Domain to Infer Interval Linear Relationships .....	309
<i>Liqian Chen, Antoine Miné, Ji Wang, and Patrick Cousot</i>	
Invariant Checking for Programs with Procedure Calls.....	326
<i>Guillem Godoy and Ashish Tiwari</i>	
Inter-program Properties .....	343
<i>Andrei Voronkov and Iman Narasamdya</i>	
<b>Author Index .....</b>	<b>361</b>