

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison, UK

Josef Kittler, UK

Friedemann Mattern, Switzerland

Moni Naor, Israel

Bernhard Steffen, Germany

Doug Tygar, USA

Takeo Kanade, USA

Jon M. Kleinberg, USA

John C. Mitchell, USA

C. Pandu Rangan, India

Demetri Terzopoulos, USA

Gerhard Weikum, Germany

## Advanced Research in Computing and Software Science

Subline of Lecture Notes in Computer Science

## Subline Series Editors

Giorgio Ausiello, *University of Rome 'La Sapienza', Italy*

Vladimiro Sassone, *University of Southampton, UK*

## Subline Advisory Board

Susanne Albers, *TU Munich, Germany*

Benjamin C. Pierce, *University of Pennsylvania, USA*

Bernhard Steffen, *University of Dortmund, Germany*

Deng Xiaotie, *City University of Hong Kong*

Jeannette M. Wing, *Microsoft Research, Redmond, WA, USA*

More information about this series at <http://www.springer.com/series/7408>

Xavier Rival (Ed.)

# Static Analysis

23rd International Symposium, SAS 2016  
Edinburgh, UK, September 8–10, 2016  
Proceedings

*Editor*  
Xavier Rival  
Ecole Normale Supérieure  
Paris  
France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-662-53412-0            ISBN 978-3-662-53413-7 (eBook)  
DOI 10.1007/978-3-662-53413-7

Library of Congress Control Number: 2016950412

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer-Verlag GmbH Germany 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer-Verlag GmbH Berlin Heidelberg

# 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 the presentation of theoretical, practical, and applicational advances in the area. Previous symposia were held in Saint-Malo, Munich, Seattle, Deauville, Venice, Perpignan, Los Angeles, Valencia, Kongens Lyngby, Seoul, London, Verona, San Diego, Madrid, Paris, Santa Barbara, Pisa, Aachen, Glasgow, and Namur. This volume contains the papers presented at SAS 2016, the 23rd International Static Analysis Symposium. The conference was held on September 8–10, 2016 in Edinburgh, UK.

The conference received 55 submissions, each of which was reviewed by at least three Program Committee members. The Program Committee decided to accept 21 papers, which appear in this volume. As in previous years, authors of SAS submissions were able to submit a virtual machine image with artifacts or evaluations presented in the paper. In accordance with this, 19 submissions came with an artifact. Artifacts were used as an additional source of information during the evaluation of the submissions.

The Program Committee also invited four leading researchers to present invited talks: Jade Alglave (Microsoft Research UK), Thomas A. Henzinger (IST Austria, Klosterneuburg, Austria), Fausto Spoto (University of Verona, Italy), and Martin Vechev (ETH Zurich, Switzerland). We deeply thank them for accepting the invitations.

SAS 2016 was collocated with the Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2016) and the Symposium on Principles and Practice of Declarative Programming (PPDP 2016) and it featured five associated workshops: the Workshop on Static Analysis and Systems Biology (SASB 2016) and the Workshop on Tools for Automatic Program Analysis (TAPAS 2016) were held before SAS, on the 7th of September; the Numerical and Symbolic Abstract Domains Workshop (NSAD 2016), the Workshop on Static Analysis of Concurrent Software, and REPS AT SIXTY were held after SAS, on the 11th of September.

The work of the Program Committee and the editorial process were greatly facilitated by the EasyChair conference management system. We are grateful to Springer for publishing these proceedings, as they have done for all SAS meetings since 1993.

Many people contributed to the success of SAS 2015. We would first like to thank the members of the Program Committee, who worked hard at carefully reviewing papers, holding extensive discussions during the on-line Program Committee meeting, and making final selections of accepted papers and invited speakers. We would also like to thank the additional referees enlisted by Program Committee members. We thank the Steering Committee members for their advice. A special acknowledgment

goes to James Cheney for leading the local organization of the conference and to the University of Edinburgh for hosting the Conference. Finally, we would like to thank our sponsors: Facebook, Fondation de l'ENS, and Springer.

July 2016

Xavier Rival

# Organization

## Program Committee

Bor-Yuh Evan Chang	University of Colorado Boulder, USA
Patrick Cousot	New York University, USA
Vijay D'Silva	Google Inc., USA
Javier Esparza	Technical University of Munich, Germany
Jérôme Feret	Inria/CNRS/Ecole Normale Supérieure, France
Pierre Ganty	IMDEA Software Institute, Spain
Roberto Giacobazzi	University of Verona, Italy
Atsushi Igarashi	Kyoto University, Japan
Andy King	University of Kent, UK
Francesco Logozzo	Facebook, USA
Roman Manevich	Ben-Gurion University of the Negev, Israel
Matthieu Martel	Université de Perpignan Via Domitia, France
Jan Midtgaard	Technical University of Denmark, Denmark
Ana Milanova	Rensselaer Polytechnic Institute, USA
Mayur Naik	Georgia Institute of Technology, USA
Francesco Ranzato	University of Padua, Italy
Xavier Rival	Inria/CNRS/Ecole Normale Supérieure, France
Sukyoung Ryu	KAIST, South Korea
Francesca Scozzari	Università di Chieti-Pescara, Italy
Caterina Urban	ETH Zürich, Switzerland
Bow-Yaw Wang	Academia Sinica, Taiwan
Kwangkeun Yi	Seoul National University, South Korea

## Additional Reviewers

Adje, Assale	Hur, Chung-Kil	Seidl, Helmut
Amato, Gianluca	Jourdan, Jacques-Henri	Seladji, Yassamine
Brutschy, Lucas	Kang, Jeehoon	Si, Xujie
Chapoutot, Alexandre	Kong, Soonho	Singh, Gagandeep
Chawdhary, Aziem	Lee, Woosuk	Stein, Benno
Chen, Yu-Fang	Meier, Shawn	Suwimonteerabuth,
Cho, Sungkeun	Meyer, Roland	Dejvuth
Dogadov, Boris	Miné, Antoine	Tsai, Ming-Hsien
Garoche, Pierre-Loic	Mover, Sergio	Walukiewicz, Igor
Haller, Leopold	Oh, Hakjoo	Werey, Alexis
Heo, Kihong	Seed, Tom	Zhang, Xin

# Contents

## Invited Papers

Simulation and Invariance for Weak Consistency . . . . .	3
<i>Jade Alglave</i>	
Quantitative Monitor Automata . . . . .	23
<i>Krishnendu Chatterjee, Thomas A. Henzinger, and Jan Otop</i>	
The Julia Static Analyzer for Java . . . . .	39
<i>Fausto Spoto</i>	

## Full Papers

Automated Verification of Linearization Policies . . . . .	61
<i>Parosh Aziz Abdulla, Bengt Jonsson, and Cong Quy Trinh</i>	
Structure-Sensitive Points-To Analysis for C and C++ . . . . .	84
<i>George Balatsouras and Yannis Smaragdakis</i>	
Bounded Abstract Interpretation . . . . .	105
<i>Maria Christakis and Valentin Wüstholtz</i>	
Completeness in Approximate Transduction . . . . .	126
<i>Mila Dalla Preda, Roberto Giacobazzi, and Isabella Mastroeni</i>	
Relational Verification Through Horn Clause Transformation . . . . .	147
<i>Emanuele De Angelis, Fabio Fioravanti, Alberto Pettorossi, and Maurizio Proietti</i>	
Securing a Compiler Transformation . . . . .	170
<i>Chaoqiang Deng and Kedar S. Namjoshi</i>	
Exploiting Sparsity in Difference-Bound Matrices . . . . .	189
<i>Graeme Gange, Jorge A. Navas, Peter Schachte, Harald Søndergaard, and Peter J. Stuckey</i>	
Flow- and Context-Sensitive Points-To Analysis Using Generalized Points-To Graphs . . . . .	212
<i>Pritam M. Gharat, Uday P. Khedker, and Alan Mycroft</i>	
Learning a Variable-Clustering Strategy for Octagon from Labeled Data Generated by a Static Analysis . . . . .	237
<i>Kihong Heo, Hakjoo Oh, and Hongseok Yang</i>	



Static Analysis by Abstract Interpretation of the Functional Correctness of Matrix Manipulating Programs . . . . .	257
<i>Matthieu Journault and Antoine Miné</i>	
Generalized Homogeneous Polynomials for Efficient Template-Based Nonlinear Invariant Synthesis . . . . .	278
<i>Kensuke Kojima, Minoru Kinoshita, and Kohei Suenaga</i>	
On the Linear Ranking Problem for Simple Floating-Point Loops . . . . .	300
<i>Fonenantsoa Maurica, Frédéric Mesnard, and Étienne Payet</i>	
Alive-FP: Automated Verification of Floating Point Based Peephole Optimizations in LLVM. . . . .	317
<i>David Menendez, Santosh Nagarakatte, and Aarti Gupta</i>	
A Parametric Abstract Domain for Lattice-Valued Regular Expressions . . . . .	338
<i>Jan Midtgaard, Flemming Nielson, and Hanne Riis Nielson</i>	
Cell Morphing: From Array Programs to Array-Free Horn Clauses . . . . .	361
<i>David Monniaux and Laure Gonnord</i>	
Loopy: Programmable and Formally Verified Loop Transformations . . . . .	383
<i>Kedar S. Namjoshi and Nimit Singhania</i>	
Abstract Interpretation of Supermodular Games. . . . .	403
<i>Francesco Ranzato</i>	
Validating Numerical Semidefinite Programming Solvers for Polynomial Invariants. . . . .	424
<i>Pierre Roux, Yuen-Lam Voronin, and Sriram Sankaranarayanan</i>	
Enforcing Termination of Interprocedural Analysis . . . . .	447
<i>Stefan Schulze Frielinghaus, Helmut Seidl, and Ralf Vogler</i>	
From Array Domains to Abstract Interpretation Under Store-Buffer-Based Memory Models . . . . .	469
<i>Thibault Suzanne and Antoine Miné</i>	
Making $k$ -Object-Sensitive Pointer Analysis More Precise with Still $k$ -Limiting . . . . .	489
<i>Tian Tan, Yue Li, and Jingling Xue</i>	
<b>Author Index . . . . .</b>	<b>511</b>