

*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, *Peking University, Beijing, China*

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

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

Andreas Podelski (Ed.)

# Static Analysis

25th International Symposium, SAS 2018  
Freiburg, Germany, August 29–31, 2018  
Proceedings

*Editor*  
Andreas Podelski  
Universität Freiburg  
Freiburg  
Germany

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-99724-7              ISBN 978-3-319-99725-4 (eBook)  
<https://doi.org/10.1007/978-3-319-99725-4>

Library of Congress Control Number: 2018952240

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2018

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

Static analysis is 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 Edinburgh, Saint-Malo, Munich, Seattle, Deauville, Venice, Perpignan, Los Angeles, Valencia, Kongens Lyngby, Seoul, London, Verona, San Diego, Madrid, Paris, Santa Barbara, Pisa, Aachen, Glasgow, Namur, and New York. This volume contains the papers presented at SAS 2018, the 25th International Static Analysis Symposium. The conference was held during August 29–31, 2018, at Freiburg, Germany.

SAS 2018 featured two associated workshops: the 9th Workshop on Static Analysis and Systems Biology (SASB 2018), and the 9th Workshop on Tools for Automatic Program Analysis (TAPAS 2017), which were held on August 27, 2018, the day before the conference.

The conference received 37 submissions. Each submission was reviewed by at least three Program Committee members. The Program Committee decided to accept 18 papers, which appear in this volume.

In addition to the regular paper review, we organized a separate evaluation for artifacts submitted by authors, together with their papers. Previous editions of SAS also allowed authors to submit artifacts, but this was the first edition where artifacts were evaluated on their own, by a specific committee. Out of the 16 submissions that came with an artifact, nine were accepted. Only the artifacts of the accepted papers were considered for the evaluation. Each of the nine artifacts was evaluated by two or three members of the artifact evaluation committee. The evaluation aimed at making sure that each artifact allows one to reproduce most or all of the results of the paper. Finally, seven artifacts were found of sufficient quality to pass the evaluation. Authors of accepted artifacts were allowed to add to their paper an artifact-approved badge. We hope that this experience will encourage effort for greater reproducibility of results in static analysis.

The program includes invited talks by Aws Albarghouthi (University of Wisconsin–Madison, USA), Zachary Kincaid (Princeton University, USA), Ruzica Piskac (Yale University, USA), Sharon Shoham (Tel Aviv University, Israel), and invited tutorials by Roberto Bagnara (University of Parma/BUGSENG, Italy), Ken McMillan (Microsoft Research, USA), Oded Padon (Tel Aviv University, Israel), and Peter O’Hearn (University College London/Facebook, UK). We warmly thank these speakers for accepting the invitations.

Many people and institutions contributed to the success of SAS 2018. We would like to thank the members of the Program Committee, who worked hard at carefully reviewing papers, holding insightful discussions during the online Program Committee meeting, and making final selections of accepted papers. We would also like to thank

the additional referees enlisted by Program Committee members. The work of the Program Committee and the editorial process was greatly facilitated by the EasyChair conference management system. We are grateful to Springer for publishing these proceedings. Finally, we would like to thank our sponsors: Hahn-Schickard, Facebook, Axivion, ENS Paris, University of Padova, and Springer.

July 2018

Andreas Podelski  
(Program Committee Chair)  
Xavier Rival  
(Artifact Evaluation Chair)

# Organization

## Program Committee

Domagoj Babic	Google
Sam Blackshear	Facebook
Marc Brockschmidt	Microsoft
Bor-Yuh Evan Chang	University of Colorado Boulder, USA
Swarat Chaudhuri	Rice University, USA
Jerome Feret	Inria, France
Ashutosh Gupta	TIFR
Nicolas Halbwachs	CNRS/Verimag, France
Lukas Holik	Brno University of Technology, Czech Republic
Barbara König	Universität Duisburg-Essen, Germany
Boris Köpf	IMDEA Software Institute, Spain
Shuvendu Lahiri	Microsoft
Hakjoo Oh	Korea University, South Korea
Andreas Podelski	University of Freiburg, Germany
Sylvie Putot	LIX, Ecole Polytechnique, France
Francesco Ranzato	University of Padova, Italy
Jakob Rehof	TU Dortmund University, Germany
Xavier Rival	Inria/CNRS/ENS Paris/PSL University, France
Sriram Sankaranarayanan	University of Colorado Boulder, USA
Harald Sondergaard	The University of Melbourne, Australia
Alexander J. Summers	ETH Zurich, Switzerland
Ashish Tiwari	SRI International, USA
Caterina Urban	ETH Zurich, Switzerland
Lenore Zuck	University of Illinois at Chicago, USA
Damien Zufferey	MPI-SWS, Germany
Florian Zuleger	Vienna University of Technology, Austria

## Additional Reviewers

Allamanis, Miltos	Choi, Wontae	Gange, Graeme
Andrion, Mak	Chu, Duc Hiep	Ghorbal, Khalil
Balakrishnan, Gogul	Cox, Arlen	Giacobazzi, Roberto
Chakarov, Aleksandar	D’Osualdo, Emanuele	Goubault, Eric
Chen, Yu-Fang	Dubreil, Jeremy	Hollingham, Nicholas
Cho, Sungkeun	Fuhs, Carsten	Journault, Matthieu

Katelaan, Jens  
Lengal, Ondrej  
Lopes, Nuno P.  
Ouadjaout, Abdelraouf  
Roux, Pierre

Simon, Axel  
Srinivasan, Venkatesh  
Stefanescu, Andrei  
Stuckey, Peter J.  
Sung, Chungha

Ulbrich, Mattias  
Unadkat, Divyesh  
Wang, Yuepeng  
Zanella, Marco



# Contents

Fairness: A Formal-Methods Perspective . . . . .	1
<i>Aws Albarghouthi</i>	
The MISRA C Coding Standard and its Role in the Development and Analysis of Safety- and Security-Critical Embedded Software. . . . .	5
<i>Roberto Bagnara, Abramo Bagnara, and Patricia M. Hill</i>	
Numerical Invariants via Abstract Machines . . . . .	24
<i>Zachary Kincaid</i>	
Deductive Verification in Decidable Fragments with Ivy . . . . .	43
<i>Kenneth L. McMillan and Oded Padon</i>	
Experience Developing and Deploying Concurrency Analysis at Facebook. . .	56
<i>Peter O’Hearn</i>	
New Applications of Software Synthesis: Verification of Configuration Files and Firewall Repair . . . . .	71
<i>Ruzica Piskac</i>	
Interactive Verification of Distributed Protocols Using Decidable Logic. . . . .	77
<i>Sharon Shoham</i>	
Abstract Interpretation of Stateful Networks . . . . .	86
<i>Kalev Alpernas, Roman Manevich, Aurojit Panda, Mooly Sagiv, Scott Shenker, Sharon Shoham, and Yaron Velner</i>	
Block-Size Independence for GPU Programs . . . . .	107
<i>Rajeev Alur, Joseph Devietti, and Nimit Singhanian</i>	
Extending Constraint-Only Representation of Polyhedra with Boolean Constraints . . . . .	127
<i>Alexey Bakirkin and David Monniaux</i>	
An Efficient Abstract Domain for Not Necessarily Closed Polyhedra. . . . .	146
<i>Anna Becchi and Enea Zaffanella</i>	
Modular Software Fault Isolation as Abstract Interpretation . . . . .	166
<i>Frédéric Besson, Thomas Jensen, and Julien Lepiller</i>	
Closing the Performance Gap Between Doubles and Rationals for Octagons. . .	187
<i>Aziem Chawdhary and Andy King</i>	

Verifying Properties of Differentiable Programs . . . . .	205
<i>Jan Hückelheim, Ziqing Luo, Sri Hari Krishna Narayanan, Stephen Siegel, and Paul D. Hovland</i>	
A Reduced Product of Absolute and Relative Error Bounds for Floating-Point Analysis. . . . .	223
<i>Maxime Jacquemin, Sylvie Putot, and Franck Védrine</i>	
Modular Static Analysis of String Manipulations in C Programs . . . . .	243
<i>Matthieu Journault, Antoine Miné, and Abdelraouf Ouadjaout</i>	
Verifying Bounded Subset-Closed Hyperproperties . . . . .	263
<i>Isabella Mastroeni and Michele Pasqua</i>	
Process-Local Static Analysis of Synchronous Processes . . . . .	284
<i>Jan Midtgaard, Flemming Nielson, and Hanne Riis Nielson</i>	
The Impact of Program Transformations on Static Program Analysis. . . . .	306
<i>Kedar S. Namjoshi and Zvonimir Pavlinovic</i>	
Efficiently Learning Safety Proofs from Appearance as well as Behaviours. . . . .	326
<i>Sumanth Prabhu, Kumar Madhukar, and R. Venkatesh</i>	
Invertible Linear Transforms of Numerical Abstract Domains . . . . .	344
<i>Francesco Ranzato and Marco Zanella</i>	
Incremental Verification Using Trace Abstraction . . . . .	364
<i>Bat-Chen Rothenberg, Daniel Dietsch, and Matthias Heizmann</i>	
Volume-Based Merge Heuristics for Disjunctive Numeric Domains. . . . .	383
<i>Andrew Ruef, Kesha Hietala, and Arlen Cox</i>	
Abstract Interpretation of CTL Properties. . . . .	402
<i>Caterina Urban, Samuel Ueltschi, and Peter Müller</i>	
Inductive Termination Proofs with Transition Invariants and Their Relationship to the Size-Change Abstraction. . . . .	423
<i>Florian Zuleger</i>	
<b>Author Index</b> . . . . .	445