

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, and Namur. This volume contains the papers presented at SAS 2017, the 24th International Static Analysis Symposium. The conference was held on August 30th - September 1st, 2017 at New York University, New York City, NY, USA.

The conference received 64 initial abstracts that materialized into 50 full submissions, each of which was reviewed by at least three Program Committee members. The Program Committee accepted 22 papers, which appear in this volume. As in previous years, authors of SAS submissions had the chance to submit a virtual machine image with artifacts presented in the paper. In accordance with this, 16 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 three outstanding researchers to present invited talks: Alex Aiken (Stanford University, USA), Francesco Logozzo (Facebook, Seattle, USA), Peter Müller (ETH Zurich, Switzerland). Additionally, the program included two invited tutorials given by leading researchers: Josh Berdine (Facebook, London, UK), Roberto Giacobazzi (IMDEA, Spain and University of Verona, Italy). We warmly thank them for accepting the invitations.

SAS 2017 featured three associated workshops: 7th Workshop on Numerical and Symbolic Abstract Domains (NSAD 2017), 8th Workshop on Static Analysis and Systems Biology (SASB 2017), 8th Workshop on Tools for Automatic Program Analysis (TAPAS 2017) were held before SAS, on August 29th, 2017.

Many people and institutions contributed to the success of SAS 2017. We would like to thank the members of the Program Committee, who worked hard at carefully reviewing papers, holding insightful 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. 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. A warm thank goes to Patrick Cousot for leading the local organization of the conference at New York University. Finally, we would like to thank our sponsors: Amazon, Courant Institute of Mathematical Sciences of New York University, Dipartimento di Matematica “Tullio Levi-Civita” of University of Padova, Facebook, and Springer.

July 2017
Padova

Francesco Ranzato

Table of Contents

| | |
|--|-----|
| Proving Program Equality: Recent Progress and New Applications | 1 |
| <i>Alex Aiken</i> | |
| From Bug Bounty to Static Analysis | 2 |
| <i>Francesco Logozzo</i> | |
| Reasoning with Permissions in Viper | 3 |
| <i>Peter Müller</i> | |
| Probabilistic Horn Clause Verification | 4 |
| <i>Aws Albarghouthi</i> | |
| Combining Forward and Backward Abstract Interpretation of Horn Clauses | 25 |
| <i>Alexey Bakirkin and David Monniaux</i> | |
| Abstract Semantic Diffing of Evolving Concurrent Programs | 46 |
| <i>Ahmed Bouajjani, Constantin Enea and Shuvendu Lahiri</i> | |
| Learning Shape Analysis | 66 |
| <i>Marc Brockschmidt, Yuxin Chen, Pushmeet Kohli, Siddharth Krishna and Daniel Tarlow</i> | |
| Securing The SSA Transform | 86 |
| <i>Chaoqiang Deng and Kedar Namjoshi</i> | |
| Relative Store Fragments for Singleton Abstraction | 105 |
| <i>Leandro Facchinetti, Zachary Palmer and Scott Smith</i> | |
| Loop Invariants from Counterexamples | 125 |
| <i>Marius Greitschus, Daniel Dietsch and Andreas Podelski</i> | |
| A Context-Sensitive Memory Model for Verification of C/C++ Programs | 146 |
| <i>Arie Gurfinkel and Jorge A. Navas</i> | |
| Effect Summaries for Thread-Modular Analysis | 167 |
| <i>Lukas Holik, Roland Meyer, Tomas Vojnar and Sebastian Wolff</i> | |
| Toward a Sound Analysis of Guarded LTI Loops with Inputs by Abstract Acceleration | 187 |
| <i>Colas Le Guernic</i> | |
| Scalable Minimizing-Operators on Polyhedra via Parametric Linear Programming | 207 |
| <i>Alexandre Maréchal, David Monniaux and Michael Perin</i> | |

| | |
|--|-----|
| Hyperhierarchy of Semantics - A formal framework for Hyperproperties Verification | 227 |
| <i>Isabella Mastroeni and Michele Pasqua</i> | |
| Thread-Local Semantics and its Efficient Sequential Abstractions for Race-Free Programs | 247 |
| <i>Suvam Mukherjee, Oded Padon, Sharon Shoham, Deepak D'Souza and Noam Rimetzky</i> | |
| Quantitative Static Analysis of Communication Protocols using Abstract Markov Chains | 268 |
| <i>Abdelraouf Ouadjaout and Antoine Miné</i> | |
| Portability Analysis for Weak Memory Models. Porthos: One Tool for all Models | 288 |
| <i>Hernan Ponce-De-Leon, Florian Furbach, Keijo Heljanko and Roland Meyer</i> | |
| Template Polyhedra with a Twist | 309 |
| <i>Sriram Sankaranarayanan and Mohamed Amin Ben Sassi</i> | |
| A new Abstraction Framework for Affine Transformers | 329 |
| <i>Tushar Sharma and Thomas Reps</i> | |
| Synthesizing Imperative Programs from Examples Guided by Static Analysis | 349 |
| <i>Sunbeom So and Hakjoo Oh</i> | |
| A Gradual Interpretation of Union Types | 366 |
| <i>Matías Toro and Éric Tanter</i> | |
| Modular Demand-Driven Analysis of Semantic Difference for Program Versions | 388 |
| <i>Anna Trostanetski, Orna Grumberg and Daniel Kroening</i> | |
| Verifying Array Manipulating Programs by Tiling | 410 |
| <i>Divyesh Unadkat, Supratik Chakraborty and Ashutosh Gupta</i> | |
| Incremental Analysis for Probabilistic Programs | 431 |
| <i>Jieyuan Zhang, Yulei Sui and Jingling Xue</i> | |

Program Committee

| | |
|---------------------|--|
| Elvira Albert | Complutense University of Madrid |
| Jade Alglave | University College London |
| Josh Berdine | Facebook |
| Aleksandar Chakarov | University of Colorado, Boulder, CO |
| Liqian Chen | National University of Defense Technology |
| Maria Christakis | University of Kent |
| Pierre Ganty | IMDEA Software Institute |
| Alberto Griggio | FBK-IRST |
| Arie Gurfinkel | University of Waterloo |
| Thomas Jensen | INRIA |
| Laura Kovacs | Vienna University of Technology |
| Ana Milanova | Rensselaer Polytechnic Institute |
| Anders Moller | Aarhus University |
| Kedar Namjoshi | Bell Labs |
| Andreas Podelski | University of Freiburg |
| Francesco Ranzato | Dipartimento di Matematica, University of Padova, Italy |
| Xavier Rival | INRIA / ENS Paris |
| Ilya Sergey | University College London |
| Fausto Spoto | Dipartimento di Informatica, Verona |
| Harald Søndergaard | The University of Melbourne |
| Caterina Urban | ETH Zürich |
| David Van Horn | University of Maryland |
| Arnaud J. Venet | Google, Inc. |
| Eran Yahav | Technion |

Additional Reviewers

B

Besson, Frederic

C

Correas Fernández, Jesús

D

Dietsch, Daniel

Dohrau, Jérôme

F

Fedyukovich, Grigory

Ferrara, Pietro

Frehse, Goran

G

Gange, Graeme

Gleiss, Bernhard

Gordillo, Pablo

Greitschus, Marius

I

Irfan, Ahmed

J

Jaroschek, Maximilian

K

Kaffe, Bishoksan

Karpenkov, Egor

Khalimov, Ayrat

Krishna, Siddharth

L

Li, Huisong

M

Martin-Martin, Enrique

N

Navas, Jorge A

P

Popeea, Corneliu

R

Rebola Pardo, Adrian

Robillard, Simon

Román-Díez, Guillermo

S

Sankaranarayanan, Sriram

Schachte, Peter

Schilling, Christian

Schrammel, Peter

Steinhöfel, Dominic