Proceedings of the 29th International Symposium (SAS 2022)

Gagandeep Singh, Caterina Urban

To cite this version:


HAL Id: hal-04249999
https://inria.hal.science/hal-04249999
Submitted on 19 Oct 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License
More information about this series at https://link.springer.com/bookseries/558
Static Analysis

29th International Symposium, SAS 2022
Auckland, New Zealand, December 5–7, 2022
Proceedings
This volume contains the proceedings of the 29th edition of the International Static Analysis Symposium, SAS 2022, held during December 5–7, 2022, in Auckland, New Zealand. The conference was a co-located event of SPLASH, the ACM SIGPLAN conference on Systems, Programming, Languages, and Applications: Software for Humanity. Travel restrictions as a result of the COVID-19 pandemic forced us to organize the conference in a hybrid form.

Static analysis is widely 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 application advances in the area. Previous symposia were held in Chicago, Porto, Freiburg, New York, Edinburgh, Saint-Malo, Munich, Seattle, Deauville, Venice, Perpignan, Los Angeles, Valencia, Korngens Lyngby, Seoul, London, Verona, San Diego, Madrid, Paris, Santa Barbara, Venice, Pisa, Paris, Aachen, Glasgow, and Namur.

SAS 2022 called for papers on topics including, but not limited to, abstract interpretation, automated deduction, data flow analysis, debugging techniques, deductive methods, emerging applications, model checking, data science, program optimizations and transformations, program synthesis, program verification, machine learning and verification, security analysis, tool environments and architectures, theoretical frameworks, type checking, and distributed or networked systems. Besides the regular papers, the authors were encouraged to submit short submissions in the NEAT category to discuss experiences with static analysis tools, industrial reports, and case studies, along with tool papers, brief announcements of work in progress, well-motivated discussions of new questions or new areas, etc. Authors were encouraged to submit artifacts accompanying their papers to strengthen evaluations and the reproducibility of results.

The conference employed a double-blind reviewing process with an author response period, supported on EasyChair. This year, SAS had 48 submitted papers (43 regular and five NEAT). Of these, five were desk rejected due to not being in scope for SAS. The Program Committee used a two-round review process, where each remaining submission received at least three first-round reviews, which the authors could then respond to. The author response period was followed by a two-week Program Committee discussion where consensus was reached on the papers to be accepted, after a thorough assessment of the relevance and the quality of the work. Overall, 18 papers were accepted for publication (16 regular and two NEAT) and appear in this volume. The submitted papers were authored by researchers around the world: Canada, China, France, Germany, India, Israel, Italy, Singapore, the UK, the USA, and several other countries.

We view the artifacts as being equally important for the success and development of static analysis as the written papers. It is important for researchers to be able to
independently reproduce experiments, which is greatly facilitated by having the original artifacts available. Marc Chevalier, the artifact committee chair, set up the artifact committee. In line with SAS 2021, the authors could submit either the Docker or Virtual Machine images as artifacts. A public archival repository for the artifacts is available on Zenodo, hosted at https://zenodo.org/communities/sas-2022. The artifacts have badges awarded at three levels: Validated (correct functionality), Extensible (with source code), and Available (on the Zenodo repository). The artwork for the badges is by Arpita Biswas (Harvard University) and Suvam Mukherjee (Microsoft). SAS 2022 had 16 valid artifact submissions, of which one was desk rejected as the authors did not submit a valid artifact. The review process for the artifacts was similar to those for the papers. Each artifact was evaluated by three members of the artifact evaluation committee, and eight out of 15 valid artifacts were accepted.

In addition to the contributed papers, SAS 2022 also featured three invited talks by distinguished researchers: Suguman Bansal (Georgia Tech, USA), Bernhard Scholz (University of Sydney, Australia), and Nengkun Yu (University of Technology Sydney, Australia). The Program Committee also selected the recipient of the Radhia Cousot Young Researcher Best Paper Award, given to a paper with a significant contribution from a student. This award was instituted in memory of Radhia Cousot, for her fundamental contributions to static analysis and having been one of the main promoters and organizers of the SAS series of conferences.

The SAS program would not have been possible without the efforts of many people. We thank them all. The members of the Program Committee, the artifact evaluation committee, and the external reviewers worked tirelessly to select a strong program, offering constructive and helpful feedback to the authors in their reviews. The organizing committee of SPLASH 2022, chaired by Alex Potanin (Australian National University, Australia), and the hybridization committee, chaired by Jonathan Aldrich (CMU, USA) and Youyou Kong (Tokyo Institute of Technology, Japan), were tremendously helpful in navigating the conference through these difficult times. The SAS steering committee provided much-needed support and advice. Finally, we thank Springer for their support of this event as well as for publishing these proceedings.

October 2022

Caterina Urban
Gagandeep Singh
Organization

Program Committee Chairs

Gagandeep Singh  VMware Research and UIUC, USA  
Caterina Urban  Inria and ENS|PSL, France  

Steering Committee

Bor-Yuh Evan Chang  University of Colorado Boulder, USA  
Patrick Cousot  New York University, USA  
Cezara Dragoi  Inria and ENS|PSL and Informal Systems, France  
Kedar Namjoshi  Nokia Bell Labs, USA  
David Pichardie  Meta, France  
Andreas Podelski  University of Freiburg, Germany  
Francesco Ranzato  University of Padua, Italy  
Mihaela Sighireanu  ENS Paris-Saclay, France  

Program Committee

Sebastien Bardin  CEA-List, France  
Liqian Chen  National University of Defense Technology, China  
Patrick Cousot  New York University, USA  
Arlen Cox  IDA and CCS, USA  
Dana Drachsler Cohen  Technion, Israel  
Jerome Feret  Inria and ENS|PSL, France  
Pietro Ferrara  Ca’ Foscari University of Venice, Italy  
Roberto Giacobazzi  University of Verona, Italy  
Kihong Heo  KAIST, South Korea  
Paddy Krishnan  Oracle Labs, Australia  
Isabella Mastroeni  University of Verona, Italy  
Antoine Miné  Sorbonne Université, France  
Raphaël Monat  Sorbonne Université, France  
David Monniaux  CNRS and VERIMAG, France  
Jorge A. Navas  SRI International, USA  
Francesco Ranzato  University of Padua, Italy  
Daniel Schoepe  Amazon, UK  
Mihaela Sighireanu  ENS Paris-Saclay, France  
Manu Sridharan  University of California, Riverside, USA  
Benno Stein  Meta, USA  
Laura Titolo  National Institute of Aerospace, USA
Artifact Evaluation Chair

Marc Chevalier  
Snyk, Switzerland

Artifact Evaluation Committee

Vincenzo Arceri  
University of Parma, Italy
Anna Becchi  
Fondazione Bruno Kessler, Italy
Dorra Ben Khalifa  
Université de Perpignan, France
Denis Bueno  
Sandia National Laboratories, USA
Marco Campion  
University of Verona, Italy
Madhurima Chakraborty  
University of California, Riverside, USA
Christiane Goltz  
Snyk, Switzerland
Kai Jia  
MIT, USA
Sifis Lagouvardos  
University of Athens, Greece
Jacob Laurel  
UIUC, USA
Denis Mazzucato  
Inria and ENS|PSL, France
Luca Negrini  
Corvallis Srl and Ca' Foscari University of Venice, Italy
Vivek Notani  
University of Verona, Italy
Luca Olivieri  
University of Verona, Italy
Francesco Parolini  
Sorbonne Université, France
Ilina Stoilkovska  
Amazon, UK

Additional Reviewers

Christophe Alias  
Victor Nicolet
Vincenzo Arceri  
Rei Odaira
Roberto Blanco  
Andreas Pavlogiannis
Loris D'Antoni  
Quentin Stievenart
Stefania Dumbrava  
Marco Zanella
Pierre Karpman  
Linpeng Zhang
Yi Lu
## Contents

### Invited Talks

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specification-Guided Reinforcement Learning</td>
<td>3</td>
</tr>
<tr>
<td>Suguman Bansal</td>
<td></td>
</tr>
<tr>
<td>Towards Efficient Reasoning of Quantum Programs</td>
<td>10</td>
</tr>
<tr>
<td>Nengkun Yu</td>
<td></td>
</tr>
</tbody>
</table>

### Regular Papers

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solving Invariant Generation for Unsolvable Loops</td>
<td>19</td>
</tr>
<tr>
<td>Daneshvar Amrollahi, Ezio Bartocci, George Kenison, Laura Kovács, Marcel Moosbrugger, and Miroslav Stankovič</td>
<td></td>
</tr>
<tr>
<td>Principles of Staged Static+Dynamic Partial Analysis</td>
<td>44</td>
</tr>
<tr>
<td>Aditya Anand and Manas Thakur</td>
<td></td>
</tr>
<tr>
<td>SecWasm: Information Flow Control for WebAssembly</td>
<td>74</td>
</tr>
<tr>
<td>Iulia Bastys, Maximilian Algehed, Alexander Sjösten, and Andrei Sabelfeld</td>
<td></td>
</tr>
<tr>
<td>Lifting Numeric Relational Domains to Algebraic Data Types</td>
<td>104</td>
</tr>
<tr>
<td>Santiago Bautista, Thomas Jensen, and Benoît Montagu</td>
<td></td>
</tr>
<tr>
<td>Automated Synthesis of Asynchronizations</td>
<td>135</td>
</tr>
<tr>
<td>Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea, and Shuvendu Lahiri</td>
<td></td>
</tr>
<tr>
<td>Case Study on Verification-Witness Validators: Where We Are and Where We Go</td>
<td>160</td>
</tr>
<tr>
<td>Dirk Beyer and Jan Strejček</td>
<td></td>
</tr>
<tr>
<td>Deciding Program Properties via Complete Abstractions on</td>
<td>175</td>
</tr>
<tr>
<td>Bounded Domains.</td>
<td></td>
</tr>
<tr>
<td>Roberto Bruni, Roberta Gori, and Nicolas Manini</td>
<td></td>
</tr>
<tr>
<td>Invariant Inference with Provable Complexity from the Monotone Theory</td>
<td>201</td>
</tr>
<tr>
<td>Yotam M. Y. Feldman and Sharon Shoham</td>
<td></td>
</tr>
<tr>
<td>Efficient Modular SMT-Based Model Checking of Pointer Programs</td>
<td>227</td>
</tr>
<tr>
<td>Isabel Garcia-Contreras, Arie Gurfinkel, and Jorge A. Navas</td>
<td></td>
</tr>
</tbody>
</table>
Property-Driven Code Obfuscations Reinterpreting Jones-Optimality in Abstract Interpretation ........................................ 247  
Roberto Giacobazzi and Isabella Mastroeni

Bootstrapping Library-Based Synthesis ................................. 272  
Kangjing Huang and Xiaokang Qiu

Boosting Robustness Verification of Semantic Feature Neighborhoods................................................................. 299  
Anan Kabaha and Dana Drachsler-Cohen

Fast and Incremental Computation of Weak Control Closure ................................................................. 325  
Abu Naser Masud

Local Completeness Logic on Kleene Algebra with Tests ................................................................. 350  
Marco Milanese and Francesco Ranzato

Semantic Foundations for Cost Analysis of Pipeline-Optimized Programs................................................................. 372  
Gilles Barthe, Adrien Koutsos, Solène Mirliaz, David Pichardie, and Peter Schwabe

Parameterized Recursive Refinement Types for Automated Program Verification ................................................................. 397  
Ryoya Mukai, Naoki Kobayashi, and Ryosuke Sato

Adversarial Logic ................................................................. 422  
Julien Vanegue

CLEVEREST: Accelerating CEGAR-based Neural Network Verification via Adversarial Attacks ................................................................. 449  
Zhe Zhao, Yedi Zhang, Guangke Chen, Fu Song, Taolue Chen, and Jiaxiang Liu

Author Index ......................................................................... 475