



**HAL**  
open science

# Proceedings of the 29th International Symposium (SAS 2022)

Gagandeep Singh, Caterina Urban

► **To cite this version:**

Gagandeep Singh, Caterina Urban. Proceedings of the 29th International Symposium (SAS 2022). Springer Nature Switzerland, 13790, 2022, Lecture Notes in Computer Science, 10.1007/978-3-031-22308-2 . hal-04249999

**HAL Id: hal-04249999**

**<https://inria.hal.science/hal-04249999v1>**

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

## Founding Editors

Gerhard Goos, Germany  
Juris Hartmanis, USA

## Editorial Board Members

Elisa Bertino, USA  
Wen Gao, China

Bernhard Steffen , Germany  
Moti Yung , USA

## 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 <https://link.springer.com/bookseries/558>

Gagandeep Singh · Caterina Urban (Eds.)

# Static Analysis

29th International Symposium, SAS 2022  
Auckland, New Zealand, December 5–7, 2022  
Proceedings

*Editors*

Gagandeep Singh  
VMware Research and University of Illinois  
Urbana-Champaign  
Urbana, IL, USA

Caterina Urban  
Inria and ENS/PSL  
Paris, France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-22307-5

ISBN 978-3-031-22308-2 (eBook)

<https://doi.org/10.1007/978-3-031-22308-2>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to  
Springer Nature Switzerland AG 2022

Chapter “Case Study on Verification-Witness Validators: Where We Are and Where We Go” is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapter.

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, expressed 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

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, Kongens 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





## **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
Irina 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

Specification-Guided Reinforcement Learning . . . . .	3
<i>Suguman Bansal</i>	
Towards Efficient Reasoning of Quantum Programs . . . . .	10
<i>Nengkun Yu</i>	

## Regular Papers

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

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 Drachler-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 Miriaz, 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