Lecture Notes in Computer Science **13182**

Founding Editors

Gerhard Goos, Germany
Juris Hartmanis, USA

Editorial Board Members

Elisa Bertino, USA
Wen Gao, China
Bernhard Steffen, Germany
Gerhard Woeginger, 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 subseries at https://link.springer.com/bookseries/7407

Bernd Finkbeiner · Thomas Wies (Eds.)

Verification, Model Checking, and Abstract Interpretation

23rd International Conference, VMCAI 2022 Philadelphia, PA, USA, January 16–18, 2022 Proceedings

Springer

Editors
Bernd Finkbeiner
Helmholtz Center for Information Security
Saarbrücken, Germany

Thomas Wies
New York University
New York, NY, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-94582-4 ISBN 978-3-030-94583-1 (eBook)
https://doi.org/10.1007/978-3-030-94583-1

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2022
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

Welcome to VMCAI 2022, the 23rd International Conference on Verification, Model Checking, and Abstract Interpretation. VMCAI 2022 was part of the 49th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL 2022), held at The Westin Philadelphia, USA, during January 16–22, 2022.

VMCAI provides a forum for researchers from the communities of verification, model checking, and abstract interpretation, facilitating interaction, cross-fertilization, and advancement of hybrid methods that combine these and related areas. The topics of the conference include program verification, model checking, abstract interpretation, program synthesis, static analysis, type systems, deductive methods, decision procedures, theorem proving, program certification, debugging techniques, program transformation, optimization, and hybrid and cyber-physical systems.

VMCAI 2022 received a total of 63 paper submissions. After a rigorous review process, with each paper reviewed by at least three Program Committee (PC) members, followed by an online discussion, the PC accepted 23 papers for publication in the proceedings and presentation at the conference. The main selection criteria were quality, relevance, and originality.

The conference program included three keynotes: Işil Dillig (University of Texas, Austin, USA) on "Computer-Aided Programming Across the Software Stack," Javier Esparza (Technical University of Munich, Germany) on "Back to the Future: A Fresh Look at Linear Temporal Logic," and Thomas A. Henzinger (Institute of Science and Technology Austria) on "Sequential Information Flow."

VMCAI 2022 continued the artifact evaluation process established by VMCAI 2020. The goals of artifact evaluation are as follows: (1) to encourage the development of tools that allow for replication of results in the paper, (2) to encourage reuse of tools by others in the community, and (3) to reward authors who spend the extra effort to create stable, portable, and usable artifacts. Artifacts are any additional material that substantiates the claims made in the paper. Examples of artifacts are software, tools, frameworks, data sets, test suites, and machine-checkable proofs. Authors of submitted papers were encouraged to submit an artifact to the VMCAI 2022 artifact evaluation committee (AEC). We also encouraged the authors to make their artifacts publicly and permanently available. Artifacts had to be provided as .zip or .tar.gz files and had to contain all necessary software for artifact evaluation as well as a README file describing the artifact and providing instructions on how to replicate the results. Artifacts were required to run in a virtual machine to ensure consistency of reproduction across the reviewing process.

All submitted artifacts were evaluated in parallel with the papers. We assigned three members of the AEC to each artifact and assessed it in two phases. First, the reviewers tested whether the artifacts were working, e.g., there were no corrupted or missing files and the evaluation did not crash on simple examples. For those artifacts that did not work, we sent the issues to the authors. The authors' answers to the reviewers were

distributed among the reviewers, and the authors were allowed to submit an updated artifact to fix issues found during the test phase. In the second phase, the assessment phase, the reviewers aimed at reproducing any experiments or activities and evaluated the artifact based on the following questions:

1. Is the artifact consistent with the paper and the claims made by the paper?
2. Are the results of the paper replicable through the artifact?
3. Is the artifact well documented?
4. Is the artifact easy to use?

In a change from the VMCAI Artifact Evaluation in 2021, this year we moved to a simplified badge model where a single badge was awarded for all passing artifacts. Of the 23 accepted papers, there were 16 submitted artifacts with 15 that passed the second phase and were thus awarded the Artifact Evaluation Badge.

We would like to thank, first of all, the authors for submitting their papers to VMCAI 2022. The PC and the AEC did a great job of reviewing: they contributed informed and detailed reports, and took part in the discussions during the virtual PC meeting. We warmly thank the keynote speakers for their participation and contributions. We also thank the general chair of the POPL 2022 week, Rajeev Alur, and his team for the overall organization. We thank the publication team at Springer for their support, and EasyChair for providing an excellent review system. Special thanks goes to the VMCAI Steering Committee for their helpful advice, assistance, and support.

December 2021

Bernd Finkbeiner
Thomas Wies
Mark Santolucito

Organization

Program Committee Chairs

Bernd Finkbeiner	CISPA Helmholtz Center for Information Security, Germany
Thomas Wies	New York University, USA

Artifact Evaluation Committee Chair

Mark Santolucito	Barnard College, USA

Program Committee

Aws Albarghouthi	University of Wisconsin-Madison, USA
Christel Baier	TU Dresden, Germany
Dirk Beyer	LMU Munich, Germany
Ahmed Bouajjani	IRIF, Université Paris Diderot, France
Yu-Fang Chen	Academia Sinica, China
Patrick Cousot	New York University, USA
Leonardo de Moura	Microsoft, USA
Rayna Dimitrova	CISPA Helmholtz Center for Information Security, Germany
Dino Distefano	Facebook, UK
Jean-Christophe Filliatre	CNRS, France
Orna Grumberg	Technion - Israel Institute of Technology, Israel
Liana Hadarean	Amazon Web Services, USA
William Harris	Galois Inc., USA
Laura Kovacs	Vienna University of Technology, Austria
Jan Kretinsky	Technical University of Munich, Germany
Siddharth Krishna	Microsoft Research, USA
Anna Lukina	TU Delft, The Netherlands
Roland Meyer	TU Braunschweig, Germany
Markus Müller-Olm	Westfälische Wilhelms-Universität Münster, Germany
Jorge A. Navas	SRI International, USA
Oded Padon	Stanford University, USA
Jens Palsberg	University of California, Los Angeles, USA
Corina Pasareanu	Carnegie Mellon University, NASA, KBR, USA
Andreas Podelski	University of Freiburg, Germany
Pavithra Prabhakar	Kansas State University, USA
Xavier Rival	Inria and ENS Paris, France
Cesar Sanchez	IMDEA Software Institute, Spain
Sriram Sankaranarayanan	University of Colorado Boulder, USA

Sven Schewe	University of Liverpool, UK
Martina Seidl	Johannes Kepler University Linz, Austria
Mihaela Sighireanu	LMF, ENS Paris-Saclay, Université Paris-Saclay and CNRS, France
Gagandeep Singh	University of Illinois Urbana-Champaign, USA
Serdar Tasiran	Amazon Web Services, USA
Cesare Tinelli	University of Iowa, USA
Laura Titolo	National Institute of Aerospace, USA
Lenore Zuck	University of Illinois Chicago, USA

Additional Reviewers

Azeem, Muqsit
Bondalakunta, Vishnu Teja
Bréhard, Florent
Capretto, Margarita
Ceresa, Martin
Chen, Yean-Ru
Chien, Po-Chun
Das, Spandan
Dietsch, Daniel
Evangelidis, Alexandros
Furbach, Florian
Garavel, Hubert
Georgiou, Pamina
Grover, Kush
Gutsfeld, Jens Oliver
Hajdu, Marton
Hajdu, Ákos
Hozzová, Petra
Iosif, Radu
Jhou, Yan-Ru
Kapus, Timotej
Klyuchnikov, Ilya
Kugler, Hillel
Kundu, Atreyee
Lal, Ratan
Larraz, Daniel
Melquiond, Guillaume
Mennicke, Stephan
Mutluergil, Suha Orhun
Noetzli, Andres
Nyx Brain, Martin
Ohrem, Christoph
Rappoport, Omer
Slagel, Joseph
Tsai, Wei-Lun
van der Wall, Sören
Vierling, Jannik
Weise, Nico
Yen, Di-De
Zufferey, Damien

Contents

Flavors of Sequential Information Flow 1
Ezio Bartocci, Thomas Ferrère, Thomas A. Henzinger, Dejan Nickovic, and Ana Oliveira da Costa

Relational String Abstract Domains 20
Vincenzo Arceri, Martina Olliaro, Agostino Cortesi, and Pietro Ferrara

Fanoos: Multi-resolution, Multi-strength, Interactive Explanations for Learned Systems 43
David Bayani and Stefan Mitsch

Loop Verification with Invariants and Contracts 69
Gidon Ernst

EPMC Gets Knowledge in Multi-agent Systems 93
Chen Fu, Ernst Moritz Hahn, Yong Li, Sven Schewe, Meng Sun, Andrea Turrini, and Lijun Zhang

High Assurance Software for Financial Regulation and Business Platforms 108
Stephen Goldbaum, Attila Mihaly, Tosha Ellison, Earl T. Barr, and Mark Marron

Gradient-Descent for Randomized Controllers Under Partial Observability . . . 127
Linus Heck, Jip Spel, Sebastian Junges, Joshua Moerman, and Joost-Pieter Katoen

Automata-Driven Partial Order Reduction and Guided Search for LTL Model Checking 151
Peter Gjøl Jensen, Jiří Srba, Nikolaj Jensen Ulrik, and Simon Mejlby Virenfeldt

Verifying Pufferfish Privacy in Hidden Markov Models 174
Depeng Liu, Bow-Yaw Wang, and Lijun Zhang

A Flow-Insensitive-Complete Program Representation 197
Solène Mirliaz and David Pichardie

Lightweight Shape Analysis Based on Physical Types 219
Olivier Nicole, Matthieu Lemerre, and Xavier Rival

Fast Three-Valued Abstract Bit-Vector Arithmetic 242
Jan Onderka and Stefan Ratschan

Satisfiability and Synthesis Modulo Oracles 263
Elizabeth Polgreen, Andrew Reynolds, and Sanjit A. Seshia

Bisimulations for Neural Network Reduction 285
Pavithra Prabhakar

NP Satisfiability for Arrays as Powers 301
Rodrigo Raya and Viktor Kunčak

STAMINA 2.0: Improving Scalability of Infinite-State Stochastic Model Checking 319
Riley Roberts, Thakur Neupane, Lukas Buecherl, Chris J. Myers, and Zhen Zhang

Generalized Arrays for Stainless Frames 332
Georg Stefan Schmid and Viktor Kunčak

Making PROGRESS in Property Directed Reachability 355
Tobias Seufert, Christoph Scholl, Arun Chandrasekharan, Sven Reimer, and Tobias Welp

Scaling Up Livelock Verification for Network-on-Chip Routing Algorithms 378
Landon Taylor and Zhen Zhang

Stateful Dynamic Partial Order Reduction for Model Checking Event-Driven Applications that Do Not Terminate 400
Rahmadi Trimananda, Weiyu Luo, Brian Demsky, and Guoqing Harry Xu

Verifying Solidity Smart Contracts via Communication Abstraction in SmartACE 425
Scott Wesley, Maria Christakis, Jorge A. Navas, Richard Trefler, Valentin Wüstholz, and Arie Gurfinkel

Out of Control: Reducing Probabilistic Models by Control-State Elimination 450
Tobias Winkler, Johannes Lehmann, and Joost-Pieter Katoen

Mixed Semantics Guided Layered Bounded Reachability Analysis of Compositional Linear Hybrid Automata 473
Yuming Wu, Lei Bu, Jiawan Wang, Xinyue Ren, Wen Xiong, and Xuandong Li

Bit-Precise Reasoning via Int-Blasting 496
Yoni Zohar, Ahmed Irfan, Makai Mann, Aina Niemetz, Andres Nötzli, Mathias Preiner, Andrew Reynolds, Clark Barrett, and Cesare Tinelli

Author Index 519