

## Founding Editors

Gerhard Goos

*Karlsruhe Institute of Technology, Karlsruhe, Germany*

Juris Hartmanis

*Cornell University, Ithaca, NY, USA*

## Editorial Board Members

Elisa Bertino

*Purdue University, West Lafayette, IN, USA*

Wen Gao

*Peking University, Beijing, China*

Bernhard Steffen 

*TU Dortmund University, Dortmund, Germany*

Gerhard Woeginger 

*RWTH Aachen, Aachen, Germany*

Moti Yung

*Columbia University, New York, NY, USA*

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

Zhe Hou · Vijay Ganesh (Eds.)

# Automated Technology for Verification and Analysis

19th International Symposium, ATVA 2021  
Gold Coast, QLD, Australia, October 18–22, 2021  
Proceedings

*Editors*

Zhe Hou   
Griffith University  
Brisbane, QLD, Australia

Vijay Ganesh  
University of Waterloo  
Waterloo, ON, Canada

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-88884-8              ISBN 978-3-030-88885-5 (eBook)  
<https://doi.org/10.1007/978-3-030-88885-5>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2021

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 papers presented at the 19th International Symposium on Automated Technology for Verification and Analysis (ATVA 2021). The ATVA series of symposia intends to promote research in theoretical and practical aspects of automated analysis, verification, and synthesis by providing a forum for interaction between the regional and international research communities and industry in related areas.

ATVA 2021 was planned to be hosted on the Gold Coast, Australia, in late October 2021. However, due to the COVID-19 pandemic and travel restrictions, the Steering Committee decided to host the conference virtually during October 18–22, 2021. ATVA 2021 received 75 submissions covering topics related to the theory of and applications in automated verification and analysis techniques. Each paper was reviewed by at least three reviewers, and the Program Committee (PC) accepted 19 regular papers and 4 tool papers, leading to a competitive and attractive scientific program.

This edition of ATVA was blessed by the presence of four prestigious keynote speakers. The first keynote was given by Sir Tony Hoare, a Turing Award and Kyoto Prize laureate. He discussed the link between algebra, geometry, and programming testing and verification using a unified theory. The second keynote speaker, Andrew Chi-Chih Yao from the Tsinghua University, is also a Turing Award and Kyoto Prize laureate. His expertise is in complexity theory and cryptography, and he presented novel ideas about computing and analysis from these angles. Moshe Vardi from the Rice University is another widely recognized top computer scientist and a Godel Prize winner. He talked about linear temporal logic and its applications in analysis and synthesis. Last, but not least, Jha from the University of Wisconsin presented insightful views on security, formal methods and adversarial machine learning. The four talks covered current hot research topics and revealed many new interesting research directions.

After the success of the workshops of the previous edition, we decided to co-host the conference with three workshops in related research areas: Security and Reliability of Machine Learning (SRML 2021), organized by Shiqi Wang, Huan Zhang, Kaidi Xu, and Suman Jana; the Workshop on Hyperproperties: Advances in Theory and Practice (HYPER 2021), organized by Daniel Fremont and Hazem Torfah; and the Workshop on Open Problems in Learning and Verification of Neural Networks 2021, organized by Anna Lukina, Guy Avni, Mirco Giacobbe, and Christian Schilling. All three workshops were hosted virtually on October 18, 2021. These workshops brought in additional participants to ATVA 2021 and helped make it an interesting and successful event. We thank all the workshop organizers for their hard work.

ATVA 2021 would not have been successful without the contributions and involvement of the Program Committee members as well as the external reviewers, who contributed to the review process (with more than 225 reviews) and the selection of the best contributions. This event would not exist if authors and contributors did not

submit their proposals. We thank every person, reviewer, author, PC member and organizing committee member involved in the success of ATVA 2021.

The EasyChair system was set up for the management of ATVA 2021 and supported the submission, review, and volume preparation processes. It proved to be a powerful framework.

Although ATVA 2021 was hosted virtually, the local host and sponsor Griffith University provided tremendous help with the registration and online facilities. The other sponsors, Formal Methods Europe, Springer, and Destination Gold Coast, contributed in different forms to help the conference run smoothly. Many thanks to all the local organisers and sponsors.

We wish to express our special thanks to the General Chair and Steering Committee members, particularly Jing Sun, Farn Wang, Jie-Hong Roland Jiang, and Yu-Fang Chen, for their valuable support.

October 2021

Zhe Hou  
Vijay Ganesh

# Organization

## General Co-chairs

Jin Song Dong  
Jing Sun

National University of Singapore, Singapore  
University of Auckland, New Zealand

## Program Co-chairs

Zhe Hou  
Vijay Ganesh

Griffith University, Australia  
University of Waterloo, Canada

## Steering Committee

Teruo Higashino  
Jie-Hong Roland Jiang  
Doron A Peled  
Yu-Fang Chen

Osaka University, Japan  
National Taiwan University, Taiwan  
Bar Ilan University, Israel  
Institute of Information Science, Academia Sinica,  
Taiwan

Ichiro Hasuo  
Yunja Choi

National Institute of Informatics, Japan  
Kyungpook National University, South Korea

## Advisory Committee

Insup Lee  
Allen Emerson  
Hsu-Chun Yen  
Farn Wang

University of Pennsylvania, USA  
The University of Texas at Austin, USA  
National Taiwan University, Taiwan  
National Taiwan University, Taiwan

## Publicity Co-chairs

Giles Reger  
Meng Sun

The University of Manchester, UK  
Peking University, China

## Workshop Co-chairs

Guy Katz  
Rayna Dimitrova

Hebrew University of Jerusalem, Israel  
CISPA Helmholtz Center for Information Security,  
Germany

## Program Committee

|                       |                                                             |
|-----------------------|-------------------------------------------------------------|
| Erika Abraham         | RWTH Aachen University, Germany                             |
| Mohamed Faouzi Atig   | Uppsala University, Sweden                                  |
| Christel Baier        | TU Dresden, Germany                                         |
| Stanley Bak           | Stony Brook University, USA                                 |
| Ezio Bartocci         | Vienna University of Technology, Austria                    |
| Saddek Bensalem       | VERIMAG, France                                             |
| Armin Biere           | Johannes Kepler University Linz, Austria                    |
| Nikolaj Bjorner       | Microsoft, USA                                              |
| Udi Boker             | Interdisciplinary Center (IDC) Herzliya, Israel             |
| Borzoo Bonakdarpour   | Michigan State University, USA                              |
| Luca Bortolussi       | University of Trieste, Italy                                |
| Jalil Boudjadar       | Aarhus University, Denmark                                  |
| Martin Brain          | University of Oxford, UK                                    |
| Franck Cassez         | ConsenSys and Macquarie University, Australia               |
| Supratik Chakraborty  | IIT Bombay, India                                           |
| Krishnendu Chatterjee | Institute of Science and Technology (IST), UK               |
| Yu-Fang Chen          | Academia Sinica, Taiwan                                     |
| Chih-Hong Cheng       | Denso Automotive Deutschland GmbH, Germany                  |
| Alessandro Cimatti    | Fondazione Bruno Kessler, Italy                             |
| Hung Dang Van         | Vietnam National University, Vietnam                        |
| Tien V. Do            | Budapest University of Technology and Economics,<br>Hungary |
| Alexandre Duret-Lutz  | LRDE, EPITA, France                                         |
| Javier Esparza        | Technical University of Munich, Germany                     |
| Bernd Finkbeiner      | CISPA Helmholtz Center for Information Security,<br>Germany |
| Pascal Fontaine       | Université de Liège, Belgium                                |
| Martin Fränzle        | Carl von Ossietzky Universität Oldenburg, Germany           |
| Pierre Ganty          | IMDEA Software Institute, Spain                             |
| Alberto Griggio       | Fondazione Bruno Kessler, Italy                             |
| Dimitar Guelev        | Bulgarian Academy of Sciences, Bulgaria                     |
| Keijo Heljanko        | University of Helsinki, Finland                             |
| Guy Katz              | The Hebrew University of Jerusalem, Israel                  |
| Siau-Cheng Khoo       | National University of Singapore, Singapore                 |
| Xuandong Li           | Nanjing University, China                                   |
| Anthony Widjaja Lin   | TU Kaiserslautern, Germany                                  |
| Alexander Nadel       | Intel, Israel                                               |
| Pham Ngoc Hung        | Vietnam National University, Vietnam                        |
| Aina Niemetz          | Stanford University, USA                                    |
| Tobias Nipkow         | Technical University of Munich, Germany                     |
| Doron Peled           | Bar Ilan University, Israel                                 |
| Mathias Preiner       | Stanford University, USA                                    |



|                      |                                                                        |
|----------------------|------------------------------------------------------------------------|
| Markus Rabe          | Google, USA                                                            |
| Andrew Reynolds      | University of Iowa, USA                                                |
| Olli Saarikivi       | Aalto University, Finland                                              |
| Indranil Saha        | Indian Institute of Technology Kanpur, India                           |
| Sven Schewe          | University of Liverpool, UK                                            |
| Anne-Kathrin Schmuck | Max-Planck-Institute for Software Systems, Germany                     |
| Daniel Selsam        | Microsoft Research, USA                                                |
| Gagandeep Singh      | VMWare Research and University of Illinois<br>at Urbana-Champaign, USA |
| Sadegh Soudjani      | Newcastle University, UK                                               |
| Jun Sun              | Singapore Management University, Singapore                             |
| Sofiene Tahar        | Concordia University, Canada                                           |
| Michael Tautschnig   | Queen Mary University of London, UK                                    |
| Tachio Terauchi      | Waseda University, Japan                                               |
| Aditya Thakur        | University of California, Davis, USA                                   |
| Cesare Tinelli       | University of Iowa, USA                                                |
| Hoang Truong         | Vietname National University, Vietname                                 |
| Bow-Yaw Wang         | Academia Sinica, Taiwan                                                |
| Zhilin Wu            | Chinese Academy of Sciences, China                                     |

# Geometric Theory for Program Testing

## (Abstract of a Keynote Talk)

Bernhard Möller<sup>1</sup>, Tony Hoare<sup>2</sup> and Zhe Hou<sup>3</sup>

<sup>1</sup> Universität Augsburg

<sup>2</sup> University of Cambridge and Honorary Member of Griffith University

<sup>3</sup> Griffith University

**Abstract.** Formal methods for verification of programs are extended to testing of programs. Their combination is intended to lead to benefits in reliable program development, testing, and evolution. Our geometric theory of testing is intended to serve as the specification of a testing environment, included as the last stage of a toolchain that assists professional programmers, amateurs, and students of Computer Science. The testing environment includes an automated algorithm which locates errors in a test that has been run, and assists in correcting them. It does this by displaying, on a monitor screen, a stick diagram of causal chains in the execution of the program under test. The diagram can then be navigated backwards in the familiar style of a satnav following roads on a map. This will reveal selections of places at which the program should be modified to remove the error.

## Summary

The relevant formal methods for testing are due to the pioneers who provided the ideas: Euclid and Descartes for geometry; Carl Adam Petri, whose nets model execution of programs; Noam Chomsky, whose structured method defines the syntax of many programming languages. Their pioneering theories are simplified and adapted to meet current needs of programmers.

A Euclidean diagram is formed by executing a set of constructors, whose feasibility is postulated by axioms and definitions. The geometric features of the diagram (axes, coordinates, points, lines, figures, ...) are labelled by identifiers chosen in drawing the diagram. These identifiers relate the diagram to the proof of a Euclidean proposition, or the text of a program under test.

As an example, we take a structured programming language, with program executions represented by Chomsky's Abstract Syntax Trees. A multiple simultaneous assignment labels the leaves of the tree with atomic commands, and constructors label the branching points. Operators are sequential composition, object class declaration, and concurrent composition of various kinds. Individual operations of the language are defined by specifying the properties of a correct interface between their operands. Errors in arithmetic expressions can be detected by labelling a tree by the value that it produces. Detection of zero divide is then just a matter of calculation. Other errors (eg. deadlock) can be defined by defining a pattern (eg. a cyclic chain of arrows).

This makes it easy to define a new language feature separately by a new constructor. A new language can be defined as the union of its features. A testing tool should be automatically extensible to deal with any combination of features.

# Contents

## Invited Paper

|                                                                  |   |
|------------------------------------------------------------------|---|
| Linear Temporal Logic – From Infinite to Finite Horizon. . . . . | 3 |
| <i>Lucas M. Tabajara and Moshe Y. Vardi</i>                      |   |

## Automata Theory

|                                                                                  |    |
|----------------------------------------------------------------------------------|----|
| Determinization and Limit-Determinization of Emerson-Lei Automata . . . . .      | 15 |
| <i>Tobias John, Simon Jantsch, Christel Baier, and Sascha Klüppelholz</i>        |    |
| Automatic Discovery of Fair Paths in Infinite-State Transition Systems . . . . . | 32 |
| <i>Alessandro Cimatti, Alberto Griggio, and Enrico Magnago</i>                   |    |
| Certifying DFA Bounds for Recognition and Separation . . . . .                   | 48 |
| <i>Orna Kupferman, Nir Lavee, and Salomon Sickert</i>                            |    |

## Machine Learning for Formal Methods

|                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------|----|
| AALpy: An Active Automata Learning Library . . . . .                                                | 67 |
| <i>Edi Muškardin, Bernhard K. Aichernig, Ingo Pill, Andrea Pferscher, and Martin Tappler</i>        |    |
| Learning Linear Temporal Properties from Noisy Data:<br>A MaxSAT-Based Approach . . . . .           | 74 |
| <i>Jean-Raphaël Gaglione, Daniel Neider, Rajarshi Roy, Ufuk Topcu, and Zhe Xu</i>                   |    |
| Mining Interpretable Spatio-Temporal Logic Properties for Spatially<br>Distributed Systems. . . . . | 91 |
| <i>Sara Mohammadinejad, Jyotirmoy V. Deshmukh, and Laura Nenzi</i>                                  |    |

## Theorem Proving and Tools

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| A Formal Semantics of the GraalVM Intermediate Representation. . . . . | 111 |
| <i>Brae J. Webb, Mark Utting, and Ian J. Hayes</i>                     |     |
| A Verified Decision Procedure for Orders in Isabelle/HOL. . . . .      | 127 |
| <i>Lukas Stevens and Tobias Nipkow</i>                                 |     |
| PJBDD: A BDD Library for Java and Multi-Threading . . . . .            | 144 |
| <i>Dirk Beyer, Karlheinz Friedberger, and Stephan Holzner</i>          |     |

## Model Checking

|                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------|-----|
| Live Synthesis . . . . .                                                                                         | 153 |
| <i>Bernd Finkbeiner, Felix Klein, and Niklas Metzger</i>                                                         |     |
| Faster Pushdown Reachability Analysis with Applications<br>in Network Verification . . . . .                     | 170 |
| <i>Peter Gjør Jensen, Stefan Schmid, Morten Konggaard Schou, Jiří Srba,<br/>Juan Vanerio, and Ingo van Duijn</i> |     |
| Verifying Verified Code. . . . .                                                                                 | 187 |
| <i>Siddharth Priya, Xiang Zhou, Yusen Su, Yakir Vizel, Yuyan Bao,<br/>and Arie Gurfinkel</i>                     |     |

## Probabilistic Analysis

|                                                                                                      |     |
|------------------------------------------------------------------------------------------------------|-----|
| Probabilistic Causes in Markov Chains . . . . .                                                      | 205 |
| <i>Christel Baier, Florian Funke, Simon Jantsch, Jakob Piribauer,<br/>and Robin Ziemek</i>           |     |
| TEMPEST - Synthesis Tool for Reactive Systems and Shields<br>in Probabilistic Environments . . . . . | 222 |
| <i>Stefan Pranger, Bettina Könighofer, Lukas Posch, and Roderick Bloem</i>                           |     |
| AQUA: Automated Quantized Inference for Probabilistic Programs. . . . .                              | 229 |
| <i>Zixin Huang, Saikat Dutta, and Sasa Misailovic</i>                                                |     |

## Software and Hardware Verification

|                                                                                                 |     |
|-------------------------------------------------------------------------------------------------|-----|
| Proving SIFA Protection of Masked Redundant Circuits . . . . .                                  | 249 |
| <i>Vedad Hadžić, Robert Primas, and Roderick Bloem</i>                                          |     |
| Verification by Gambling on Program Slices . . . . .                                            | 266 |
| <i>Murad Akhundov, Federico Mora, Nick Feng, Vincent Hui,<br/>and Marsha Chechik</i>            |     |
| Runtime Enforcement of Hyperproperties. . . . .                                                 | 283 |
| <i>Norine Coenen, Bernd Finkbeiner, Christopher Hahn, Jana Hofmann,<br/>and Yannick Schillo</i> |     |

## System Synthesis and Approximation

|                                                     |     |
|-----------------------------------------------------|-----|
| Compositional Synthesis of Modular Systems. . . . . | 303 |
| <i>Bernd Finkbeiner and Noemi Passing</i>           |     |

|                                                                                                                                                                  |     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Event-B Refinement for Continuous Behaviours Approximation . . . . .                                                                                             | 320 |
| <i>Guillaume Dupont, Yamine Aït-Ameur, Marc Pantel,<br/>and Neeraj K. Singh</i>                                                                                  |     |
| Incorporating Monitors in Reactive Synthesis Without Paying the Price . . . . .                                                                                  | 337 |
| <i>Shaun Azzopardi, Nir Piterman, and Gerardo Schneider</i>                                                                                                      |     |
| <b>Verification of Machine Learning</b>                                                                                                                          |     |
| pyNeVer: A Framework for Learning and Verification<br>of Neural Networks . . . . .                                                                               | 357 |
| <i>Dario Guidotti, Luca Pulina, and Armando Tacchella</i>                                                                                                        |     |
| Property-Directed Verification and Robustness Certification of Recurrent<br>Neural Networks . . . . .                                                            | 364 |
| <i>Igor Khmel'nitsky, Daniel Neider, Rajarshi Roy, Xuan Xie,<br/>Benoît Barbot, Benedikt Bollig, Alain Finkel, Serge Haddad,<br/>Martin Leucker, and Lina Ye</i> |     |
| <b>Author Index</b> . . . . .                                                                                                                                    | 381 |