

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 series at <http://www.springer.com/series/7408>

Dang Van Hung · Oleg Sokolsky (Eds.)

Automated Technology for Verification and Analysis

18th International Symposium, ATVA 2020
Hanoi, Vietnam, October 19–23, 2020
Proceedings

Editors

Dang Van Hung
Vietnam National University (VNU-UET)
Hanoi, Vietnam

Oleg Sokolsky
University of Pennsylvania
Philadelphia, PA, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-59151-9

ISBN 978-3-030-59152-6 (eBook)

<https://doi.org/10.1007/978-3-030-59152-6>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2020

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 18th International Symposium on Automated Technology for Verification and Analysis (ATVA 2020) held in Hanoi, Vietnam, during October 19–23, 2020.

The ATVA series of symposia is dedicated to promoting research in theoretical and practical aspects of automated analysis, verification, and synthesis by providing an international venue for the researchers to present new results. At the same time, they provide a forum for interaction between the regional and international research communities and industry in the field.

ATVA 2020 received 75 full paper submissions coauthored by researchers from 29 countries. Each submission was reviewed by at least three Program Committee (PC) members with the help from reviewers outside the PC. After 10 days of online discussions, the committee decided to accept 32 papers for presentation at the conference.

We would like to express our gratitude to all the researchers who submitted their work to the symposium. We are particularly thankful to all colleagues who served on the PC, as well as the external reviewers, whose hard work in the review process helped us prepare the conference program. The international diversity of the PC as well as external reviewers is noteworthy as well: PC members and external reviewers have affiliations with institutes in 20 countries.

Special thanks go to the three invited speakers – Tobias Nipkow, from TU Munich, Germany; Klaus Havelund, from CalTech and NASA JPL, USA; and David Dill, from Stanford University, USA. The papers of the two first invited talks are included in this volume.

A number of colleagues have worked very hard to make this conference a success. We wish to express our thanks to the Local Organizing Committee: Hung Pham Ngoc, Hieu Vo Dinh, and many student volunteers. We would also like to thank the University of Engineering and Technology of the Vietnam National University, Hanoi, Vietnam, the host of the conference, who provided various support and facilities for organizing the conference and its tutorials. Finally, we are thankful for the institutional and financial support from Vingroup Innovation Foundation (VINIF) and Toshiba Software Development in Vietnam (TSDV).

The conference program was prepared with the help of EasyChair. We thank Springer for continuing to publish the conference proceedings.

October 2020

Dang Van Hung
Oleg Sokolsky

Doron Peled	Bar-Ilan University, Israel
Do Van Tien	Budapest University of Technology and Economics, Hungary
Dimitar Guelev	Bulgarian Academy of Sciences, Bulgaria
Bernd Finkbeiner	Saarland University, Germany
Keijo Heljanko	University of Helsinki, Finland
Krishnendu Chatterjee	Institute of Science and Technology (IST), Austria
Sven Schewe	The University of Liverpool, UK
Franck Cassez	Macquarie University, Australia
Jun Sun	Singapore University of Technology and Design, Singapore
Lu Feng	University of Virginia, USA
Hakjoo Oh	Korea University, South Korea
Udi Boker	Interdisciplinary Center (IDC) Herzliya, Israel
Luca Bortolussi	University of Trieste, Italy
Michael Tautschnig	Queen Mary University of London, UK
Bow-Yaw Wang	Academia Sinica, Taiwan
Lijun Zhang	Institute of Software, Chinese Academy of Sciences, China
Quan Thanh Tho	Ho Chi Minh University of Technology, Vietnam
David Lo	SMU, Singapore
Swen Jacobs	CISPA Helmholtz Center for Information Security, Germany
Farn Wang	National Taiwan University, Taiwan
Meenakshi D'Souza	International Institute of Information Technology, India
Vo Dinh Hieu	VNU, Vietnam
Indranil Saha	Indian Institute of Technology Kanpur, India

Additional Reviewers

Andrea Turrini	Etienne Renault
Yong Li	Fathiyeh Faghieh
Malte Schledjewski	Luca Laurenti
Alexander Rabinovich	Lukáš Holík
Lei Bu	Catalin Dima
Carbone	Vijay Ganesh
Tobias Meggendorfer	Yu Wang
Salomon Sickert	Shuling Wang
Maximilian Weininger	Jingyi Wang
Minxue Pan	Roman Rabinovich
Wenchao Yu	Ales Smrcka
Meiyi Ma	Yun-Sheng Chang
Ennio Visconti	Mouhammad Sakr
Meiyi Ma	Mikhail Raskin
Shibashis Guha	Linzhang Wang

Norine Coenen
Christoph Haase
Mouhammad Sakr
Adrien Pommellet
Niklas Metzger
Jianhua Zhao
Song Gao
Francesca Cairolì
Wei-Lun Tsai
Taolue Chen
Tony Sloane
Tzu-Chi Lin

Lei Bu
Tobias Meggendorfer
Andrea Turrini
Jesko Hecking-Harbusch
Yong Li
Vojtěch Havlena
Peter Habermehl
Philipp J. Meyer
Mikhail Raskin
Laurent Doyen
A. R. Balasubramanian
Hongfei Fu

Sponsoring Institutions

Vingroup Innovation Foundation (VINIF)
Toshiba Software Development in Vietnam (TSDV)

Contents

Invited Papers

First-Order Timed Runtime Verification Using BDDs	3
<i>Klaus Havelund and Doron Peled</i>	
Verified Textbook Algorithms	25
<i>Tobias Nipkow, Manuel Eberl, and Maximilian P. L. Haslbeck</i>	

Neural Networks and Machine Learning

Verifying Recurrent Neural Networks Using Invariant Inference	57
<i>Yuval Jacoby, Clark Barrett, and Guy Katz</i>	
NeuralExplorer: State Space Exploration of Closed Loop Control Systems Using Neural Networks	75
<i>Manish Goyal and Parasara Sridhar Duggirala</i>	
DeepAbstract: Neural Network Abstraction for Accelerating Verification	92
<i>Pranav Ashok, Vahid Hashemi, Jan Křetínský, and Stefanie Mohr</i>	
Faithful and Effective Reward Schemes for Model-Free Reinforcement Learning of Omega-Regular Objectives	108
<i>Ernst Moritz Hahn, Mateo Perez, Sven Schewe, Fabio Somenzi, Ashutosh Trivedi, and Dominik Wojtczak</i>	

Automata

Practical “Paritizing” of Emerson-Lei Automata	127
<i>Florian Renkin, Alexandre Duret-Lutz, and Adrien Pommellet</i>	
Complexity of Verification and Synthesis of Threshold Automata	144
<i>A. R. Balasubramanian, Javier Esparza, and Marijana Lazić</i>	
On (I/O)-Aware Good-For-Games Automata.	161
<i>Rachel Faran and Orna Kupferman</i>	
Urgent Partial Order Reduction for Extended Timed Automata	179
<i>Kim G. Larsen, Marius Mikučionis, Marco Muñiz, and Jiří Srba</i>	
Eliminating Message Counters in Threshold Automata.	196
<i>Ilina Stoilkovska, Igor Konnov, Josef Widder, and Florian Zuleger</i>	

Logics

Context-Aware Temporal Logic for Probabilistic Systems	215
<i>Mahmoud Elfar, Yu Wang, and Miroslav Pajic</i>	
Multi-head Monitoring of Metric Dynamic Logic	233
<i>Martin Raszyk, David Basin, and Dmitriy Traytel</i>	

Techniques for Verification, Analysis and Testing

Faster Algorithms for Quantitative Analysis of MCs and MDPs with Small Treewidth	253
<i>Ali Asadi, Krishnendu Chatterjee, Amir Kafshdar Goharshady, Kiarash Mohammadi, and Andreas Pavlogiannis</i>	
Robustness Verification for Classifier Ensembles	271
<i>Dennis Gross, Nils Jansen, Guillermo A. Pérez, and Stephan Raaijmakers</i>	
Verification of Indefinite-Horizon POMDPs	288
<i>Alexander Bork, Sebastian Junges, Joost-Pieter Katoen, and Tim Quatmann</i>	
Verification of a Generative Separation Kernel	305
<i>Inzemamul Haque, D. D'Souza, P. Habeeb, A. Kundu, and Ganesh Babu</i>	

Model Checking and Decision Procedures

A Decision Procedure for Path Feasibility of String Manipulating Programs with Integer Data Type	325
<i>Taolue Chen, Matthew Hague, Jinlong He, Denghang Hu, Anthony Widjaja Lin, Philipp Rümmer, and Zhilin Wu</i>	
From Checking to Inference: Actual Causality Computations as Optimization Problems.	343
<i>Amjad Ibrahim and Alexander Pretschner</i>	
Boosting Sequential Consistency Checking Using Saturation	360
<i>Rachid Zennou, Mohamed Faouzi Atig, Ranadeep Biswas, Ahmed Bouajjani, Constantin Enea, and Mohammed Erradi</i>	
Parallel Graph-Based Stateless Model Checking	377
<i>Magnus Lång and Konstantinos Sagonas</i>	

Model Checking Branching Properties on Petri Nets with Transits	394
<i>Bernd Finkbeiner, Manuel Giesekeing, Jesko Hecking-Harbusch, and Ernst-Rüdiger Olderog</i>	

Synthesis

Explainable Reactive Synthesis	413
<i>Tom Baumeister, Bernd Finkbeiner, and Hazem Torfah</i>	
Robust Controller Synthesis for Duration Calculus	429
<i>Kalyani Dole, Ashutosh Gupta, and Shankara Narayanan Krishna</i>	
Dependency-Based Compositional Synthesis.	447
<i>Bernd Finkbeiner and Noemi Passing</i>	

Randomization and Probabilistic Systems

Proving Non-inclusion of Büchi Automata Based on Monte Carlo Sampling.	467
<i>Yong Li, Andrea Turrini, Xuechao Sun, and Lijun Zhang</i>	
Probabilistic Hyperproperties of Markov Decision Processes.	484
<i>Rayna Dimitrova, Bernd Finkbeiner, and Hazem Torfah</i>	
Minimal Witnesses for Probabilistic Timed Automata	501
<i>Simon Jantsch, Florian Funke, and Christel Baier</i>	
Probabilistic Hyperproperties with Nondeterminism.	518
<i>Erika Abraham, Ezio Bartocci, Borzoo Bonakdarpour, and Oyendrila Dobe</i>	

Tool Papers

ReachNN*: A Tool for Reachability Analysis of Neural-Network Controlled Systems	537
<i>Jiameng Fan, Chao Huang, Xin Chen, Wenchao Li, and Qi Zhu</i>	
RVX - A Tool for Concolic Testing of Embedded Binaries Targeting RISC-V Platforms.	543
<i>Vladimir Herdt, Daniel Große, and Rolf Drechsler</i>	
Peregrine 2.0: Explaining Correctness of Population Protocols Through Stage Graphs	550
<i>Javier Esparza, Martin Helfrich, Stefan Jaax, and Philipp J. Meyer</i>	

DG: Analysis and Slicing of LLVM Bitcode 557
 Marek Chalupa

RTAMT: Online Robustness Monitors from STL 564
 Dejan Ničković and Tomoya Yamaguchi

Author Index 573