

**Yamine Aït-Ameur
Florin Crăciun (Eds.)**

LNCS 13299

Theoretical Aspects of Software Engineering

**16th International Symposium, TASE 2022
Cluj-Napoca, Romania, July 8–10, 2022
Proceedings**



Springer

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

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>


Yamine Aït-Ameur · Florin Crăciun (Eds.)

Theoretical Aspects of Software Engineering

16th International Symposium, TASE 2022
Cluj-Napoca, Romania, July 8–10, 2022
Proceedings

 Springer

Editors

Yamine Ait-Ameur 
IRIT
Toulouse, France

Florin Crăciun 
Babeş-Bolyai University
Cluj-Napoca, Romania

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-10362-9

ISBN 978-3-031-10363-6 (eBook)

<https://doi.org/10.1007/978-3-031-10363-6>

© 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

The International Symposium on Theoretical Aspects of Software Engineering (TASE) gathers researchers and practitioners interested by the new results on innovative advances in software engineering. It records the latest developments in formal and theoretical software engineering methods and techniques.

The 16th edition of TASE was held in the beautiful city of Cluj-Napoca in Romania during July 8–10, 2022. TASE 2022 received 71 submissions covering different areas of theoretical software engineering. Each paper was reviewed by at least three reviewers and the Program Committee accepted 21 long papers and five short papers leading to an attractive scientific program.

This edition of TASE was enhanced by the presence of four keynote speakers. The first talk, given by Erika Àbrahàm from RWTH Aachen University in Germany, entitled “SMT Solving: Historical Roots, Recent Developments and Future Directions” dealt with SMT-based formal verification techniques and provided a technical view on the progress in SMT solving. In the second talk entitled “Practical Theory of Computation on Structures”, Klaus-Dieter Schewe, from the ZJU-UIUC Institute in China, sketched a theory of computation centered around the notion of algorithmic systems. The two other talks dealt with formal software engineering and artificial intelligence. The talk of Sun Jun, from the Singapore Management University in Singapore, entitled “Neural Network Discrimination: Evaluation, Mitigation and Certification” addressed certification of fairness of neural networks using formal verification techniques. The last talk entitled “Rigorous system design for AI software” given by Saddek Bensalem, from Verimag at the University of Grenoble Alpes in France, presented the results of the FOCETA European project in rigorous verification and validation of critical systems.

TASE 2022 would not have succeeded without the deep investment and involvement of the Program Committee members and the external reviewers who evaluated (with more than 215 reviews) and selected the best contributions. This event would not exist without the authors and contributors who submitted their proposals. We address our thanks to everyone—reviewers, authors, Program Committee members, and organization committee members—involved in the success of TASE 2022.

The EasyChair system was set up for the management of TASE 2022, supporting submission, review, and volume preparation processes. It proved to be a powerful framework.

TASE 2022 had one affiliated workshop, the International Workshop on Formal Engineering of Cyber-Physical Systems, which brought additional participants to the symposium and helped make it an interesting and successful event. We thank all the workshop chairs, organizers, and authors for their hard work on this.

TASE 2022 was hosted and sponsored by Babeş-Bolyai University, Cluj-Napoca, Romania. The local organization committee offered all the facilities to run the event in a lovely and friendly atmosphere. Many thanks to all the local organizers.

Lastly, we wish to express our special thanks to the steering committee members, in particular Shengchao Qin and Huibiao Zhu, for their valuable support.

July 2022

Yamine Aït-Ameur
Florin Crăciun

Organization

Program Committee

Erika Abraham	RWTH Aachen University, Germany
Yamine Ait Ameur (Chair)	IRIT, INPT-ENSEEIH, France
Étienne André	Loria, Université de Lorraine, France
Toshiaki Aoki	JAIST, Japan
Christian Attiogbe	LS2N, Université de Nantes, France
Guangdong Bai	University of Queensland, Australia
Richard Banach	University of Manchester, UK
Luís Soares Barbosa	University of Minho, Portugal
Marcello Bonsangue	Leiden University, The Netherlands
Marius Bozga	Verimag, Université Grenoble Alpes, France
Liqian Chen	National University of Defense Technology, China
Wei-Ngan Chin	National University of Singapore, Singapore
Horatiu Cirstea	Loria, France
Florin Craciun (Chair)	Babeş-Bolyai University, Romania
Guillaume Dupont	Institut de Recherche en Informatique de Toulouse, France
Flavio Ferrarotti	Software Competence Centre Hagenberg, Austria
Simon Foster	University of York, UK
Marc Frappier	Université de Sherbrooke, Canada
Radu Grosu	Stony Brook University, USA
Kim Guldstrand Larsen	Aalborg University, Denmark
Thai Son Hoang	University of Southampton, UK
Zoltán Horváth	Eotvos Lorand University, Budapest
Zhe Hou	Griffith University, Australia
Fuyuki Ishikawa	National Institute of Informatics, Japan
Andreas Katis	KBR Inc., NASA Ames Research Center, USA
Olga Kouchnarenko	University of Franche-Comté, France
Regine Laleau	Paris-East Créteil University, France
Guoqiang Li	Shanghai Jiao Tong University, China
Qin Li	East China Normal University, China
Dorel Lucanu	Alexandru Ioan Cuza University, Romania
Frederic Mallet	Université Nice Sophia-Antipolis, France
Amel Mammar	Telecom SudParis, France
Dominique Mery	Loria, Université de Lorraine, France
Simona Motogna	Babeş-Bolyai University, Romania

Kazuhiro Ogata	JAIST, Japan
Jun Pang	University of Luxembourg, Luxembourg
Shengchao Qin	Teesside University, UK
Adrian Riesco	Universidad Complutense de Madrid, Spain
Cristina Seceleanu	Mälardalen University, Sweden
Neeraj Singh	IRIT, INPT-ENSEEIH, University of Toulouse, France
Meng Sun	Peking University, China
Rob van Glabbeek	Data61, CSIRO, Australia
Naijun Zhan	Institute of Software, Chinese Academy of Sciences, China
Huibiao Zhu	East China Normal University, China
Xue-Yang Zhu	Institute of Software, Chinese Academy of Sciences, China

Additional Reviewers

An, Jie	Liu, Zengyu
Ardourel, Gilles	Marinho, Dylan
Chen, Mingshuai	Masson, Pierre-Alain
Cheng, Zheng	McClurg, Jedidiah
Chouali, Samir	Merz, Stephan
Dubois, Catherine	Nguyen, Thuy
Ehrlinger, Lisa	Pardillo Laursen, Christian
Enoiu, Eduard Paul	Pintér, Balázs
Fan, Guangsheng	Seceleanu, Tiberiu
Fehnker, Ansgar	Shi, Ling
Gervais, Frédéric	Sochor, Hannes
Gibson, J. Paul	Sun, Weidi
Guo, Xiaoyun	Tejfel, Máté
Guok, Ernest	Tomita, Takashi
Hajder, Levente	Truscan, Dragos
Halder, Raju	Wang, Shuling
He, Mengda	Wen, Cheng
Ishii, Daisuke	Xue, Bai
Jérôme, Rocheteau	Yan, Fang
Kobayashi, Tsutomu	Zhan, Bohua
Kölbl, Martin	Zhang, Haitao
Ligeti, Peter	Zhang, Miaomiao
Lin, Bo	Zhao, Ying
Lin, Shang-Wei	Zhao, Yongxin
Liu, Ai	

Keynotes

Neural Network Discrimination: Evaluation, Mitigation and Certification

Jun Sun

Singapore Management University

Abstract. In recent years, neural network based machine learning has found its way into various aspects of people's daily life, such as face recognition, personal credit rating, and medical diagnose. One desirable property of neural networks for applications with societal impact is fairness. Since there are often societal biases in the training data, the resultant neural networks might be discriminative as well. Recently, there have been multiple attempts on improving fairness of neural networks, with a focus on fairness testing.

In this line of research, we develop a series of approaches and associated software tool-kits to evaluate a given neural network's fairness by systematically generating discriminatory instance (published at ICSE'20), to mitigate discrimination in the neural network by fining tuning a small number of guilty neurons (published at ICSE'22), and to certify the neural network's fairness through formal verification (published at FM'21). We demonstrate that with our approaches are both effective and efficiency using real-world applications.

SMT Solving: Historical Roots, Recent Developments and Future Directions

Erika Ábrahám

RWTH Aachen University, Germany

The development of decision procedures for checking the satisfiability of logical formulas has a long history in mathematical logic and symbolic computation. Besides theoretical interest, their automation in the 60's raised their practical importance and increased the intensity of research in this area. Besides computer algebra systems on the mathematical side, in the 90's another line of developments has been initiated in computer science. Unified under the name *satisfiability checking*, powerful SAT and SAT-modulo-theories (SMT) solvers have been developed that are nowadays at the heart of many techniques for the synthesis and analysis of software and hardware systems with probabilistic, timed, discrete, dynamical or discrete-continuous components, and in general for all types of large combinatorial problems like complex planning and scheduling tasks.

In this talk we give a historical overview of this development, describe our own solver SMT-RAT, discuss some fascinating new developments for checking the satisfiability of real-arithmetic formulas, and conclude with some challenges for potential future research directions.

Rigorous System Design for AI Software

Saddek Bensalem

University Grenoble Alpes, VERIMAG, Grenoble, France
Saddek.Bensalem@univ-grenoble-alpes.fr

Abstract. The convergence of scientific and technological developments in computing and networking with the physical side and Artificial Intelligence (AI) will impact the forthcoming period concerning several system aspects and disciplines. Learning-enabled Systems represent an example of that convergence, which embraces engineering and technological products. The learning-enabled system technologies are expected to bring large-scale improvements through new products and services across various applications ranging from healthcare to logistics through manufacturing, transport, and more. Software is inarguably the enabling factor for realizing such systems. Unfortunately, we still encounter deployment limitations in the safety-critical application (transportation, healthcare, etc.) due to a lack of trust, behavioral uncertainty, and technology compatibility with safe and secure system development methods. I will first provide an overview of the project FOCETA1 (FOundations for Continuous Engineering of Trustworthy Autonomy) and discuss its strategic goal and its challenges. In the second part of my talk, I will present the problem of the verification and validation methods considered in the project and discuss future research directions.

Contents

Practical Theory of Computation on Structures	1
<i>Klaus-Dieter Schewe</i>	
Complexity of Distributed Petri Net Synthesis	15
<i>Raymond Devillers and Ronny Tredup</i>	
Repairing Adversarial Texts Through Perturbation	29
<i>Guoliang Dong, Jingyi Wang, Jun Sun, Sudipta Chattopadhyay, Xinyu Wang, Ting Dai, Jie Shi, and Jin Song Dong</i>	
Formal Verification of a Keystore	49
<i>Jaap Boender and Goran Bavec</i>	
A Case Study in the Automated Translation of BSV Hardware to PVS Formal Logic with Subsequent Verification	65
<i>Nicholas Moore and Mark Lawford</i>	
Sound Static Analysis of Regular Expressions for Vulnerabilities to Denial of Service Attacks	73
<i>Francesco Parolini and Antoine Miné</i>	
On Verification of Smart Contracts via Model Checking	92
<i>Yulong Bao, Xue-Yang Zhu, Wenhui Zhang, Wuwei Shen, Pengfei Sun, and Yingqi Zhao</i>	
Equivalence of Denotational and Operational Semantics for Interaction Languages	113
<i>Erwan Mahe, Christophe Gaston, and Pascale Le Gall</i>	
Automatic Classification of Bug Reports Based on Multiple Text Information and Reports' Intention	131
<i>Fanqi Meng, Xuesong Wang, Jingdong Wang, and Peifang Wang</i>	
Collaborative Verification of Uninterpreted Programs	148
<i>Yide Du, Weijiang Hong, Zhenbang Chen, and Ji Wang</i>	
MSDetector: A Static PHP Webshell Detection System Based on Deep-Learning	155
<i>Baijun Cheng, Yanhui Guo, Yan Ren, Gang Yang, and Guosheng Xu</i>	

Extending Process Algebra with an Undefined Action	173
<i>S. Arun-Kumar</i>	
Machine-Assisted Proofs for Institutions in Coq	180
<i>Conor Reynolds and Rosemary Monahan</i>	
Optimizing Trans-Compilers in Runtime Verification Makes Sense – Sometimes	197
<i>Hannes Kallwies, Martin Leucker, Meiko Prilop, and Malte Schmitz</i>	
Testing Vehicle-Mounted Systems: A Stepwise Symbolic Execution Approach for OSEK/VDX Programs	205
<i>Haitao Zhang and Bowen Pu</i>	
Dynamic Specification Mining Based on Transformer	220
<i>Ying Gao, Meng Wang, and Bin Yu</i>	
Dynamic Environment Simulation for Database Performance Evaluation	238
<i>Chunxi Zhang, Rong Zhang, and Kai Liu</i>	
Extending SYSML with Refinement and Decomposition Mechanisms to Generate EVENT-B Specifications	256
<i>Racem Bougacha, Régine Laleau, Simon Collart-Dutilleul, and Rahma Ben Ayed</i>	
Development of Monitoring Systems for Anomaly Detection Using ASTD Specifications	274
<i>El Jabri Chaymae, Frappier Marc, Ecarot Thibaud, and Tardif Pierre-Martin</i>	
A Language-Based Causal Model for Safety	290
<i>Marcello Bonsangue, Georgiana Caltais, Hui Feng, and Hüınkar Can Tunç</i>	
Consistency of Heterogeneously Typed Behavioural Models: A Coalgebraic Approach	308
<i>Harald König and Uwe Wolter</i>	
Improving Adversarial Robustness of Deep Neural Networks via Linear Programming	326
<i>Xiaochao Tang, Zhengfeng Yang, Xuanming Fu, Jianlin Wang, and Zhenbing Zeng</i>	
AllSynth: Transiently Correct Network Update Synthesis Accounting for Operator Preferences	344
<i>Kim Guldstrand Larsen, Anders Mariegaard, Stefan Schmid, and Jiří Srba</i>	

End-to-End Heat-Pump Control Using Continuous Time Stochastic Modelling and UPPAAL STRATEGO	363
<i>Imran Riaz Hasrat, Peter Gjøøl Jensen, Kim Guldstrand Larsen, and Jiří Srba</i>	
Security Vulnerabilities Detection Through Assertion-Based Approach	381
<i>Salim Yahia Kissi, Rabéa Ameur-Boulifa, and Yassamin Seladji</i>	
The Complexity of Evaluating Nfer	388
<i>Sean Kauffman and Martin Zimmermann</i>	
Supporting Algorithm Analysis with Symbolic Execution in Alk	406
<i>Alexandru-Ioan Lungu and Dorel Lucanu</i>	
Author Index	425