

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>

Owolabi Legunsen · Grigore Rosu (Eds.)

Model Checking Software

28th International Symposium, SPIN 2022
Virtual Event, May 21, 2022
Proceedings

Editors

Owolabi Legunsen
Cornell University
Ithaca, NY, USA

Grigore Rosu 
University of Illinois Urbana-Champaign
Urbana, IL, USA

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-15076-0

ISBN 978-3-031-15077-7 (eBook)

<https://doi.org/10.1007/978-3-031-15077-7>

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

This volume contains the proceedings of the 28th International Symposium on Model Checking Software, SPIN 2022, held online from Chicago, Illinois, on May 21, 2022. Since 1995, the event has evolved and has been consolidated as a reference symposium in the area of formal methods related to model checking. The previous edition of the SPIN symposium took place in Leiden, the Netherlands, with a record number of submissions and participants.

The SPIN 2022 edition requested regular papers, short papers, and tool demos in the following areas: formal verification techniques for automated analysis of software; formal analysis for modeling languages, such as UML/state charts; formal specification languages, temporal logic, and design-by-contract; model checking and automated theorem proving, including SAT and SMT; verifying compilers; abstraction and symbolic execution techniques; static analysis and abstract interpretation; combination of verification techniques; modular and compositional verification techniques; verification of timed and probabilistic systems; automated testing using advanced analysis techniques; combination of static and dynamic analyses; derivation of specifications, test cases, or other useful material via formal analysis; case studies of interesting systems or with interesting results; engineering and implementation of software verification and analysis tools; benchmark and comparative studies for formal verification and analysis tools; formal methods education and training; and insightful surveys or historical accounts on topics of relevance to the symposium.

The symposium attracted 11 submissions that were each carefully reviewed by three Program Committee (PC) members. The selection process included further online discussion open to all PC members. As a result, eight papers were selected for presentation at the symposium and publication in Springer's proceedings. The program consisted of eight regular papers and two invited talks.

We would like to thank all the authors who submitted papers, the Steering Committee, the PC, the additional reviewers, the invited speakers, the participants, and the organizers of the cohosted events for making SPIN 2022 a successful event. We also thank all the sponsors that provided online facilities and financial support to make the symposium possible.

May 2022

Owolabi Legunsen
Grigore Rosu

Organization

Program Committee Chairs

Owolabi Legunsen
Grigore Rosu

Cornell University, USA
University of Illinois at Urbana-Champaign, USA

Steering Committee

Dragan Bosnacki (Chair)

Susanne Graf
Gerard Holzmann
Stefan Leue
Jaco van de Pol
Neha Rungta
Willem Visser

Eindhoven University of Technology,
The Netherlands

Verimag, France
Nimble Research, USA
University of Konstanz, Germany
Aarhus University, Denmark
Amazon Web Services, USA
Stellenbosch University, South Africa

Program Committee

Axel Legay
Cristina Seceleanu
Doron Peled
Jaco van de Pol
Kyungmin Bae

Stefan Leue
Neeraj Suri
Georgiana Caltais
Madalina Erascu
Richard DeFrancisco
Christian Schilling
Gerard Holzmann
Corina Pasareanu
Sandeep Kulkarni
Klaus Havelund
Alberto Lluch Lfuentes
Andrei Stefanescu
Allison Sullivan

UCLouvain, Belgium
Mälardalen University, Sweden
Bar Ilan University, Israel
Aarhus University, Denmark
Pohang University of Science and Technology,
South Korea
University of Konstanz, Germany
Lancaster University, UK
University of Konstanz, Germany
West University of Timisoara, Romania
Augusta University, USA
Aalborg University, Denmark
Nimble Research, USA
Carnegie Mellon University and NASA, USA
Michigan State University, USA
Jet Propulsion Laboratory, USA
Technical University of Denmark, Denmark
University of Illinois at Urbana-Champaign, USA
University of Texas at Arlington, USA

Kuen-Bang Hou Favnja

Dragan Bosnacki

Liyi Li

University of Minnesota, USA

Eindhoven University of Technology,
The Netherlands

University of Maryland, USA

Local Organization Committee

Neil Zhao

Xiaohong Chen

Maryam Rostamigiv

University of Illinois at Urbana-Champaign, USA

University of Illinois at Urbana-Champaign, USA

TU Dresden, Germany

Additional Reviewers

Fabien Duchene

Martin Kölbl

Tiberiu Seceleanu

Andrew Sogokon

Fabian Bauer-Marquart

Contents

Automated Consistency Analysis for Legal Contracts	1
<i>Alan Khoja, Martin Kölbl, Stefan Leue, and Rüdiger Wilhelm</i>	
Monitoring Cyber-Physical Systems Using a Tiny Twin to Prevent Cyber-Attacks	24
<i>Fereidoun Moradi, Maryam Bagheri, Hanieh Rahmati, Hamed Yazdi, Sara Abbaspour Asadollah, and Marjan Sirjani</i>	
Synthesis of Rigorous Floating-Point Predicates	44
<i>Thanh Son Nguyen, Ben Jones, and Zvonimir Rakamarić</i>	
Statistical Model Checking for Probabilistic Hyperproperties of Real-Valued Signals	61
<i>Shiraj Arora, René Rydhof Hansen, Kim Guldstrand Larsen, Axel Legay, and Danny Bøgsted Poulsen</i>	
SpecRepair: Counter-Example Guided Safety Repair of Deep Neural Networks	79
<i>Fabian Bauer-Marquart, David Boetius, Stefan Leue, and Christian Schilling</i>	
Verifying the SHA-3 Implementation from OpenSSL with the Software Analysis Workbench	97
<i>Parker Hanson, Benjamin Winters, Eric Mercer, and Brett Decker</i>	
Bounded-Memory Runtime Enforcement	114
<i>Saumya Shankar, Antoine Rollet, Srinivas Pinisetty, and Yliès Falcone</i>	
Solving String Theories Involving Regular Membership Predicates Using SAT	134
<i>Mitja Kulczynski, Kevin Lotz, Dirk Nowotka, and Danny Bøgsted Poulsen</i>	
Correction to: Bounded-Memory Runtime Enforcement	C1
<i>Saumya Shankar, Antoine Rollet, Srinivas Pinisetty, and Yliès Falcone</i>	
Author Index	153