

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 <https://link.springer.com/bookseries/7408>

Roderick Bloem · Rayna Dimitrova ·
Chuchu Fan · Natasha Sharygina (Eds.)

Software Verification

13th International Conference, VSTTE 2021
New Haven, CT, USA, October 18–19, 2021
and 14th International Workshop, NSV 2021
Los Angeles, CA, USA, July 18–19, 2021
Revised Selected Papers

Editors

Roderick Bloem
Graz University of Technology
Graz, Austria

Chuchu Fan 
Massachusetts Institute of Technology
Cambridge, MA, USA

Rayna Dimitrova
CISPA
Helmholtz Center for Information Security
Saarbrücken, Germany

Natasha Sharygina
Faculty of Informatics
Università della Svizzera italiana
Lugano, Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-95560-1 ISBN 978-3-030-95561-8 (eBook)
<https://doi.org/10.1007/978-3-030-95561-8>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© 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

VSTTE 2021 Preface

This volume contains the papers presented at the 13th Working Conference on Verified Software: Theories, Tools, and Experiments (VSTTE 2021), held virtually during October 18–19, 2021. The conference was co-located with the 21st Conference on Formal Methods in Computer-Aided Design (FMCAD 2021).

The Verified Software Initiative (VSI), spearheaded by Tony Hoare and Jayadev Misra, is an ambitious research program for making large-scale verified software a practical reality. VSTTE is the main forum for advancing the initiative. VSTTE brings together experts spanning the spectrum of software verification in order to foster international collaboration on the critical research challenges.

There were 17 submissions to VSTTE 2021, with authors from 11 countries. The Program Committee consisted of 23 distinguished computer scientists from all over the world. Each submission was reviewed by three Program Committee members in single-blind mode. In order to obtain domain-specific expertise, we also involved seven external reviewers: Robby Findler, Antti Hyvärinen, Makai Mann, Andres Noetzli, Rodrigo Otoni, Alex Ozdemir, and Daniel Riley. After a comprehensive discussion on the strengths and weaknesses of papers, the committee decided to accept seven papers. The technical program also included two invited talks by Tom Henzinger (IST Austria) and Michael Whalen (Amazon Web Services and University of Minnesota, USA), as well as two invited tutorials (joint with FMCAD) by Matteo Maffei (TU Wien, Austria) and Frits Vaandrager (Institute for Computing and Information Sciences, Radboud University Nijmegen, The Netherlands). We greatly appreciate the help we got from the members of the Formal Verification Lab of the University of Lugano, Switzerland, and in particular from Masoud Asadzadeh for setting up and maintaining the VSTTE website. We are thankful to EasyChair for providing an easy and efficient mechanism for submission of papers and management of reviews.

December 2021

Roderick Bloem
Natasha Sharygina

VSTTE 2021 Organization

General Chair

Natarajan Shankar

SRI International, USA

Program Committee Chairs

Roderick Bloem

Graz University of Technology, Austria

Natasha Sharygina

USI Lugano, Switzerland

Program Committee

Christel Baier

TU Dresden, Germany

Nikolaj Bjørner

Microsoft Research, USA

Roderick Bloem

TU Graz, Austria

Borzoo Bonakdarpour

Michigan State University, USA

Supratik Chakraborty

IIT Bombay, India

Hana Chockler

King's College London, UK

Grigory Fedyukovich

Florida State University, USA

Jean-Christophe Filliâtre

CNRS, France

Bernd Finkbeiner

CISPA Helmholtz Center for Information Security,
Germany

Carlo A. Furia

USI Lugano, Switzerland

Ganesh Gopalakrishnan

University of Utah, USA

Orna Grumberg

Technion, Israel

Swen Jacobs

CISPA Helmholtz Center for Information Security,
Germany

Rajeev Joshi

AWS, USA

Peter Müller

ETH Zurich, Switzerland

Kedar Namjoshi

Bell Labs, USA

Aina Niemetz

Stanford University, USA

Natasha Sharygina

USI Lugano, Switzerland

Sharon Shoham

Tel Aviv University, Israel

Yakir Vizel

Technion, Israel

Chao Wang

University of Southern California, USA

Thomas Wies

NYU, USA

Valentin Wüstholtz

ConsenSys Diligence, Germany

NSV 2021 Preface

This volume contains the contributed papers presented at the 14th International Workshop on Numerical Software Verification (NSV 2021), which was held virtually during July 18–19, 2021. NSV 2021 was co-located with the 33rd International Conference on Computer-Aided Verification (CAV 2021).

Numerical computations are ubiquitous in digital systems: supervision, prediction, simulation, and signal processing rely heavily on numerical calculus to achieve desired goals. Design and verification of numerical algorithms has a unique set of challenges, which set it apart from the rest of software verification. To achieve the verification and validation of global properties, numerical techniques need to precisely represent local behaviors of each component. The implementation of numerical techniques on modern hardware adds another layer of approximation because of the use of finite representations of infinite precision numbers that usually lack basic arithmetic properties, such as commutativity and associativity. Finally, the development and analysis of cyber-physical systems (CPS), which involve interacting continuous and discrete components, pose a further challenge. It is hence imperative to develop logical and mathematical techniques for the reasoning about programmability and reliability. The NSV workshop is dedicated to the development of such techniques.

This edition of NSV had strong emphasis on the challenges of the verification of cyber-physical systems with machine learning components. This topic was featured both in invited presentations and in contributed papers.

A highlight of NSV 2021 was the presence of high-profile invited speakers from computer science and from control theory, who gave the following talks:

- Stanley Bak (Stony Brook University, USA):
“Verifying Neural Networks and Cyber-Physical Systems using Reachability”
- Eva Darulova (Max Planck Institute for Software Systems, Germany):
“Soundly Approximating Numerical Kernels & Beyond”
- Sanjit A. Seshia (University of California, Berkeley, USA):
“Verified AI-Based Autonomy: A Numerical Software Perspective”
- Yu Wang (Duke University, USA):
“Statistical Verification of Hyperproperties for Cyber-Physical Systems”
- Bai Xue (State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China):
“Convex Computations for Reach Sets”

Regarding the contributed papers, NSV 2021 received three submissions, each of which received three or four reviews, and all of the submissions were accepted. We would like to thank the CAV 2021 organizers, in particular, the workshop chair Arie

Gurfinkel, for their support and the organization of the video conferencing and messaging system, and the NSV Steering Committee, in particular Sergiy Bogomolov, for giving us the opportunity to organize NSV 2021.

December 2021

Rayna Dimitrova
Chuchu Fan

NSV 2021 Organization

Program Committee Chairs

Rayna Dimitrova	CISPA Helmholtz Center for Information Security, Germany
Chuchu Fan	Massachusetts Institute of Technology, USA

Steering Committee

Sergiy Bogomolov	Newcastle University, UK
Radu Grosu	TU Vienna, Austria
Matthieu Martel	Université de Perpignan, France
Pavithra Prabhakar	Kansas State University, USA
Sriram Sankaranarayanan	UC Boulder, USA

Program Committee

Houssam Abbas	Oregon State University, USA
Jyotirmoy Deshmukh	University of Southern California, USA
Bruno Dutertre	SRI International, USA
Sicun Gao	University of California, San Diego, USA
Mirco Giacobbe	University of Oxford, UK
Taylor T. Johnson	Vanderbilt University, USA
Soonho Kong	Toyota Research Institute, USA
Laura Nenzi	University of Trieste, Italy
Nicola Paoletti	Royal Holloway, University of London, UK
Yasser Shoukry	University of California, Irvine, USA
Miriam García Soto	IST Austria, Austria
Sadegh Soudjani	Newcastle University, UK
Hoang-Dung Tran	Vanderbilt University, USA
Tichakorn	Iowa State University, USA
(Nok) Wongpiromsarn	
Paolo Zuliani	Newcastle University, UK

Contents

VSTTE 2021

Quantitative Monitoring of Software	3
<i>Thomas A. Henzinger</i>	
Making Proofs of Floating-Point Programs Accessible to Regular Developers	7
<i>Claire Dross and Johannes Kanig</i>	
A Calculus for Multi-language Operational Semantics	25
<i>Matteo Cimini</i>	
Partial Order Reduction for Timed Actors	43
<i>Maryam Bagheri, Marjan Sirjani, Ehsan Khamespanah, Hossein Hojjat, and Ali Movaghar</i>	
Uncertainty-Aware Signal Temporal Logic Inference	61
<i>Nasim Baharisangari, Jean-Raphaël Gaglione, Daniel Neider, Ufuk Topcu, and Zhe Xu</i>	
Designing and Proving Properties of the Abaco Autoscaler Using TLA+	86
<i>Smruti Padhy and Joe Stubbs</i>	
Case Study: Analysis of Autonomous Center Line Tracking Neural Networks	104
<i>Ismet Burak Kadron, Divya Gopinath, Corina S. Păsăreanu, and Huafeng Yu</i>	
Abstract Interpretation of LLVM with a Region-Based Memory Model	122
<i>Arie Gurfinkel and Jorge A. Navas</i>	

NSV 2021

Formal Verification of Neural Network Controllers for Collision-Free Flight.	147
<i>Daniel Genin, Ivan Papusha, Joshua Brulé, Tyler Young, Galen Mullins, Yanni Kouskoulas, Rosa Wu, and Aurora Schmidt</i>	
An Efficient Summation Algorithm for the Accuracy, Convergence and Reproducibility of Parallel Numerical Methods	165
<i>Farah Benmouhoub, Pierre-Loic Garoche, and Matthieu Martel</i>	

Modeling Round-Off Errors in Hydrodynamic Simulations.	182
<i>William Weens, Thibaud Vazquez-Gonzalez,</i> <i>and Louise Ben Salem-Knapp</i>	
Author Index	197