

## 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>

Dirk Beyer · Chantal Keller (Eds.)

# Tests and Proofs

13th International Conference, TAP 2019

Held as Part of the Third World Congress on Formal Methods 2019

Porto, Portugal, October 9–11, 2019

Proceedings

*Editors*

Dirk Beyer   
Ludwig-Maximilians-Universität München  
Munich, Germany

Chantal Keller  
University of Paris-Sud  
Orsay, France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-31156-8              ISBN 978-3-030-31157-5 (eBook)  
<https://doi.org/10.1007/978-3-030-31157-5>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2019

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

Welcome to TAP 2019, the 13th edition of the International Conference on Tests and Proofs. TAP 2019 is part of the Third World Congress on Formal Methods (FM Week 2019). The conference is held in the Alfândega Porto Congress Centre in Porto, Portugal, during October 9–11, 2019.

*Conference Description.* The TAP conference promotes research in verification and formal methods that targets the interplay of proofs and testing: the advancement of techniques of each kind and their combination, with the ultimate goal of improving software and system dependability.

Research in verification has recently seen a steady convergence of heterogeneous techniques and a synergy between the traditionally distinct areas of testing (and dynamic analysis) and of proving (and static analysis). Formal techniques for counter-example generation based on, for example, symbolic execution, SAT/SMT-solving, or model checking, furnish evidence for the potential of a combination of tests and proofs. The combination of predicate abstraction with testing-like techniques based on exhaustive enumeration opens the perspective for novel techniques of proving correctness. On the practical side, testing offers cost-effective debugging techniques of specifications or crucial parts of program proofs (such as invariants). Last but not least, testing is indispensable when it comes to the validation of the underlying assumptions of complex system models involving hardware or system environments. Over the years, there has been a growing acceptance in research communities that testing and proving are complementary rather than mutually exclusive techniques.

TAP’s scope encompasses many aspects of verification technology, including foundational work, tool development, and empirical research. Its topics of interest center around the connection between proofs (and other static techniques) and testing (and other dynamic techniques).

*Focus on Replicability of Research Results.* We consider that reproducibility of results is of the utmost importance for the TAP community. Therefore, we encouraged all authors of accepted papers to submit an artifact for evaluation. For the first time, TAP 2019 included an optional artifact evaluation (AE) process for accepted papers. An artifact is any additional material (software, data sets, machine-checkable proofs, etc.) that substantiates the claims made in a paper and ideally makes them fully replicable. The evaluation and archival of artifacts improves replicability and traceability for the benefit of future research and the broader TAP community.

*Paper Selection.* This year, 19 papers were submitted to TAP. After a rigorous review process, with each paper reviewed by at least three Program Committee (PC) members, followed by an online discussion, 10 papers were accepted by the PC for publication in these proceedings and presentation at the conference.

*Invited Talks.* The conference program and the proceedings also include a keynote by Heike Wehrheim from Paderborn University, Germany, on “Extracting Unverified Program Parts from Software Verification Runs” and an invited tutorial by

Ana Cavalcanti from University of York, UK, on “RoboStar Technology - Testing in Robotics Using Process Algebra.”

*Artifact-Evaluation Process.* For the first time, TAP 2019 used an AE process. The goals of AE are (1) to have more substantial evidence for the claims in the papers, (2) simplify the replication of results in the paper, and (3) reward authors who create artifacts, i.e., any additional material like software, tools, data sets, test suites, and machine-checkable proofs that substantiates the claims made in the paper.

To valorize their papers, authors of accepted papers could submit an artifact for evaluation to the TAP 2019 artifact-evaluation committee (AEC). Artifacts had to be provided as `.zip` files including all necessary software for AE and a `README` file that explains the artifact and guides the user through the replication of the results. AE had to be possible in the TAP 2019 virtual machine, which runs a Ubuntu 19.04 with Linux 5.0.0.

Each artifact was evaluated by four members of the AEC. The AE proceeded in two phases. In the first phase, the reviewers checked if the artifacts were functional, e.g., no corrupted or missing files exist and the evaluation does not crash on simple examples. All submitted artifacts passed the first phase without any problems and we skipped the author clarification phase in which authors could respond to problems in the test-phase evaluation. In the second phase, the assessment phase, the reviewers tried to reproduce any experiments or activities, and evaluated the artifact with respect to the following five questions:

1. Is the artifact consistent with the paper and the claims made by the paper?
2. Are the results of the paper reproducible using the artifact?
3. Is the artifact complete, i.e., how many of the results of the paper are replicable?
4. Is the artifact well-documented?
5. Is the artifact easy to use?

All submitted artifacts also passed this second phase. Corresponding papers were granted the TAP evaluation badge and two additional pages to describe the artifact. Unfortunately, for only one of the ten accepted papers an artifact was submitted. However, this artifact was of very good quality.

*Acknowledgments.* We would like to thank, first of all, the authors who submitted their papers to TAP 2019. The PC and the AEC, who did a great job of reviewing, contributed informed and detailed reports, and took part in the discussions during the virtual PC meeting. Special thanks go to the general chair of the FM Week 2019, José Nuno Oliveira, and his overall organization team, for taking care of the local organization. We also thank Alfred Hofmann and his publication team at Springer for their support.

August 2019

Dirk Beyer  
Chantal Keller  
PC Chairs  
Daniel Dietsch  
Marie-Christine Jakobs  
AEC Chairs

# Organization

## Program Committee

Dirk Beyer (PC Chair)	LMU Munich, Germany
Chantal Keller (PC Chair)	LRI, Université Paris-Sud, France
Bernhard Beckert	KIT, Germany
Marcel Böhme	Monash University, Australia
Achim D. Brucker	University of Exeter, UK
Catherine Dubois	ENSIIE-Samovar, France
Reiner Hähnle	TU Darmstadt, Germany
Klaus Havelund	Jet Propulsion Laboratory, USA
Marieke Huisman	University of Twente, The Netherlands
Marie-Christine Jakobs	TU Darmstadt, Germany
Nikolai Kosmatov	CEA List, France
Laura Kovacs	Vienna University of Technology, Austria
Peter Lammich	TU Munich, Germany
Caroline Lemieux	University of California, Berkeley, USA
Martin Nowack	Imperial College London, UK
Corina S. Păsăreanu	CMU/NASA Ames Research Center, USA
François Pessaux	ENSTA ParisTech, France
Alexander K. Petrenko	ISP RAS, Russia
Michael Tautschnig	Queen Mary University of London, UK
Burkhard Wolff	LRI, Université Paris-Sud, France

## Artifact Evaluation Committee (AEC)

Daniel Dietsch (AEC Chair)	University of Freiburg, Germany
Marie-Christine Jakobs (AEC Chair)	TU Darmstadt, Germany
Martin Bromberger	MPI, Germany
Maryam Dabaghchian	University of Utah, USA
Simon Dierl	TU Dortmund, Germany
Rayna Dimitrova	University of Leicester, UK
Mathias Fleury	MPI, Germany
Marcel Hark	RWTH Aachen, Germany
Martin Jonáš	Masaryk University, Czech Republic
Sven Linker	University of Liverpool, UK
Felipe R. Monteiro	Federal University of Amazonas, Brazil
Marco Muñoz	Aalborg University, Denmark
Gabriel Radanne	University of Freiburg, Germany
Cedric Richter	Paderborn University, Germany
Asieh Salehi Fathabadi	University of Southampton, UK

Christian Schilling IST Austria, Austria  
Martin Tappler TU Graz, Austria

### **Steering Committee**

Bernhardt K. Aichernig TU Graz, Austria  
Jasmin Blanchette Vrije Universiteit Amsterdam, The Netherlands  
Achim D. Brucker University of Sheffield, UK  
Catherine Dubois ENSIIE, France  
Martin Gogolla University of Bremen, Germany  
Nikolai Kosmatov CEA, France  
Burkhard Wolff LRI, France

### **Additional Reviewers**

Richard Bubel  
Michael Forster  
Eduard Kamburjan  
Matthieu Lemerre  
Yakoub Nemouchi  
Thuan Pham  
Alexander Weigl  
Nicky Williams  
Nina Yevtushenko



# Contents

## Invited Contributions

- When Are Software Verification Results Valid for Approximate Hardware? . . . 3  
*Tobias Isenberg, Marie-Christine Jakobs, Felix Pauck,  
and Heike Wehrheim*
- Testing Robots Using CSP . . . . . 21  
*Ana Cavalcanti, James Baxter, Robert M. Hierons, and Raluca Lefticaru*

## Regular Contributions

- Constraints in Dynamic Symbolic Execution: Bitvectors or Integers? . . . . . 41  
*Timotej Kapus, Martin Nowack, and Cristian Cadar*
- Fast, Automatic, and Nearly Complete Structural Unit-Test  
Generation Combining Genetic Algorithms and Formal Methods . . . . . 55  
*Eric Lavillonnière, David Mentré, and Denis Cousineau*
- Coverage-Based Testing with Symbolic Transition Systems . . . . . 64  
*Petra van den Bos and Jan Tretmans*
- BTestBox*: A Tool for Testing B Translators and Coverage of B Models . . . . . 83  
*Diego de Azevedo Oliveira, Valério Medeiros Jr., David Déharbe,  
and Martin A. Musicante*
- Predicting and Testing Latencies with Deep Learning: An IoT Case Study . . . 93  
*Bernhard K. Aichernig, Franz Pernkopf, Richard Schumi,  
and Andreas Wurm*
- Learning Communicating State Machines . . . . . 112  
*Alexandre Petrenko and Florent Avellaneda*
- Repairing Timed Automata Clock Guards through Abstraction and Testing . . . 129  
*Étienne André, Paolo Arcaini, Angelo Gargantini, and Marco Radavelli*
- Proving a Non-blocking Algorithm for Process Renaming with TLA<sup>+</sup> . . . . . 147  
*Aurélie Hurault and Philippe Quéinnec*
- Tame Your Annotations with METACSL: Specifying, Testing  
and Proving High-Level Properties . . . . . 167  
*Virgile Robles, Nikolai Kosmatov, Virgile Prevosto, Louis Rilling,  
and Pascale Le Gall*

**Property-Based Test Case Generators for Free** . . . . . 186  
*Emanuele De Angelis, Fabio Fioravanti, Adrián Palacios,  
Alberto Pettorossi, and Maurizio Proietti*

**Author Index** . . . . . 207