Lecture Notes in Computer Science **10427**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7407

Rupak Majumdar · Viktor Kunčak (Eds.)

Computer Aided Verification

29th International Conference, CAV 2017
Heidelberg, Germany, July 24–28, 2017
Proceedings, Part II

Springer

Editors
Rupak Majumdar
Max Planck Institute for Software Systems
Kaiserslautern, Rheinland-Pfalz
Germany

Viktor Kunčak
School of Computer and Communication Sciences
EPFL - IC - LARA
Lausanne
Switzerland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-63389-3 ISBN 978-3-319-63390-9 (eBook)
DOI 10.1007/978-3-319-63390-9

Library of Congress Control Number: 2017946069

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

It has been our privilege to serve as the program chairs for CAV 2017, the 29th International Conference on Computer-Aided Verification. CAV 2017 was held in beautiful Heidelberg, Germany, during July 22–28, 2017. The pre-conference workshops took place at the Crowne Plaza Hotel in Heidelberg City Centre. The main conference took place at the Stadthalle by the river Neckar.

The CAV conference series is dedicated to the advancement of the theory and practice of computer-aided formal analysis of hardware and software systems. The conference covers the spectrum from theoretical results to concrete applications, with an emphasis on practical verification tools and the algorithms and techniques that are needed for their implementation. CAV considers it vital to continue spurring advances in hardware and software verification while expanding to new domains such as biological systems and computer security.

Out of 191 submissions to the conference, we chose 50 regular papers and seven tool papers. These papers cover a wide range of topics and techniques, from algorithmic and logical foundations of verification to practical applications in distributed, networked, and cyber-physical systems. One direction of topical interest is the increasingly sophisticated combination of "traditional" techniques for reasoning and search with data-driven techniques. The program featured invited talks by Chris Hawblitzel (Microsoft), Marta Kwiatkowska (Oxford), and Viktor Vafeiadis (MPI-SWS), as well as invited tutorials, by Loris D'Antoni and Mayur Naik. As traditional, one of the winners of the CAV award also gave a presentation. We also had a special workshop to celebrate David Dill's many contributions to CAV on the occasion of his 60th birthday.

In addition to the main conference, CAV hosted the Verification Mentoring Workshop for junior scientists entering the field and six pre-conference technical workshops: the Workshop on Synthesis (SYNT), Satisfiability Modulo Theories (SMT), Verified Software: Theories, Tools, and Experiments (VSTTE), Design and Analysis of Robust Systems (DARS), Formal Approaches to Explainable Verification (FEVER), and Numerical Software Verification (NSV).

Organizing a conference is a community effort. The Program Committee for CAV consisted of 56 members; we kept the number large to ensure each PC member would have a reasonable number of papers to review and be able to provide thorough reviews. In addition, we used 104 external reviewers. All together, the reviewers drafted over 730 reviews and put in enormous effort in ensuring a good-quality program.

This year, we made artifact evaluation mandatory for tool submissions and optional but encouraged for regular submissions. We used an artifact evaluation committee of 26 members. Our goal for artifact evaluation was to provide friendly "beta-testing" to tool developers; we recognize that developing a stable tool on a cutting-edge research topic is certainly not easy and we hope the constructive comments provided by the AEC were of help to the developers. Needless to say we were impressed by the quality

of the artifacts and in fact all accepted tools passed artifact evaluation. We are grateful to the reviewers for their outstanding efforts in making sure each paper got a fair chance.

We would like to thank Eva Darulova for chairing the workshop organization process, Barbara Jobstmann and Thomas Wahl for managing sponsorship and student fellowships, respectively, Mikaël Mayer for maintaining the CAV website, and the always helpful Steering Committee members Orna Grumberg, Aarti Gupta, Daniel Kroening, and Kenneth McMillan. We worked closely with Pavithra Prabhakar, Andrey Rybalchenko, and Damien Zufferey, who organized the Verification Mentoring Workshop. Finally, we would like to thank Roslyn Stricker, who helped us tremendously in the administration and organization of CAV.

We hope that you find the proceedings of CAV 2017 thought provoking!

July 2017

Rupak Majumdar
Viktor Kunčak

Organization

Program Chairs

Rupak Majumdar	Max Planck Institute for Software Systems, Germany
Viktor Kunčak	EPFL, Switzerland

Workshop Chair

Eva Darulova	Max Planck Institute for Software Systems, Germany

Sponsorship Chair

Barbara Jobstmann	EPFL, Switzerland and Cadence Design Systems

Fellowship Chair

Thomas Wahl	Northeastern University, USA

Program Committee

Aws Albarghouthi	University of Wisconsin, USA
Christel Baier	TU Dresden, Germany
Per Bjesse	Synopsys, USA
Jasmin Blanchette	Inria Nancy – Grand Est, France
Sergiy Bogomolov	Australian National University, Australia
Ahmed Bouajjani	IRIF, Paris Diderot University, France
Rohit Chadha	University of Missouri, USA
Bor-Yuh Evan Chang	University of Colorado at Boulder, USA
Swarat Chaudhuri	Rice University, USA
Wei-Ngan Chin	National University of Singapore, Singapore
Hana Chockler	King's College London, UK
Alessandro Cimatti	Fondazione Bruno Kessler, Italy
Isil Dilig	University of Texas at Austin, USA
Dino Distefano	Facebook and Queen Mary University of London, UK
Michael Emmi	Nokia Bell Labs, USA
Javier Esparza	TU Munich, Germany
Georgios Fainekos	Arizona State University, USA
Azadeh Farzan	University of Toronto, Canada
Aarti Gupta	Princeton University, USA
Gerard Holzmann	Nimble Research, USA
Marieke Huisman	University of Twente, The Netherlands
Radu Iosif	Verimag, France

Franjo Ivančić	Google, USA
Stefan Kiefer	Oxford University, UK
Zachary Kincaid	Princeton University, USA
Barbara König	University of Duisburg-Essen, Germany
Daniel Kroening	Oxford University, UK
Rustan Leino	Microsoft Research, USA
Kenneth McMillan	Microsoft Research, Redmond, USA
Alexander Nadel	Intel, USA
Madhusudan Parthasarathy	University of Illinois at Urbana Champaign, USA
Corina Pasareanu	NASA Ames and Carnegie Mellon University, USA
Nadia Polikarpova	MIT, USA
Pavithra Prabhakar	Kansas State University, USA
Arjun Radhakrishna	University of Pennsylvania, USA
Zvonimir Rakamaric	University of Utah, USA
Andrey Rybalchenko	Microsoft Research, Cambridge, UK
Roopsha Samanta	Purdue University, USA
Rahul Sharma	Microsoft Research, India
Anna Slobodova	Centaur Technology, USA
Ana Sokolova	University of Salzburg, Austria
Zhendong Su	University of California at Davis, USA
Serdar Tasiran	Amazon Web Services, USA
Emina Torlak	University of Washington, USA
Willem Visser	Stellenbosch University, South Africa
Mahesh Viswanathan	University of Illinois at Urbana Champaign, USA
Yakir Vizel	Princeton University, USA
Tomas Vojnar	Brno University of Technology, Czechia
Thomas Wahl	Northeastern University, USA
Bow-Yaw Wang	Academia Sinica, Taiwan
Georg Weissenbacher	Vienna University of Technology, Austria
Verena Wolf	Saarland University, Germany
Lenore Zuck	University of Illinois at Chicago, USA
Damien Zufferey	Max Planck Institute for Software Systems, Germany

Artifact Evaluation Committee

Ayca Balkan	University of California, Los Angeles, USA
Stephanie Balzer	Carnegie Mellon University, USA
James Bornholt	University of Washington, USA
Simon Cruanes	Inria Nancy, France
Matthias Dangl	University of Passau, Germany
Marko Doko	Max Planck Institute for Software Systems, Germany
Chuchu Fan	University of Illinois, Urbana-Champaign, USA
Pietro Ferrara	Julia Software, Italy
Johannes Hoelzl	TU Munich, Germany
Lars Hupel	TU Munich, Germany

Swen Jacobs	Saarland University, Germany
Moa Johansson	Chalmers, Sweden
Dejan Jovanovic	SRI International, USA
Ralf Jung	Max Planck Institute for Software Systems, Germany
Ivan Kuraj	MIT, USA
Andreas Lochbihler	ETH Zurich, Switzerland
Jose Morales	IMDEA Software, Spain
Van Chan Ngo	Carnegie Mellon University, USA
Zvonimir Pavlinovic	New York University, USA
Markus Rabe	University of California, Berkeley, USA
Mukund Raghothaman	University of Pennsylvania, USA
Andrew Reynolds	University of Iowa, USA
Nima Roohi	University of Illinois, Urbana-Champaign, USA
Christian Schilling	University of Freiburg, Germany
Muralidaran Vijayaraghavan	MIT, USA
Nicolas Voirol	EPFL, Switzerland

Additional Reviewers

Alireza Abyaneh	Constantin Enea	K. Narayan Kumar
Mahmudul Faisal Al Ameen	Chuchu Fan	Sebastian Küpper
Sebastian Arming	Samira Farahani	Axel Legay
Konstantinos Athanasiou	Grigory Fedyukovich	Sorin Lerner
Mohamed Faouzi Atig	Pierre Flener	Peizin Liu
Domagoj Babic	Matthias Fleury	Le Quang Loc
Michael Backenköhler	Wan Fokkink	Andreas Lochbihler
Gogul Balakrishnan	Zhoulai Fu	Alexander Lück
Clark Barrett	Nils Gesbert	Ravichandran Madhavan
Matthew Bauer	Shilpi Goel	Victor Magron
Ryan Beckett	Yijia Gu	Assaf Marron
Harsh Beohar	Arie Gurfinkel	Umang Mathur
Olaf Beyersdorff	Vahid Hashemi	Todd Millstein
Pavol Bielik	Bardh Hoxha	Sergio Mover
Armin Biere	Johannes Hölzl	Suvam Mukherjee
Jesse Bingham	Catalin Hritcu	Daniel Neider
Stefan Blom	Mens Irini-Eleftheria	Dennis Nolte
Stefan Bucur	Himanshu Jain	Peter O'Hearn
Dario Cattaruzza	Chuan Jiang	Wytse Oortwijn
Ed Cerny	George Karpenkov	Gustavo Petri
Le Ton Chanh	Dileep Kini	Lauren Pick
Dmitry Chistikov	Hui Kong	Markus Rabe
Andreea Costea	Aamod Kore	Jaideep Ramachandran
Eva Darulova	Jan Křetínský	Rajarshi Ray
	Thilo Krüger	Andrew Reynolds

Nima Roohi
Philipp Ruemmer
Sarah Sallinger
Anne-Kathrin Schmuck
Peter Schrammel
Daniel Schwartz-Narbonne
Cristina Serban
Alexey Solovyev
Sadegh Soudjani
Benno Stein
Ofer Strichman
Kausik Subramanian
Rob Sumners
Sol Swords
Michael Tautschnig
Nguyen Toan Thanh
Dmitriy Traytel
Nikos Tzevelekos
Viktor Vafeiadis
Freark van der Berg
Jules Villard
Mike Whalen
Christoph Wintersteiger
Xiao Xu
Shakiba Yaghoubi
Eugen Zalinescu
Qirun Zhang
Yiji Zhang
Cai Zhouhong
Florian Zuleger

Steering Committee

Orna Grumberg	Technion, Israel
Aarti Gupta	Princeton University, USA
Daniel Kroening	Oxford University, UK
Kenneth McMillan	Microsoft Research, USA

CAV Award Committee

Tom Ball (Chair)	Microsoft Research, USA
Kim G. Larsen	Aalborg University, Denmark
Natarajan Shankar	SRI International, USA
Pierre Wolper	Liege University, Belgium

Verification Mentoring Workshop

Pavithra Prabhakar	Kansas State University, USA
Andrey Rybalchenko	Microsoft Research, UK
Damien Zufferey	Max Planck Institute for Software Systems, Germany

Publicity Chair

Mikaël Mayer	EPFL, Switzerland

Contents – Part II

Contents – Part I

Data Driven Techniques

Runtime Verification

Cyber-Physical Systems