Editorial Board

David Hutchison
   Lancaster University, Lancaster, UK

Takeo Kanade
   Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
   University of Surrey, Guildford, UK

Jon M. Kleinberg
   Cornell University, Ithaca, NY, USA

Friedemann Mattern
   ETH Zurich, Zurich, Switzerland

John C. Mitchell
   Stanford University, Stanford, CA, USA

Moni Naor
   Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan
   Indian Institute of Technology, Madras, India

Bernhard Steffen
   TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos
   University of California, Los Angeles, CA, USA

Doug Tygar
   University of California, Berkeley, CA, USA

Gerhard Weikum
   Max Planck Institute for Informatics, Saarbrücken, Germany
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 Weissenhacker  
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
Additional Reviewers

Alireza Abyaneh
Mahmudul Faisal
   Al Ameen
Sebastian Arming
Konstantinos Athanasiou
Mohamed Faouzi Atig
Domagoj Babic
Michael Backenköhler
Gogul Balakrishnan
Clark Barrett
Matthew Bauer
Ryan Beckett
Harsh Beohar
Olaf Beyersdorff
Pavol Bielik
Armin Biere
Jesse Bingham
Stefan Blom
Stefan Bucur
Dario Cattaruzza
Ed Cerny
Le Ton Chanh
Dmitry Chistikov
Andreea Costea
Eva Darulova

Constantin Enea
Chuchu Fan
Samira Farahani
Grigory Fedyukovich
Pierre Flener
Matthias Fleury
Wan Fokkink
Zhoulai Fu
Nils Gesbert
Shilpi Goel
Yijia Gu
Arie Gurfinkel
Vahid Hashemi
Bardh Hoxha
Johannes Hölzl
Catalin Hritcu
Mens Irini-Eleftheria
Hiimanshu Jain
Chuan Jiang
George Karpenkov
Dileep Kini
Hui Kong
Aamod Kore
Jan Křetínský
Thilo Krüger

K. Narayan Kumar
Sebastian Küpper
Axel Legay
Sorin Lerner
Peizin Liu
Le Quang Loc
Andreas Lochbihler
Alexander Lück
Ravichandran Madhavan
Victor Magron
Assaf Marron
Umang Mathur
Todd Millstein
Sergio Mover
Suvam Mukherjee
Daniel Neider
Dennis Nolte
Peter O’Hearn
Wytse Oortwijn
Gustavo Petri
Lauren Pick
Markus Rabe
Jaideep Ramachandran
Rajarshi Ray
Andrew Reynolds
Nima Roohi Ofer Strichman Mike Whalen
Philipp Ruemmer Kausik Subramanian Christoph Wintersteiger
Sarah Sallinger Rob Sumners Xiao Xu
Anne-Kathrin Schmuck Sol Swords Shakiba Yaghoubi
Peter Schrammel Michael Tauchschnig Eugen Zalinescu
Daniel Nguyen Toan Thanh Qirun Zhang
Schwartz-Narbonne Dmitriy Traytel Yiji Zhang
Cristina Serban Nikos Tzevelekos Cai Zhouhong
Alexey Solovyev Viktor Vafeiadis Florian Zuleger
Sadegh Soudjani Freark van der Berg
Benno Stein Jules Villard

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
Fast Verification of Fast Cryptography for Secure Sockets (Invited Paper)

Chris Hawblitzel
Microsoft Research, Redmond, USA

Abstract. The Everest project is a joint effort between Microsoft Research, INRIA, and CMU to build a formally verified replacement for core HTTPS components, including the TLS protocol, cryptographic primitives, and certificate processing. The goal is to build an efficient implementation of these components, and the cryptographic primitives are especially critical to performance. Therefore, the project has developed verified hand-written assembly language implementations of common cryptographic primitives such as AES, SHA, and Poly1305.

This talk will present an overview of Everest, its verified assembly language cryptography, and the tools used to verify the code, including Vale, Dafny, F*, and Z3. It will discuss challenges in using such tools to verify low-level cryptographic code, including the need to reason about bit-level operations, large integers, and polynomials. A key challenge is the speed of the verification, and the talk will discuss ongoing efforts to combine tactics with SMT solving to make verification fast without sacrificing automation.
Contents – Part I

Invited Contributions

Safety Verification of Deep Neural Networks ..................................... 3
Xiaowei Huang, Marta Kwiatkowska, Sen Wang, and Min Wu

Program Verification Under Weak Memory Consistency
Using Separation Logic ................................................................. 30
Viktor Vafeiadis

The Power of Symbolic Automata and Transducers ......................... 47
Loris D’Antoni and Margus Veanes

Maximum Satisfiability in Software Analysis: Applications
and Techniques ................................................................. 68
Xujie Si, Xin Zhang, Radu Grigore, and Mayur Naik

Probabilistic Systems

Reluplex: An Efficient SMT Solver for Verifying Deep Neural Networks . . . 97
Guy Katz, Clark Barrett, David L. Dill, Kyle Julian,
and Mykel J. Kochenderfer

Automated Recurrence Analysis for Almost-Linear
Expected-Runtime Bounds .................................................. 118
Krishnendu Chatterjee, Hongfei Fu, and Aniket Murhekar

Markov Automata with Multiple Objectives .................................. 140
Tim Quatmann, Sebastian Junges, and Joost-Pieter Katoen

Ensuring the Reliability of Your Model Checker: Interval Iteration
for Markov Decision Processes ............................................. 160
Christel Baier, Joachim Klein, Linda Leuschner, David Parker,
and Sascha Wunderlich

Repairing Decision-Making Programs Under Uncertainty ................. 181
Aws Albarghouthi, Loris D’Antoni, and Samuel Drews

Value Iteration for Long-Run Average Reward in Markov
Decision Processes .......................................................... 201
Pranav Ashok, Krishnendu Chatterjee, Przemyslaw Daca,
Jan Křetínský, and Tobias Meggendorfer
Data Driven Techniques

STLInspector: STL Validation with Guarantees ........................... 225
   Hendrik Roehm, Thomas Heinz, and Eva Charlotte Mayer

Learning a Static Analyzer from Data ................................. 233
   Pavol Bielik, Veselin Raychev, and Martin Vechev

Synthesis with Abstract Examples ..................................... 254
   Dana Drachsler-Cohen, Sharon Shoham, and Eran Yahav

Data-Driven Synthesis of Full Probabilistic Programs ............... 279
   Sarah Chasins and Phitchaya Mangpo Phothilimthana

Logical Clustering and Learning for Time-Series Data ............... 305
   Marcell Vazquez-Chanlatte, Jyotirmoy V. Deshmukh, Xiaoming Jin,
   and Sanjit A. Seshia

Runtime Verification

MONTRE: A Tool for Monitoring Timed Regular Expressions .......... 329
   Dogan Ulus

Runtime Monitoring with Recovery of the SENT Communication Protocol .... 336
   Konstantin Selyunin, Stefan Jaksic, Thang Nguyen, Christian Reidl,
   Udo Hafner, Ezio Bartocci, Dejan Nickovic, and Radu Grosu

Runtime Verification of Temporal Properties over Out-of-Order
   Data Streams .................................................................. 356
   David Basin, Felix Klaedtke, and Eugen Zălinescu

Cyber-Physical Systems

Lagrangian Reachability .................................................. 379
   Jacek Cyranka, Md. Ariful Islam, Greg Byrne, Paul Jones,
   Scott A. Smolka, and Radu Grosu

Simulation-Equivalent Reachability of Large Linear Systems with Inputs .... 401
   Stanley Bak and Parasara Sridhar Duggirala

MIGHTYL: A Compositional Translation from MITL to Timed Automata .... 421
   Thomas Brihaye, Gilles Geeraerts, Hsi-Ming Ho,
   and Benjamin Monmege

DRYVR: Data-Driven Verification and Compositional Reasoning
   for Automotive Systems ............................................... 441
   Chuchu Fan, Bolun Qi, Sayan Mitra, and Mahesh Viswanathan
Automated Formal Synthesis of Digital Controllers for State-Space Physical Plants ......................................................... 462
  Alessandro Abate, Iury Bessa, Dario Cattaruzza, Lucas Cordeiro, Cristina David, Pascal Kesseli, Daniel Kroening, and Elizabeth Polgreen

Classification and Coverage-Based Falsification for Embedded Control Systems ................................................................. 483
  Arvind Adimoolam, Thao Dang, Alexandre Donzé, James Kapinski, and Xiaoqing Jin

Concurrency

GPUDrano: Detecting Uncoalesced Accesses in GPU Programs ............... 507
  Rajeev Alur, Joseph Devietti, Omar S. Navarro Leija, and Nimit Singhania

Context-Sensitive Dynamic Partial Order Reduction ............................. 526
  Elvira Albert, Puri Arenas, María García de la Banda, Miguel Gómez-Zamalloa, and Peter J. Stuckey

Starling: Lightweight Concurrency Verification with Views ....................... 544
  Matt Windsor, Mike Dodds, Ben Simner, and Matthew J. Parkinson

Compositional Model Checking with Incremental Counter-Example Construction ................................................................. 570
  Anton Wijs and Thomas Neele

Pithya: A Parallel Tool for Parameter Synthesis of Piecewise Multi-affine Dynamical Systems ............................................. 591
  Nikola Beneš, Luboš Brim, Martin Demko, Samuel Pastva, and David Šafraňek

Author Index .................................................................................. 599
## Contents – Part II

### Analysis of Software and Hardware

- **Verified Compilation of Space-Efficient Reversible Circuits**
  
  *Matthew Amy, Martin Roetteler, and Krysta M. Svore*
  
  Page 3

- **Ascertaining Uncertainty for Efficient Exact Cache Analysis**
  
  *Valentin Touzeau, Claire Maïza, David Monniaux, and Jan Reineke*
  
  Page 22

- **Non-polynomial Worst-Case Analysis of Recursive Programs**
  
  *Krishnendu Chatterjee, Hongfei Fu, and Amir Kafshdar Goharshady*
  
  Page 41

- **Automated Resource Analysis with Coq Proof Objects**
  
  *Quentin Carbonneaux, Jan Hoffmann, Thomas Reps, and Zhong Shao*
  
  Page 64

- **Look for the Proof to Find the Program: Decorated-Component-Based Program Synthesis**
  
  *Adrià Gascon, Ashish Tiwari, Brent Carmer, and Umang Mathur*
  
  Page 86

- **E-QED: Electrical Bug Localization During Post-silicon Validation Enabled by Quick Error Detection and Formal Methods**
  
  *Eshan Singh, Clark Barrett, and Subhasish Mitra*
  
  Page 104

- **SMTCoq: A Plug-In for Integrating SMT Solvers into Coq**
  
  *Burak Ekici, Alain Mebsout, Cesare Tinelli, Chantal Keller, Guy Katz, Andrew Reynolds, and Clark Barrett*
  
  Page 126

### Foundations of Verification

- **Efficient Parallel Strategy Improvement for Parity Games**
  
  *John Fearnley*
  
  Page 137

- **Model-Checking Linear-Time Properties of Parametrized Asynchronous Shared-Memory Pushdown Systems**
  
  *Marie Fortin, Anca Muscholl, and Igor Walukiewicz*
  
  Page 155

- **Minimization of Symbolic Transducers**
  
  *Olli Saarikivi and Margus Veanes*
  
  Page 176

- **Abstract Interpretation with Unfoldings**
  
  *Marcelo Sousa, César Rodríguez, Vijay D’Silva, and Daniel Kroening*
  
  Page 197

- **Cutoff Bounds for Consensus Algorithms**
  
  *Ognjen Marić, Christoph Sprenger, and David Basin*
  
  Page 217
Towards Verifying Nonlinear Integer Arithmetic ........................................... 238
Paul Beame and Vincent Liew

Distributed and Networked Systems

Network-Wide Configuration Synthesis ....................................................... 261
Ahmed El-Hassany, Petar Tsankov, Laurent Vanbever, and Martin Vechev

Verifying Equivalence of Spark Programs .................................................... 282
Shelly Grossman, Sara Cohen, Shachar Itzhaky, Noam Rinetzky, and Mooly Sagiv

Synchronization Synthesis for Network Programs .......................................... 301
Jedidiah McClurg, Hossein Hojjat, and Pavol Černý

Synthesis

BoSy: An Experimentation Framework for Bounded Synthesis ....................... 325
Peter Faymonville, Bernd Finkbeiner, and Leander Tentrup

Bounded Synthesis for Streett, Rabin, and CTL* ........................................ 333
Ayrat Khalimov and Roderick Bloem

Quantitative Assume Guarantee Synthesis .................................................. 353
Shaull Almagor, Orna Kupferman, Jan Oliver Ringert, and Yaron Velner

Syntax-Guided Optimal Synthesis for Chemical Reaction Networks. ............. 375
Luca Cardelli, Milan Češka, Martin Fränzle, Marta Kwiatkowska, Luca Laurenti, Nicola Paoletti, and Max Whitby

Decision Procedures and Their Applications

Model Counting for Recursively-Defined Strings ........................................ 399
Minh-Thai Trinh, Duc-Hiep Chu, and Joxan Jaffar

A Three-Tier Strategy for Reasoning About Floating-Point Numbers in SMT ........ 419
Sylvain Conchon, Mohamed Iguernlala, Kailiang Ji, Guillaume Melquiond, and Clément Fumex

A Correct-by-Decision Solution for Simultaneous Place and Route ............... 436
Alexander Nadel

Scaling Up DPLL(T) String Solvers Using Context-Dependent Simplification ....... 453
Andrew Reynolds, Maverick Woo, Clark Barrett, David Brumley, Tianyi Liang, and Cesare Tinelli
On Expansion and Resolution in CEGAR Based QBF Solving ........................................ 475
  Leander Tentrup

A Decidable Fragment in Separation Logic with Inductive Predicates
  and Arithmetic ................................................................. 495
  Quang Loc Le, Makoto Tatsuta, Jun Sun, and Wei-Ngan Chin

Software Analysis

Finding Fix Locations for CFL-Reachability Analyses via Minimum Cuts . . . 521
  Andrei Marian Dan, Manu Sridharan, Satish Chandra,
  Jean-Baptiste Jeannin, and Martin Vechev

Proving Linearizability Using Forward Simulations .............................. 542
  Ahmed Bouajjani, Michael Emmi, Constantin Enea,
  and Suha Orhun Mutluergil

EAHyper: Satisfiability, Implication, and Equivalence Checking
  of Hyperproperties ............................................................. 564
  Bernd Finkbeiner, Christopher Hahn, and Marvin Stenger

Automating Induction for Solving Horn Clauses ................................. 571
  Hiroshi Unno, Sho Torii, and Hiroki Sakamoto

A STORM is Coming: A Modern Probabilistic Model Checker ............... 592
  Christian Dehnert, Sebastian Junges, Joost-Pieter Katoen,
  and Matthias Volk

On Multiphase-Linear Ranking Functions ....................................... 601
  Amir M. Ben-Amram and Samir Genaim

Author Index ................................................................. 621