Lecture Notes in Computer Science

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

Editorial Board

David Hutchison
   *Lancaster University, UK*

Takeo Kanade
   *Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler
   *University of Surrey, Guildford, UK*

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

Alfred Kobsa
   *University of California, Irvine, CA, USA*

Friedemann Mattern
   *ETH Zurich, Switzerland*

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

Moni Naor
   *Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz
   *University of Bern, Switzerland*

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

Bernhard Steffen
   *University of Dortmund, Germany*

Madhu Sudan
   *Massachusetts Institute of Technology, MA, USA*

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

Doug Tygar
   *University of California, Berkeley, CA, USA*

Gerhard Weikum
   *Max-Planck Institute of Computer Science, Saarbruecken, Germany*
Preface

This volume contains the proceedings of the 20th International Conference on Computer Aided Verification (CAV) held in Princeton, New Jersey, USA, during July 7–14, 2008. CAV is dedicated to the advancement of the theory and practice of computer-aided formal analysis methods for hardware and software systems. Its scope ranges from theoretical results to concrete applications, with an emphasis on practical verification tools and the underlying algorithms and techniques.

Overall, 2008 has been a historical year for CAV.

– It marks the 20th anniversary of CAV, which has served as a forum for ideas whose impact is now clearly felt in research and practice.
– It celebrates the recognition received by Edmund M. Clarke, E. Allen Emerson and Joseph Sifakis as winners of the 2007 ACM Turing Award for their research in model checking. CAV is proud to have been the intellectual home for model checking over these 20 years.
– In recognition of the large body of contributions made to the field of computer-aided verification, the CAV Award was instituted this year with the first winner announced at the conference, and a citation to appear in the proceedings of the 21st CAV.

There were 131 paper submissions, divided into 104 regular and 27 tool papers. These went through an active review process, with each submission reviewed by at least 3, and on average 4, members of the Program Committee. We also sought external reviews from experts in certain areas. Authors had the opportunity to respond to the initial reviews during an author response period. All these inputs were used by the Program Committee in selecting a final program with 33 regular papers and 14 tool papers.

In addition to the reviewed papers, the program included:

– A session recognizing the Turing Award winners, with invited talks by them on the future of model checking.
– Two invited talks:
  • Edward Felten (Princeton University): *Coping with Outside-the-Box Attacks*
  • James Larus (Microsoft Research): *Singularity: Designing Better Software*
– Four invited tutorials:
  • Harry Foster (Mentor Graphics): *Assertion-based Verification*
  • John Harrison (Intel): *Theorem Proving for Verification*
  • Peter O’Hearn (University of London): *Tutorial on Separation Logic*
  • Reinhard Wilhelm (Saarland University): *Abstract Interpretation with Applications to Timing Validation*
– Reports on the results of two competitions:
  • The fourth *Satisfiability Modulo Theories Competition (SMT-Comp)*
  • The second *Hardware Model Checking Competition (HWMCC)*

CAV 2008 had seven affiliated workshops:

– Automated Formal Methods (AFM)
– Bit-Precise Reasoning (BPR)
– Exploiting Concurrency Efficiently and Correctly ((EC)$^2$)
– Formal verification of Analog Circuits (FAC)
– Heap Analysis and Verification (HAV)
– Numerical abstractions for Software Verification (NSV)
– Satisfiability Modulo Theories (SMT)

We gratefully acknowledge the support to CAV 2008 from Princeton University through facilities and other resources, the Institute for Advanced Study for hosting the conference banquet, and our corporate sponsors – Cadence Design Systems, IBM, Intel, Jasper Design Automation, Mentor Graphics, Microsoft Research, NEC Labs America, and Synopsys – for their financial contributions.

Many individuals were very generous with their time and expertise that went into putting the conference together. We thank the Program Committee and the external reviewers for their efforts in the assessment and evaluation needed to put together the technical program. We thank Alan Hu and Byron Cook for their help in organizing the tutorials and workshops, respectively. We thank the CAV 2007 Chairs and organizers – Werner Damm, Holger Hermanns, and Jürgen Niehaus – for their help and advice. We thank Avi Wigderson for his support for the Conference Banquet, held at the Institute for Advanced Study. We thank the CAV Steering Committee – Ed Clarke, Mike Gordon, Bob Kurshan and Amir Pnueli – for their help and advice.

We would especially like to thank Tara Zarillo (Conference Services, Princeton University), Stacey Weber Jackson (Electrical Engineering, Princeton University) and Susan Olson (Institute for Advanced Study) for their help with local arrangements; Maggie Westergaard (Communications Office, Princeton University) for designing the conference poster; and Nadia Papakonstantinou (NEC Labs America) for serving as the webmaster. We thank Andrei Voronkov for creating and supporting the invaluable EasyChair conference management system. Finally, we thank Springer for their help in publishing the 20th Anniversary DVD Compendium (with proceedings of CAV 1-20), and for providing a complimentary copy of the proceedings of the 25MC Workshop (held at FLoC 2006) to all CAV 2008 attendees.

July 2008

Aarti Gupta
Sharad Malik
Conference Organization

Program Chairs

Aarti Gupta (NEC Laboratories America, USA)
Sharad Malik (Princeton University, USA)

Program Committee

Rajeev Alur (University of Pennsylvania, USA)
Nina Amla (Cadence, USA)
Clark Barrett (New York University, USA)
Armin Biere (Johannes Kepler Universität Linz, Austria)
Roderick Bloem (TU Graz, Austria)
Ahmed Bouajjani (University Paris 7, France)
Alessandro Cimatti (IRST Trento, Italy)
Werner Damm (Carl von Ossietzky Universität Oldenburg, Germany)
Steven German (IBM, USA)
Ganesh Gopalakrishnan (University of Utah, USA)
Michael Gordon (University of Cambridge, UK)
Orna Grumberg (Technion, Israel)
David Harel (Weizmann Institute, Israel)
John Harrison (Intel, USA)
Thomas Henzinger (EPFL, Switzerland)
Holger Hermanns (Universität des Saarlandes, Germany)
Pei-Hsin Ho (Synopsys, USA)
Robert Jones (Intel, USA)
Daniel Kroening (Oxford University, UK)
Orna Kupferman (Hebrew University, Israel)
Shuvendu Lahiri (Microsoft Research, USA)
Rupak Majumdar (University of California – Los Angeles, USA)
Oded Maler (Verimag, France)
Kenneth McMillan (Cadence, USA)
Kedar Namjoshi (Alcatel-Lucent Bell Labs, USA)
Corina Pasareanu (NASA, USA)
Amir Pnueli (New York University)
Andreas Podelski (University of Freiburg, Germany)
Shaz Qadeer (Microsoft Research, USA)
Koushik Sen (University of California – Berkeley, USA)
Fabio Somenzi (University of Colorado, USA)
Ofer Strichman (Technion, Israel)
Karen Yorav (IBM Haifa, Israel)
Lenore Zuck (University of Illinois, USA)
VIII Organization

Organizing Committee

Tutorials Chair: Alan J. Hu (University of British Columbia, Canada)
Workshops Chair: Byron Cook (Microsoft Research, UK)

Steering Committee

Edmund M. Clarke (Carnegie Mellon University, USA)
Michael Gordon (University of Cambridge, UK)
Robert P. Kurshan (Cadence, USA)
Amir Pnueli (New York University, USA)

Sponsors

Princeton University
Cadence Design Systems
IBM
Intel Corporation
Jasper Design Automation
Mentor Graphics
Microsoft Research
NEC Laboratories America
Synopsys

Reviewers

Yasmina Abdeddaim  Jesse Bingham
Parosh Abdulla  Per Bjesse
Alfred Aho  Nicolas Blanc
Daphna Amit  Mihaela Gheorghiu Bobaru
Eli Arbel  Marius Bozga
Gilad Arnold  Marco Bozzano
Tamarah Arons  Aaron Bradley
Cyrille Valentin Artho  Davide Bresolin
Eugene Asarin  Angelo Brillout
Joanne Atlee  James Brotherston
Domagoj Babic  Robert Brummayer
Christel Baier  Roberto Brutomesso
Gogul Balakrishnan  Annette Bunker
Gérard Basler  Sebastian Burckhardt
Gregory Batt  Luis Caïres
Jason Baumgartner  Paul Caspi
Dirk Beyer  Rohit Chadha
Kunal Bindal  Yury Chebiryak
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dejan Nickovic</td>
<td>Stephen Siegel</td>
</tr>
<tr>
<td>Rotem Oshman</td>
<td>Mihaela Sighireanu</td>
</tr>
<tr>
<td>Joel Ouaknine</td>
<td>Eli Singerman</td>
</tr>
<tr>
<td>Chang-Seo Park</td>
<td>Vasu Singh</td>
</tr>
<tr>
<td>Seung-Joon Park</td>
<td>Oleg Sokolsky</td>
</tr>
<tr>
<td>Udo Payer</td>
<td>Scott Stoller</td>
</tr>
<tr>
<td>Dmitry Pidan</td>
<td>Andre Süßflow</td>
</tr>
<tr>
<td>Ingo Pill</td>
<td>Murali Talupur</td>
</tr>
<tr>
<td>Carl Pixley</td>
<td>Oliver Theel</td>
</tr>
<tr>
<td>Alberto Policriti</td>
<td>Gregory Theoduloz</td>
</tr>
<tr>
<td>Mitra Purandare</td>
<td>Ronald Tögl</td>
</tr>
<tr>
<td>Zvonimir Rakamaric</td>
<td>Stefano Tonetta</td>
</tr>
<tr>
<td>Silvio Ranise</td>
<td>Tayssir Touili</td>
</tr>
<tr>
<td>Jean-Francois Raskin</td>
<td>Stavros Tripakis</td>
</tr>
<tr>
<td>Kavita Ravi</td>
<td>Viktor Vafeiadis</td>
</tr>
<tr>
<td>Arend Rensink</td>
<td>Martin Vechev</td>
</tr>
<tr>
<td>Marco Roveri</td>
<td>Helmut Veith</td>
</tr>
<tr>
<td>Amitabha Roy</td>
<td>Michael Veksler</td>
</tr>
<tr>
<td>Pritam Roy</td>
<td>Miroslav Velev</td>
</tr>
<tr>
<td>Abhik Roychoudhury</td>
<td>Yakir Visel</td>
</tr>
<tr>
<td>Mirron Rozanov</td>
<td>Willem Visser</td>
</tr>
<tr>
<td>Theo Ruys</td>
<td>Anh Vo</td>
</tr>
<tr>
<td>Michael Ryabytsev</td>
<td>Tomas Vojnar</td>
</tr>
<tr>
<td>Andrey Rybalchenko</td>
<td>Bjoern Wachter</td>
</tr>
<tr>
<td>Sriram Sankaranarayanan</td>
<td>Silke Wagner</td>
</tr>
<tr>
<td>Jun Sawada</td>
<td>Thomas Wahl</td>
</tr>
<tr>
<td>Julien Schmaltz</td>
<td>Ou Wei</td>
</tr>
<tr>
<td>Viktor Schuppan</td>
<td>Georg Weissenbacher</td>
</tr>
<tr>
<td>Roberto Sebastiani</td>
<td>Bernd Westphal</td>
</tr>
<tr>
<td>Peter-Michael Seidel</td>
<td>Thomas Wies</td>
</tr>
<tr>
<td>Sanjit A. Seshia</td>
<td>Christoph M. Wintersteiger</td>
</tr>
<tr>
<td>Subodh Sharma</td>
<td>Verena Wolf</td>
</tr>
<tr>
<td>Natasha Sharygina</td>
<td>Jin Yang</td>
</tr>
<tr>
<td>Vitaly Shmatikov</td>
<td>Yu Yang</td>
</tr>
<tr>
<td>Sharon Shoham</td>
<td>Greta Yorsh</td>
</tr>
</tbody>
</table>
CAV Award

An annual award, called the CAV Award, has been established:

“For a specific fundamental contribution or a series of outstanding contributions to the field of computer-aided verification.”

The cited contribution(s) must have been made not more recently than 5 years ago and not over 20 years ago. In addition, the contribution(s) should not yet have received recognition via a major award, such as the ACM Turing or Kanellakis Awards. (The nominee may have received such an award for other contributions.)

The award of $10,000 will be granted to an individual or group of individuals chosen by the Award Committee from a list of nominations. The Award Committee will select the nomination that most compellingly demonstrates a specific fundamental contribution or a series of outstanding contributions to the field of computer-aided verification, evidenced by its influence over the last 5–20 years, and ratified by a majority of the Award Committee. If the Award Committee does not so ratify any nomination, then no award shall be made in the given year.

The CAV Award shall be presented in an award ceremony at the Computer-Aided Verification Conference.

The Award Committee will provide a detailed citation that explains the basis of the award. This citation will be published together with selected papers from the conference in a forthcoming Special Issue of a Journal of Record. The present Journal of Record is the Springer journal *Formal Methods in System Design*.

Anyone, with the exception of members of the Award Committee, is eligible to receive the Award.

CAV Award Process

A description of the full process governing the administration of the CAV Award follows. This will also be published in the Journal of Record in which the citation for the first CAV Award is given.

Nominations

Anyone can submit a nomination. The Award Committee can originate a nomination.

A nomination must state clearly the contribution(s), explain why the contribution is fundamental or the series of contributions is outstanding, and be accompanied by supporting letters and other evidence of worthiness. Nominations should include a proposed citation (up to 25 words), a succinct (100-250 words) description of the contribution(s), and a detailed statement to justify the nomination.
A call for nominations will be part of the CAV call for papers, with the same
deadline as for papers.
Nominations shall be sent to the Award Committee Chair.

**Award Committee**

The Award Committee consists of four individuals, each of whom shall have been
an author of a paper accepted by CAV within the previous five years, unless this
requirement is waived by the CAV Steering Committee. The members of the CAV
Steering Committee are not eligible to serve on the Award Committee.

Two members of the Award Committee shall hold positions in the United
States and two shall hold non-U.S. positions.

The four positions on the Award Committee are referred to as p₁, p₂, p₃
and p₄. The Steering Committee has appointed the first Award Committee to
the respective positions.

The tenure of a member in position pᵢ will be i years.

In respective subsequent years, the member in position p₁ will retire, the
member in position pᵢ (i > 1) will assume position pᵢ₋₁, and the current
Award Committee will select a member to fill position p₄ in the following year,
by a majority vote of the current Award Committee.

The retiring member in position p₁ will not be selected for position p₄ in
the following year, in order to assure turn-over in the Award Committee.

The member in position p₁ will serve as Chair of the Award Committee,
with the responsibility of receiving nominations, distributing them to the other
members of the Award Committee, and overseeing the selection processes for
the Award and new member.

The Award Committee will take into account all individuals who have con-
tributed to an awarded accomplishment, as well as independent discoveries of
an awarded accomplishment, and assure that all individuals are treated fairly.

Awards will be for contributions not already honored by another major award.

The 2008 CAV Award Committee consisted of Thomas Henzinger (Chair),
Randal Bryant, Orna Grumberg, and Moshe Vardi.

The 2009 CAV Award Committee consists of Randal Bryant (Chair), Orna
Grumberg, Moshe Vardi, and Joseph Sifakis.

**Rights of the Steering Committee**

In the event of an unanticipated vacancy of a sitting Award Committee, the
Steering Committee will assign someone to fill the vacated position.

Any circumstances that are unaccounted for through the above process will be
resolved by the Steering Committee. The Steering Committee reserves the right
to change the amount of the award, change the Journal of Record for citations or
dissolve the Award Committee and cancel the CAV Award at any time.

The Steering Committee reserves the right to veto the selection by the Award
Committee of a member for position p₄, in which case the Award Committee
will select someone else.
Table of Contents

Invited Talks

Singularity: Designing Better Software ........................................... 1
James R. Larus

Coping with Outside-the-Box Attacks ........................................... 3
Edward W. Felten

Invited Tutorials

Assertion-Based Verification: Industry Myths to Realities ................. 5
Harry Foster

Theorem Proving for Verification .................................................. 11
John Harrison

Tutorial on Separation Logic ....................................................... 19
Peter O’Hearn

Abstract Interpretation with Applications to Timing Validation ......... 22
Reinhard Wilhelm and Björn Wachter

Session 1: Concurrency

Reducing Concurrent Analysis Under a Context Bound to Sequential Analysis ................................................................. 37
Akash Lal and Thomas Reps

Monitoring Atomicity in Concurrent Programs ................................ 52
Azadeh Farzan and P. Madhusudan

Dynamic Verification of MPI Programs with Reductions in Presence of Split Operations and Relaxed Orderings .............................. 66
Sarvani Vakkalanka, Ganesh Gopalakrishnan, and Robert M. Kirby

A Hybrid Type System for Lock-Freedom of Mobile Processes ........ 80
Naoki Kobayashi and Davide Sangiorgi

Session 2: Memory Consistency

Implied Set Closure and Its Application to Memory Consistency Verification ................................................................. 94
Surender Baswana, Shashank K. Mehta, and Vishal Powar
Effective Program Verification for Relaxed Memory Models................. 107  
*Sebastian Burckhardt and Madanlal Musuvathi*

Mechanical Verification of Transactional Memories with Non-transactional Memory Accesses .................................................. 121  
*Ariel Cohen, Amir Pnueli, and Lenore D. Zuck*

Session 3: Abstraction/Refinement

Automated Assume-Guarantee Reasoning by Abstraction Refinement . . 135  
*Mihaela Gheorghiu Bobaru, Corina S. Păsăreanu, and Dimitra Giannakopoulou*

Local Proofs for Linear-Time Properties of Concurrent Programs ...... 149  
*Ariel Cohen and Kedar S. Namjoshi*

Probabilistic CEGAR .......................................................... 162  
*Holger Hermanns, Björn Wachter, and Lijun Zhang*

Session 4: Hybrid Systems

Computing Differential Invariants of Hybrid Systems as Fixedpoints . . 176  
*André Platzer and Edmund M. Clarke*

Constraint-Based Approach for Analysis of Hybrid Systems .......... 190  
*Sumit Gulwani and Ashish Tiwari*

Session 5: Tools – Dynamic Verification

AutoMOTGen: Automatic Model Oriented Test Generator for Embedded Control Systems ....................................................... 204  
*Ambar A. Gadkari, Anand Yeolekar, J. Suresh, S. Ramesh, Swarup Mohalik, and K.C. Shashidhar*

FShell: Systematic Test Case Generation for Dynamic Analysis and Measurement ......................................................... 209  
*Andreas Holzer, Christian Schallhart, Michael Tautschnig, and Helmut Veith*

Session 6: Modeling and Specification Formalisms

Applying the Graph Minor Theorem to the Verification of Graph Transformation Systems ..................................................... 214  
*Salil Joshi and Barbara König*

Conflict-Tolerant Features ................................................. 227  
*Deepak D’Souza and Madhu Gopinathan*
Session 7: Decision Procedures

Efficient Craig Interpolation for Linear Diophantine (Dis)Equations and Linear Modular Equations .................................................. 254
  Himanshu Jain, Edmund Clarke, and Orna Grumberg
Linear Arithmetic with Stars ................................................. 268
  Ruzica Piskac and Viktor Kuncak
Inferring Congruence Equations Using SAT .......................... 281
  Andy King and Harald Søndergaard

Session 8: Tools – Decision Procedures

The Barcelogic SMT Solver .................................................. 294
  Miquel Bofill, Robert Nieuwenhuis, Albert Oliveras,
  Enric Rodríguez-Carbonell, and Albert Rubio
The MathSAT 4 SMT Solver ............................................... 299
  Roberto Bruttomesso, Alessandro Cimatti, Anders Franzén,
  Alberto Griggio, and Roberto Sebastiani
CSISat: Interpolation for LA+EUF ....................................... 304
  Dirk Beyer, Damien Zufferey, and Rupak Majumdar
Prover’s Palette: A User-Centric Approach to Verification with Isabelle and QEPCAD-B ............................................. 309
  Laura I. Meikle and Jacques D. Fleuriot

Session 9: Program Verification

Heap Assumptions on Demand ............................................. 314
  Andreas Podelski, Andrey Rybalchenko, and Thomas Wies
Proving Conditional Termination ........................................ 328
  Byron Cook, Sumit Gulwani, Tal Lev-Ami,
  Andrey Rybalchenko, and Mooly Sagiv
Monotonic Abstraction for Programs with Dynamic Memory Heaps .... 341
  Parosh Aziz Abdulla, Ahmed Bouajjani, Jonathan Cederberg,
  Frédéric Haziza, and Ahmed Rezine
Enhancing Program Verification with Lemmas .......................... 355
  Huu Hai Nguyen and Wei-Ngan Chin
Session 10: Program and Shape Analysis

A Numerical Abstract Domain Based on Expression Abstraction and Max Operator with Application in Timing Analysis

Bhargav S. Gulavani and Sumit Gulwani

Scalable Shape Analysis for Systems Code

Hongseok Yang, Oukseh Lee, Josh Berdine, Cristiano Calcagno, Byron Cook, Dino Distefano, and Peter O’Hearn

Thread Quantification for Concurrent Shape Analysis

J. Berdine, T. Lev-Ami, R. Manevich, G. Ramalingam, and M. Sagiv

Session 11: Tools – Security and Program Analysis

The Scyther Tool: Verification, Falsification, and Analysis of Security Protocols

Cas J.F. Cremers

The CASPA Tool: Causality-Based Abstraction for Security Protocol Analysis

Michael Backes, Stefan Lorenz, Matteo Maffei, and Kim Pecina

Jakstab: A Static Analysis Platform for Binaries

Johannes Kinder and Helmut Veith

THOR: A Tool for Reasoning about Shape and Arithmetic

Stephen Magill, Ming-Hsien Tsai, Peter Lee, and Yih-Kuen Tsay

Session 12: Hardware Verification I

Functional Verification of Power Gated Designs by Compositional Reasoning

Cindy Eisner, Amir Nahir, and Karen Yorav

A Practical Approach to Word Level Model Checking of Industrial Netlists

Per Bjesse

Session 13: Hardware Verification II

Validating High-Level Synthesis

Sudipta Kundu, Sorin Lerner, and Rajesh Gupta

An Algebraic Approach for Proving Data Correctness in Arithmetic Data Paths

Oliver Wienand, Markus Wedler, Dominik Stoffel, Wolfgang Kunz, and Gert-Martin Greuel
Application of Formal Word-Level Analysis to Constrained Random Simulation ...................................................... 487

Hyondeuk Kim, Hoonsang Jin, Kavita Ravi, Petr Spacek, John Pierce, Bob Kurshan, and Fabio Somenzi

Session 14: Model Checking

Producing Short Counterexamples Using “Crucial Events” ............ 491
Sujatha Kashyap and Vijay K. Garg

Discriminative Model Checking ........................................ 504
Peter Niebert, Doron Peled, and Amir Pnueli

Session 15: Space Efficient Algorithms

Correcting a Space-Efficient Simulation Algorithm ................ 517
Rob van Glabbeek and Bas Ploeger

Semi-external LTL Model Checking ..................................... 530
Stefan Edelkamp, Peter Sanders, and Pavel Šimeček

Session 16: Tools – Model Checking

QMC: A Model Checker for Quantum Systems ......................... 543
Simon J. Gay, Rajagopal Nagarajan, and Nikolaos Papanikolaou

T(O)RMC: A Tool for (ω)-Regular Model Checking .................. 548
Axel Legay

Faster Than UPPAAL ..................................................... 552
Sebastian Kupferschmid, Martin Wehrle, Bernhard Nebel, and Andreas Podelski

Author Index .............................................................. 557