

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

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, 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

Tayssir Touili Byron Cook Paul Jackson (Eds.)

Computer Aided Verification

22nd International Conference, CAV 2010
Edinburgh, UK, July 15-19, 2010
Proceedings

Volume Editors

Tayssir Touili

LIAFA, CNRS and University Paris Diderot

Case 7014, 75205 Paris Cedex 13, France

E-mail: touili@liafa.jussieu.fr

Byron Cook

Microsoft Research, Roger Needham Building

JJ Thomson Avenue, Cambridge CB3 0FB, UK

E-mail: bycook@microsoft.com

Paul Jackson

University of Edinburgh, School of Informatics

Edinburgh EH8 9AB, UK

E-mail: pbj@inf.ed.ac.uk

Library of Congress Control Number: 2010929755

CR Subject Classification (1998): F.3, D.2, D.3, D.2.4, F.4.1, C.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN 0302-9743

ISBN-10 3-642-14294-X Springer Berlin Heidelberg New York

ISBN-13 978-3-642-14294-9 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

springer.com

© Springer-Verlag Berlin Heidelberg 2010

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper 06/3180

Preface

This volume contains the proceedings of the 22nd International Conference on Computer-Aided Verification (CAV) held in Edinburgh, UK, July 15–19 2010. CAV is dedicated to the advancement of the theory and practice of computer-assisted formal analysis methods for software and hardware 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.

We received 145 submissions: 101 submissions of regular papers and 44 submissions of tool papers. These submissions went through a meticulous review process; each submission was reviewed by at least 4, and on average 4.2 Program Committee members. Authors had the opportunity to respond to the initial reviews during an author response period. This helped the Program Committee members to select 51 papers: 34 regular papers and 17 tool papers.

In addition to the accepted papers, the program also included:

– Five invited talks:

- *Policy Monitoring in First-Order Temporal Logic*, by David Basin (ETH Zurich)
- *Retrofitting Legacy Code for Security*, by Somesh Jha (University of Wisconsin-Madison)
- *Induction, Invariants, and Abstraction*, by Deepak Kapur (University of New Mexico)
- *Quantitative Information Flow: From Theory to Practice?* by Pasquale Malacaria (Queen Mary University) and
- *Memory Management in Concurrent Algorithms*, by Maged Michael (IBM)

– Four invited tutorials:

- *ABC: An Academic Industrial-Strength Verification Tool*, by Robert Brayton (University of California, Berkeley)
- *Software Model Checking*, by Kenneth McMillan (Cadence Berkeley Labs)
- *There's Plenty of Room at the Bottom: Analyzing and Verifying Machine Code*, by Thomas Reps (University of Wisconsin-Madison) and
- *Constraint Solving for Program Verification: Theory and Practice by Example*, by Andrey Rybalchenko (Technische Universität München)

The program also included a session dedicated to the memory of Amir Pnueli, who died on November 2, 2009. Amir was one of the main leaders of modern advances in formal verification, and up to this year, he served on the CAV Steering Committee. His death is a big loss to our community. We dedicate these proceedings to his memory.

CAV 2010 was part of the Federated Logic Conference (FLoC 2010), hosted by the School of Informatics at the University of Edinburgh, Scotland. It was jointly organized with ICLP (International Conference on Logic Programming), IJCAR (International Joint Conference on Automated Reasoning), LICS (Logic in Computer Science), RTA (Rewriting Techniques and Applications), SAT (Theory and Applications of Satisfiability Testing), CSF (The Computer Security Foundations Symposium), and ITP (International Conference on Interactive Theorem Proving). In particular, the invited talks by David Basin and Deepak Kapur were, respectively, FLoC plenary and keynote talks.

CAV 2010 had eight affiliated workshops:

- The Fifth Automated Formal Methods Workshop (AFM 2010)
- Exploiting Concurrency Efficiently and Correctly (EC2-2010)
- Workshop on Evaluation Methods for Solvers, and Quality Metrics for Solutions (EMSQMS 2010)
- The First Hardware Verification Workshop (HWVW 2010)
- The Third International Workshop on Numerical Software Verification (NSV-3)
- The Second International Workshop on Practical Synthesis for Concurrent Systems (PSY 2010)
- International Workshop on Satisfiability Modulo Theories (SMT 2010)
- Synthesis, Verification and Analysis of Rich Models (SVARM 2010)

During the organization of CAV 2010, Edmund Clarke retired from the Steering Committee, and Orna Grumberg and Kenneth McMillan joined. Edmund Clarke was one of the founders of CAV, and we would like to especially thank him for his support of CAV from the start. We also thank the other Steering Committee members and the Chairs of CAV 2008 and CAV 2009 for their help and advice. We wish also to thank the Program Committee members and the external reviewers for their work in evaluating the submissions and assuring a high-quality program. We also thank Tomas Vojnar for his help in organizing the workshops. Finally, we thank Andrei Voronkov for creating and supporting the EasyChair conference management system.

CAV 2010 was supported by generous sponsorships. We gratefully acknowledge the support from Jasper Design Automation, IBM Research, Microsoft Research, NEC, EPSRC, NSF, Association for Symbolic Logic, CADE Inc., Google, Hewlett-Packard, and Intel.

July 2010

Tayssir Touili
Byron Cook
Paul Jackson

Conference Organization

Program Chairs

Tayssir Touili	LIAFA-CNRS, France
Byron Cook	Microsoft Research, UK
Paul Jackson	University of Edinburgh, UK

Program Committee

Rajeev Alur	University of Pennsylvania, USA
Domagoj Babić	UC Berkeley, USA
Christel Baier	Technical University of Dresden, Germany
Roderick Bloem	Graz University of Technology, Austria
Ahmed Bouajjani	LIAFA-University of Paris Diderot, France
Alessandro Cimatti	FBK-irst, Italy
Javier Esparza	Technische Universität München, Germany
Azadeh Farzan	University of Toronto, Canada
Martin Fränzle	University of Oldenburg, Germany
Ganesh Gopalakrishnan	University of Utah, USA
Mike Gordon	University of Cambridge, UK
Orna Grumberg	Technion, Israel
Ziyad Hanna	Jasper, USA
Holger Hermanns	Saarland University, Germany
Alan Hu	University of British Columbia, Canada
Kevin Jones	City University London, UK
Vineet Kahlon	NEC Labs, USA
Jean Krivine	PPS-CNRS, France
Daniel Kroening	Oxford University, UK
Sava Krstić	Intel Corporation, USA
Marta Kwiatkowska	Oxford University, UK
Oded Maler	VERIMAG-CNRS, France
Kenneth McMillan	Cadence, USA
David Monniaux	VERIMAG-CNRS, France
Markus Müller-Olm	Münster University, Germany
Kedar Namjoshi	Bell Labs, USA
Doron Peled	Bar Ilan University, Israel
Shaz Qadeer	Microsoft Research, USA
Jean-François Raskin	Brussels University, Belgium
Natasha Sharygina	University of Lugano, Switzerland

Helmut Veith	Vienna University of Technology, Austria
Kwangkeun Yi	Seoul National University, Korea
Karen Yorav	IBM Haifa, Israel
Greta Yorsh	IBM, USA

Steering Committee

Edmund M. Clarke	Carnegie Mellon University, USA
Mike Gordon	University of Cambridge, UK
Orna Grumberg	Technion, Israel
Robert P. Kurshan	Cadence, USA
Kenneth McMillan	Cadence, USA

Sponsors

Jasper Design Automation, IBM Research, Microsoft Research, NEC, EPSRC, NSF, Association for Symbolic Logic, CADE Inc., Google, Hewlett-Packard, Intel.

External Reviewers

Erika Ábrahám	Sylvain Conchon
Eli Arbel	Christopher Conway
Mohamed-Fauzi Atig	Scott Cotton
Jason Baumgartner	Thao Dang
Jesse Bingham	Vincent Danos
Nikolaj Bjørner	Aldric Degorre
Magnus Bjork	Flavio M. De Paula
Sandrine Blazy	Henning Dierks
Pieter-Tjerk de Boer	Antonio Dimalanta
Borzoo Bonakdarpour	Kyung-Goo Doh
Dragan Bosnacki	Alastair Donaldson
Matko Botinčan	Zhao Dong
Patricia Bouyer-Decitre	Alexandre Donzé
Marco Bozzano	Laurent Doyen
Tomas Brazdil	Klaus Dräger
Angelo Brillout	Vijay D'Silva
Roberto Bruttomesso	Jeremy Dubreil
Sebastian Burckhardt	Andreas Eggers
Mike Case	Tayfun Elmas
Franck Cassez	Michael Emmi
Pavol Cerny	Constantin Enea
Hana Chockler	Germain Faure
Frank Ciesinski	John Fearnley
Ariel Cohen	Jérôme Feret
Thomas Colcombet	Alessandro Ferrante

Emmanuel Filiot
Seth Fogarthy
Anders Franzen
Goran Frehse
Laurent Fribourg
Vashti Galpin
Gilles Geraerts
Steven German
Naghme Ghafari
Amit Goel
Alexey Gotsman
Susanne Graf
Karin Greimel
Andreas Griesmayer
Alberto Griggio
Marcus Groesser
Jim Grundy
Ashutosh Gupta
Dan Gutfreund
Peter Habermehl
Ernst Moritz Hahn
Leopold Haller
Philipp Haller
John Harrison
Arnd Hartmanns
John Hatcliff
Nannan He
Christian Herde
Hakan Hjort
Georg Hofferek
Andreas Holzer
William Hung
Hardi Hungar
Radu Iosif
Franjo Ivancić
Alexander Ivrii
Shahid Jabbar
Visar Januzaj
Bertrand Jeannot
Naiyong Jin
Barbara Jobstmann
Carson Jones
Yungbum Jung
Alexander Kaiser
Joost-Pieter Katoen

Mark Kattenbelt
Gal Katz
Jean-françois Kempf
Christian Kern
Sunghun Kim
Zachary Kincaid
Johannes Kinder
Joachim Klein
Sascha Klüppelholz
William Knottenbelt
Robert Könighofer
Soonho Kong
Maciej Koutny
Victor Kravets
Stephane Lafortune
Mario Lamberger
Peter Lammich
Cosimo Laneve
Frédéric Lang
François Laroussinie
Salvatore La Torre
Doug Lea
Oukseh Lee
Wonchan Lee
Axel Legay
Colas Le Guernic
Martin Leucker
Guodong Li
Henrik Lipskoch
Laurie Lugrin
Lars Lundgren
Parthasarathy Madhusudan
Rupak Majumdar
Nicolas Maquet
Johan Martensson
Radu Mateescu
Stephen McCamant
Bill McCloskey
Annabelle McIver
Igor Melatti
Yael Meller
Eric Mercer
Roland Meyer
Alan Mishchenko
John Moondanos

Leonardo de Moura
Sergio Mover
Matthieu Moy
Iman Narasamdya
Ziv Nevo
Dejan Nickovic
Gethin Norman
Hakjoo Oh
Avigail Orni
Rotem Oshman
Joel Ouaknine
Sungwoo Park
David Parker
Edgar Pek
Ruzica Piskac
Nir Piterman
Andreas Podelski
Corneliu Popeea
Mitra Purandare
Kairong Qian
Zvonimir Rakamarić
Yusi Ramadian
Stefan Ratschan
Jakob Rehof
Noam Rinetzkyy
Oleg Rokhlenko
Simone Rollini
Sitvanit Ruah
Philipp Rümmer
Marco Roveri
Andrey Rybalchenko
Sukyoung Ryu
Yaniv Sa'ar
Marko Samer
Sriram Sankaranarayanan
Gerald Sauter
Prateek Saxena
Christian Schallhart
Sven Schewe
Sylvain Schmitz
Viktor Schuppan
Stefan Schwoon
Alexander Serebrenik
Frédéric Servais
Ali Sezgin

Ohad Shacham
Subodh Sharma
Sarai Sheinvald
Mihaela Sighireanu
Nishant Sinha
Sebastian Skalberg
Jeremy Sproston
Stefan Staber
Mani Swaminathan
Nathalie Sznajder
Greg Szubzda
Paulo Tabuada
Murali Talupur
Michael Tautschnig
Tino Teige
PS Thiagarajan
Cesare Tinelli
Ashish Tiwari
Stefano Tonetta
Stavros Tripakis
Aliaksei Tsitovich
Frits Vaandrager
Viktor Vafeiadis
Martin Vechev
Tatyana Veksler
Mahesh Viswanathan
Yakir Vizel
Anh Vo
Björn Wachter
Thomas Wahl
Bow-Yaw Wang
Chao Wang
Andrzej Wasowski
Georg Weissenbacher
Alexander Wenner
Stephan Wilhelm
Ralf Wimmer
Christoph Wintersteiger
Verena Wolf
Nicolás Wolovick
Avi Yadgar
Eran Yahav
Sergio Yovine
Lijun Zhang
Florian Zuleger

Table of Contents

Invited Talks

Policy Monitoring in First-Order Temporal Logic	1
<i>David Basin, Felix Klaedtke, and Samuel Müller</i>	
Retrofitting Legacy Code for Security	19
<i>Somesh Jha</i>	
Quantitative Information Flow: From Theory to Practice?	20
<i>Pasquale Malacaria</i>	
Memory Management in Concurrent Algorithms	23
<i>Maged M. Michael</i>	

Invited Tutorials

ABC: An Academic Industrial-Strength Verification Tool	24
<i>Robert Brayton and Alan Mishchenko</i>	
There's Plenty of Room at the Bottom: Analyzing and Verifying Machine Code	41
<i>Thomas Reps, Junghee Lim, Aditya Thakur, Gogul Balakrishnan, and Akash Lal</i>	
Constraint Solving for Program Verification: Theory and Practice by Example	57
<i>Andrey Rybalchenko</i>	

Session 1. Software Model Checking

Invariant Synthesis for Programs Manipulating Lists with Unbounded Data	72
<i>Ahmed Bouajjani, Cezara Drăgoi, Constantin Enea, Ahmed Rezine, and Mihaela Sighireanu</i>	
Termination Analysis with Compositional Transition Invariants	89
<i>Daniel Kroening, Natasha Sharygina, Aliaksei Tsitovich, and Christoph M. Wintersteiger</i>	
Lazy Annotation for Program Testing and Verification	104
<i>Kenneth L. McMillan</i>	

The Static Driver Verifier Research Platform	119
<i>Thomas Ball, Ella Bounimova, Vladimir Levin, Rahul Kumar, and Jakob Lichtenberg</i>	
Dsolve: Safety Verification via Liquid Types	123
<i>Ming Kawaguchi, Patrick M. Rondon, and Ranjit Jhala</i>	
CONTESSA: Concurrency Testing Augmented with Symbolic Analysis . . .	127
<i>Sudipta Kundu, Malay K. Ganai, and Chao Wang</i>	

Session 2. Model Checking and Automata

Simulation Subsumption in Ramsey-Based Büchi Automata Universality and Inclusion Testing	132
<i>Parosh Aziz Abdulla, Yu-Fang Chen, Lorenzo Clemente, Lukáš Holík, Chih-Duo Hong, Richard Mayr, and Tomáš Vojnar</i>	
Efficient Emptiness Check for Timed Büchi Automata	148
<i>Frédéric Herbreteau, B. Srivathsan, and Igor Walukiewicz</i>	

Session 3. Tools

MERIT: An Interpolating Model-Checker	162
<i>Nicolas Caniart</i>	
Breach, A Toolbox for Verification and Parameter Synthesis of Hybrid Systems	167
<i>Alexandre Donzé</i>	
JTLV: A Framework for Developing Verification Algorithms	171
<i>Amir Pnueli, Yaniv Sa’ar, and Lenore D. Zuck</i>	
Petruchio: From Dynamic Networks to Nets	175
<i>Roland Meyer and Tim Strazny</i>	

Session 4. Counter and Hybrid Systems Verification

Synthesis of Quantized Feedback Control Software for Discrete Time Linear Hybrid Systems	180
<i>Federico Mari, Igor Melatti, Ivano Salvo, and Enrico Tronci</i>	
Safety Verification for Probabilistic Hybrid Systems	196
<i>Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn</i>	

A Logical Product Approach to Zonotope Intersection	212
<i>Khalil Ghorbal, Eric Goubault, and Sylvie Putot</i>	
Fast Acceleration of Ultimately Periodic Relations	227
<i>Marius Bozga, Radu Iosif, and Filip Konečný</i>	
An Abstraction-Refinement Approach to Verification of Artificial Neural Networks	243
<i>Luca Pulina and Armando Tacchella</i>	

Session 5. Memory Consistency

Fences in Weak Memory Models	258
<i>Jade Alglave, Luc Maranget, Susmit Sarkar, and Peter Sewell</i>	
Generating Litmus Tests for Contrasting Memory Consistency Models	273
<i>Sela Mador-Haim, Rajeev Alur, and Milo M.K. Martin</i>	

Session 6. Verification of Hardware and Low Level Code

Directed Proof Generation for Machine Code	288
<i>Aditya Thakur, Junghee Lim, Akash Lal, Amanda Burton, Evan Driscoll, Matt Elder, Tycho Andersen, and Thomas Reps</i>	
Verifying Low-Level Implementations of High-Level Datatypes	306
<i>Christopher L. Conway and Clark Barrett</i>	
Automatic Generation of Inductive Invariants from High-Level Microarchitectural Models of Communication Fabrics	321
<i>Satrajit Chatterjee and Michael Kishinevsky</i>	
Efficient Reachability Analysis of Büchi Pushdown Systems for Hardware/Software Co-verification	339
<i>Juncao Li, Fei Xie, Thomas Ball, and Vladimir Levin</i>	

Session 7. Tools

LTSmin: Distributed and Symbolic Reachability	354
<i>Stefan Blom, Jaco van de Pol, and Michael Weber</i>	
libalf: The Automata Learning Framework	360
<i>Benedikt Bollig, Joost-Pieter Katoen, Carsten Kern, Martin Leucker, Daniel Neider, and David R. Piegdon</i>	

Session 8. Synthesis

Symbolic Bounded Synthesis 365
Rüdiger Ehlers

Measuring and Synthesizing Systems in Probabilistic Environments ... 380
*Krishnendu Chatterjee, Thomas A. Henzinger,
 Barbara Jobstmann, and Rohit Singh*

Achieving Distributed Control through Model Checking 396
Susanne Graf, Doron Peled, and Sophie Quinton

Robustness in the Presence of Liveness 410
*Roderick Bloem, Krishnendu Chatterjee, Karin Greimel,
 Thomas A. Henzinger, and Barbara Jobstmann*

RATSY – A New Requirements Analysis Tool with Synthesis 425
*Roderick Bloem, Alessandro Cimatti, Karin Greimel,
 Georg Hofferek, Robert Könighofer, Marco Roveri,
 Viktor Schuppan, and Richard Seeber*

Comfusy: A Tool for Complete Functional Synthesis 430
Viktor Kunčak, Mikael Mayer, Ruzica Piskac, and Philippe Suter

Session 9. Concurrent Program Verification I

Universal Causality Graphs: A Precise Happens-Before Model for
 Detecting Bugs in Concurrent Programs 434
Vineet Kahlon and Chao Wang

Automatically Proving Linearizability 450
Viktor Vafeiadis

Model Checking of Linearizability of Concurrent List
 Implementations 465
*Pavol Černý, Arjun Radhakrishna, Damien Zufferey,
 Swarat Chaudhuri, and Rajeev Alur*

Local Verification of Global Invariants in Concurrent Programs 480
Ernie Cohen, Michał Moskal, Wolfram Schulte, and Stephan Tobies

Abstract Analysis of Symbolic Executions 495
Aws Albarghouthi, Arie Gurfinkel, Ou Wei, and Marsha Chechik

Session 10. Compositional Reasoning

Automated Assume-Guarantee Reasoning through Implicit Learning ... 511
*Yu-Fang Chen, Edmund M. Clarke, Azadeh Farzan,
 Ming-Hsien Tsai, Yih-Kuen Tsay, and Bow-Yaw Wang*

Learning Component Interfaces with May and Must Abstractions	527
<i>Rishabh Singh, Dimitra Giannakopoulou, and Corina Păsăreanu</i>	
A Dash of Fairness for Compositional Reasoning	543
<i>Ariel Cohen, Kedar S. Namjoshi, and Yaniv Sa'ar</i>	
SPLIT: A Compositional LTL Verifier	558
<i>Ariel Cohen, Kedar S. Namjoshi, and Yaniv Sa'ar</i>	

Session 11. Tools

A Model Checker for AADL	562
<i>Marco Bozzano, Alessandro Cimatti, Joost-Pieter Katoen, Viet Yen Nguyen, Thomas Noll, Marco Roveri, and Ralf Wimmer</i>	
PESSOA: A Tool for Embedded Controller Synthesis	566
<i>Manuel Mazo Jr., Anna Davitian, and Paulo Tabuada</i>	

Session 12. Decision Procedures

On Array Theory of Bounded Elements	570
<i>Min Zhou, Fei He, Bow-Yaw Wang, and Ming Gu</i>	
Quantifier Elimination by Lazy Model Enumeration	585
<i>David Monniaux</i>	

Session 13. Concurrent Program Verification II

Bounded Underapproximations	600
<i>Pierre Ganty, Rupak Majumdar, and Benjamin Monmege</i>	
Global Reachability in Bounded Phase Multi-stack Pushdown Systems	615
<i>Anil Seth</i>	
Model-Checking Parameterized Concurrent Programs Using Linear Interfaces	629
<i>S. La Torre, P. Madhusudan, and G. Parlato</i>	
Dynamic Cutoff Detection in Parameterized Concurrent Programs	645
<i>Alexander Kaiser, Daniel Kroening, and Thomas Wahl</i>	

Session 14. Tools

PARAM: A Model Checker for Parametric Markov Models	660
<i>Ernst Moritz Hahn, Holger Hermanns, Björn Wachter, and Lijun Zhang</i>	

GIST: A Solver for Probabilistic Games	665
<i>Krishnendu Chatterjee, Thomas A. Henzinger, Barbara Jobstmann, and Arjun Radhakrishna</i>	
A NuSMV Extension for Graded-CTL Model Checking	670
<i>Alessandro Ferrante, Maurizio Memoli, Margherita Napoli, Mimmo Parente, and Francesco Sorrentino</i>	
Author Index	675