

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

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Armin Biere Roderick Bloem (Eds.)

Computer Aided Verification

26th International Conference, CAV 2014
Held as Part of the Vienna Summer of Logic, VSL 2014
Vienna, Austria, July 18-22, 2014
Proceedings

 Springer

Volume Editors

Armin Biere
Johannes Kepler University Linz
Altenbergerstr. 69, 4040 Linz, Austria
E-mail: biere@jku.at

Roderick Bloem
IAIK, Graz University of Technology
Inffeldgasse 16a, 8010 Graz, Austria
E-mail: roderick.bloem@iaik.tugraz.at

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-319-08866-2

e-ISBN 978-3-319-08867-9

DOI 10.1007/978-3-319-08867-9

Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014942534

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

© Springer International Publishing Switzerland 2014

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. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

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.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

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

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)



logic n. 1 the science of reasoning.

– ORIGIN from Greek *logikē teknē*
'art of reason'.



Foreword



In the summer of 2014, Vienna hosted the largest scientific conference in the history of logic. The Vienna Summer of Logic (VSL, <http://vsl2014.at>) consisted of twelve large conferences and 82 workshops, attracting more than 2000 researchers from all over the world. This unique event was organized by the Kurt Gödel Society and took place at Vienna University of Technology during July 9 to 24, 2014, under the auspices of the Federal President of the Republic of Austria, Dr. Heinz Fischer.

The conferences and workshops dealt with the main theme, logic, from three important angles: logic in computer science, mathematical logic, and logic in artificial intelligence. They naturally gave rise to respective streams gathering the following meetings:

Logic in Computer Science / Federated Logic Conference (FLoC)

- 26th International Conference on Computer Aided Verification (CAV)
- 27th IEEE Computer Security Foundations Symposium (CSF)
- 30th International Conference on Logic Programming (ICLP)
- 7th International Joint Conference on Automated Reasoning (IJCAR)
- 5th Conference on Interactive Theorem Proving (ITP)
- Joint meeting of the 23rd EACSL Annual Conference on Computer Science Logic (CSL) and the 29th ACM/IEEE Symposium on Logic in Computer Science (LICS)
- 25th International Conference on Rewriting Techniques and Applications (RTA) joint with the 12th International Conference on Typed Lambda Calculi and Applications (TLCA)
- 17th International Conference on Theory and Applications of Satisfiability Testing (SAT)
- 76 FLoC Workshops
- FLoC Olympic Games (System Competitions)

Mathematical Logic

- Logic Colloquium 2014 (LC)
- Logic, Algebra and Truth Degrees 2014 (LATD)
- Compositional Meaning in Logic (GeTFun 2.0)
- The Infinity Workshop (INFINITY)
- Workshop on Logic and Games (LG)
- Kurt Gödel Fellowship Competition

Logic in Artificial Intelligence

- 14th International Conference on Principles of Knowledge Representation and Reasoning (KR)
- 27th International Workshop on Description Logics (DL)
- 15th International Workshop on Non-Monotonic Reasoning (NMR)
- 6th International Workshop on Knowledge Representation for Health Care 2014 (KR4HC)

The VSL keynote talks which were directed to all participants were given by Franz Baader (Technische Universität Dresden), Edmund Clarke (Carnegie Mellon University), Christos Papadimitriou (University of California, Berkeley) and Alex Wilkie (University of Manchester); Dana Scott (Carnegie Mellon University) spoke in the opening session. Since the Vienna Summer of Logic contained more than a hundred invited talks, it would not be feasible to list them here.

The program of the Vienna Summer of Logic was very rich, including not only scientific talks, poster sessions and panels, but also two distinctive events. One was the award ceremony of the Kurt Gödel Research Prize Fellowship Competition, in which the Kurt Gödel Society awarded three research fellowship prizes endowed with 100.000 Euro each to the winners. This was the third edition of the competition, themed Logical Mind: Connecting Foundations and Technology this year.

The 1st FLoC Olympic Games formed the other event and were hosted by the Federated Logic Conference (FLoC) 2014. Intended as a new FLoC element, the Games brought together 12 established logic solver competitions by different research communities. In addition to the competitions, the Olympic Games facilitated the exchange of expertise between communities, and increased the visibility and impact of state-of-the-art solver technology. The winners in the competition categories were honored with Kurt Gödel medals at the FLoC Olympic Games award ceremonies.

Organizing an event like the Vienna Summer of Logic was a challenge. We are indebted to numerous people whose enormous efforts were essential in making this vision become reality. With so many colleagues and friends working with us, we are unable to list them individually here. Nevertheless, as representatives of the three streams of VSL, we would like to particularly express our gratitude to all people who helped to make this event a success: the sponsors and the Honorary Committee; the Organization Committee and

the local organizers; the conference and workshop chairs and Program Committee members; the reviewers and authors; and of course all speakers and participants of the many conferences, workshops and competitions.

The Vienna Summer of Logic continues a great legacy of scientific thought that started in Ancient Greece and flourished in the city of Gödel, Wittgenstein and the Vienna Circle. The heroes of our intellectual past shaped the scientific world-view and changed our understanding of science. Owing to their achievements, logic has permeated a wide range of disciplines, including computer science, mathematics, artificial intelligence, philosophy, linguistics, and many more. Logic is everywhere – or in the language of Aristotle, πάντα πλήρη λογικῆς τέχνης.

July 2014

Matthias Baaz
Thomas Eiter
Helmut Veith

Preface

This volume contains the papers presented at CAV 2014: International Conference on Computer Aided Verification held during July 18–22, 2014 in Vienna, Austria.

CAV 2014 was the 26th in a series dedicated to the advancement of the theory and practice of computer-aided formal analysis methods for hardware and software systems.

As part of the Federated Logic Conference (FLoC) and the Vienna Summer of Logic, CAV 2014 was collocated with many other conferences in logic. 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.

The conference covered 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. The proceedings of the conference will have been the Springer-Verlag Lecture Notes in Computer Science series. A selection of papers was invited to a special issue of Formal Methods in System Design and the Journal of the ACM.

There were 229 paper submissions, 175 regular papers and 54 short papers. Each submission was reviewed by at least three, and on average 4 Program Committee members. The Program Committee decided to accept 57 papers which is an acceptance rate of 25%, consisting of 46 regular papers (26%) and 11 short papers (20%).

There were 293 abstract submissions originally and a couple of papers, not included in the number of 229 papers above, immediately rejected due to excessively exceeding the page limit. Among the 172 rejected papers considered for computing the acceptance rate, there were 7 regular and one short paper withdrawn on behalf of the authors after first versions of reviews had been sent out during the rebuttal phase.

Regarding paper format, CAV 2014 saw some important changes compared to previous versions. Beside long papers, e.g., regular papers, there were also short papers, but short papers were not restricted to be tool papers anymore. It was also encouraged to submit high quality tool papers and empirical evaluations as long papers. These regular papers with mostly only empirical results, and not necessarily new theory, produced some reservations on the side of the reviewers and was an import topic during the discussion of the Program Committee. Further, references did not count towards the page limit.

Beside the presentations of the accepted papers, and shared FLoC sessions, the program of CAV 2014 featured two tutorials, two CAV invited talks, three competition presentations and last but not least the presentation of the CAV award.

The first tutorial was given by David Monniaux, Verimag, Grenoble, France, on “How Do We Get Inductive Invariants?” and the second tutorial by Fabio Somenzi, University of Colorado at Boulder, USA, on “Hardware Model Checking”.

The first invited talk by Erik Winfree, Caltech, Pasadena, California, USA, had “Designing and Verifying Molecular Circuits and Systems Made of DNA” as the title. The second invited talk by Rance Cleaveland, University of Maryland and Fraunhofer, USA, discussed “Automated Testing”.

The CAV 2014 affiliated competitions consisted of the first “Syntax-Guided Synthesis Competition”, organized by Rajeev Alur, Dana Fisman, Rishabh Singh and Armando Solar-Lezama. Then there was the presentation of the results of the first Synthesis Competition for Reactive Systems “SYNTCOMP” organized by Swen Jacobs, Roderick Bloem, Rüdiger Ehlers and the 7th incarnation of the “Hardware Model Checking Competition”, which was organized by Armin Biere and Keijo Heljanko.

The CAV award was presented by the CAV Award Committee, which consisted of Moshe Vardi, Ahmed Bouajjani, Tom Ball, and headed by Marta Kwiatkowska.

The FLoC 2014 Interconference Topics on Security and SAT/SMT/QBF are a FLoC 2014 initiative by CAV, CSF, and IJCAR to foster exchange and discussion between conferences. The Interconference Topics consist of sessions from the participating conferences with a joint thematic focus. They provide a special opportunity for FLoC participants with particular interest in these topics.

We would like to thank our workshop and competition chair Martina Seidl, for caring about 21 CAV workshops, including 4 workshops affiliated with other FLoC conferences too. As publication chair Swen Jacobs did an excellent job setting up the web-pages and producing the proceedings.

Of course without the tremendous effort put in the reviewing process by our Program Committee members this conference would not have been possible. We would further thank the Steering Committee for support and guidance during the whole conference process as well as Andrei Voronkov for providing the EasyChair service in general and excellent support during using EasyChair for CAV 2014.

May 2014

Armin Biere
Roderick Bloem

Organization

Program Chairs

Armin Biere
Roderick Bloem

Johannes Kepler University of Linz, Austria
Graz University of Technology, Austria

Program Committee

Rajeev Alur	University of Pennsylvania, USA
Domagoj Babic	Google, USA
Gogul Balakrishnan	University of Wisconsin, USA
Nikolaj Bjorner	Microsoft Research, USA
Ahmed Bouajjani	LIAFA, University Paris Diderot, France
Aaron Bradley	University of Colorado Boulder, USA
Pavol Cerny	University of Colorado Boulder, USA
Koen Claessen	Chalmers University of Technology, Sweden
Byron Cook	Microsoft Research, UK
Azadeh Farzan	University of Toronto, Canada
Bernd Finkbeiner	Saarland University, Germany
Jasmin Fisher	Microsoft Research, UK
Mike Gordon	University of Cambridge, UK
Orna Grumberg	Technion - Israel Institute of Technology, Israel
Leopold Haller	University of Oxford, UK
Keijo Heljanko	Aalto University, Finland
William Hung	Synopsys Inc, USA
Somesh Jha	University of Wisconsin, USA
Susmit Jha	Intel, USA
Barbara Jobstmann	EPFL, Jasper DA, CNRS-Verimag, Switzerland/France
Bengt Jonsson	Uppsala University, Sweden
Laura Kovacs	Chalmers University of Technology, Sweden
Daniel Kroening	University of Oxford, UK
Marta Kwiatkowska	University of Oxford, UK
Kim Guldstrand Larsen	Aalborg University, Denmark
Joao Marques-Silva	University College Dublin, Ireland
Kedar Namjoshi	Bell Labs, USA
Corina Pasareanu	CMU and NASA Ames Research Center, USA
Doron Peled	Bar Ilan University, Israel
Pavithra Prabhakar	IMDEA Software Institute, Spain
Jean-Francois Raskin	Université Libre de Bruxelles, Belgium

Koushik Sen	University of California Berkeley, USA
Natasha Sharygina	Università della Svizzera Italiana, Switzerland
Nishant Sinha	IBM Research, India
Anna Slobodova	Centaur Technology, USA
Fabio Somenzi	University of Colorado Boulder, USA
Cesare Tinelli	University of Iowa, USA
Thomas Wahl	Northeastern University, USA
Georg Weissenbacher	Vienna University of Technology, Austria
Eran Yahav	Technion - Israel Institute of Technology, Israel

Organization Committee

Swen Jacobs	Graz University of Technology, Austria
Martina Seidl	Johannes Kepler University Linz, Austria

Steering Committee

Michael Gordon	University of Cambridge, UK
Orna Grumberg	Technion - Israel Institute of Technology, Israel
Aarti Gupta	NEC Laboratories, USA
Kenneth McMillan	Microsoft Research, USA

Additional Reviewers

Abate, Alessandro	Batty, Mark
Abd Elkader, Karam	Belov, Anton
Adzkiya, Dieky	Ben Sassi, Mohamed Amin
Albarghouthi, Aws	Bingham, Jesse
Alberti, Francesco	Birgmeier, Johannes
Alglave, Jade	Blackshear, Sam
Alt, Leonardo	Bogomolov, Sergiy
Althoff, Matthias	Boker, Udi
Aronis, Stavros	Boldo, Sylvie
Atig, Mohamed Faouzi	Botincan, Matko
Avigad, Jeremy	Boudjadar, A. Jalil
Bacci, Giorgio	Boulmé, Sylvain
Bacci, Giovanni	Bozianu, Rodica
Bandhakavi, Sruthi	Brain, Martin
Bansal, Kshitij	Brenguier, Romain
Basler, Gerard	Brockschmidt, Marc
Basset, Nicolas	Bucheli, Samuel
Bastani, Osbert	Bultan, Tevfik
Basu, Samik	Cabodi, Gianpiero

Cassel, Sofia
Cassez, Franck
Ceska, Milan
Chadha, Rohit
Chakarov, Aleksandar
Chen, Hong-Yi
Chen, Hongyi
Chen, Xin
Chen, Yu-Fang
Chockler, Hana
Choi, Wontae
Chowdhury, Omar
Christodorescu, Mihai
Ciardo, Gianfranco
Clemente, Lorenzo
Cordeiro, Lucas
D'Amorim, Marcelo
D'Antoni, Loris
D'Silva, Vijay
D'Souza, Deepak
Daca, Przemyslaw
Dalsgaard, Andreas Engelbrecht
Dang, Thao
David, Alexandre
David, Cristina
Davidson, Drew
Davis, Jared
De Carli, Lorenzo
De Moura, Leonardo
Dehnert, Christian
Delahaye, Benoit
Delaune, Stephanie
Delzanno, Giorgio
Dhawan, Mohan
Dillig, Isil
Dodds, Mike
Donaldson, Alastair
Doyen, Laurent
Drachsler, Dana
Dragoi, Cezara
Duret-Lutz, Alexandre
Een, Niklas
Emmi, Michael
Enea, Constantin
Falcone, Ylies
Faymonville, Peter
Fedyukovich, Grigory
Feng, Lu
Ferrara, Pietro
Filieri, Antonio
Filiot, Emmanuel
Fisman, Dana
Forejt, Vojtech
Fredrikson, Matt
Fränzle, Martin
Fu, Hongfei
Fuhs, Carsten
Furia, Carlo A.
Galenson, Joel
Ganai, Malay
Ganty, Pierre
Gerke, Michael
Girard, Antoine
Gopan, Denis
Greaves, David
Greenstreet, Mark
Griesmayer, Andreas
Griggio, Alberto
Groce, Alex
Grosu, Radu
Grundy, Jim
Gupta, Ashutosh
Gurfinkel, Arie
Haase, Christoph
Hadarean, Liana
Haddad, Axel
Hahn, Ernst Moritz
Hall, Ben
Hao, Kecheng
Harris, William
Hassan, Zyad
He, Fei
Hendriks, Martijn
Herbreteau, Frédéric
Hermanns, Holger
Hoare, Tony
Hochreiter, Sepp
Holik, Lukas
Holzer, Andreas
Hunter, Paul

Hyvärinen, Antti
 Ignatiev, Alexey
 Iosif, Radu
 Itzhaky, Shachar
 Ivancic, Franjo
 Jacobs, Swen
 Jaeger, Manfred
 Janota, Mikolas
 Jansen, Nils
 Jha, Sumit Kumar
 Jin, Hoon Sang
 Johansson, Moa
 Joshi, Saurabh
 Jovanovic, Aleksandra
 Kahlon, Vineet
 Kahsai, Temesghen
 Kannan, Jayanthkumar
 Katz, Omer
 Khlaaf, Heidy
 Kiefer, Stefan
 Kim, Chang Hwan Peter
 Kim, Hyondeuk
 Kincaid, Zachary
 Klein, Felix
 Komuravelli, Anvesh
 Konev, Boris
 Konnov, Igor
 Kotek, Tomer
 Kuismin, Tuomas
 Kuncak, Viktor
 Kupferman, Orna
 Kupriyanov, Andrey
 Kähkönen, Kari
 Lal, Akash
 Landsberg, David
 Lee, Wonchan
 Leino, Rustan
 Leonardsson, Carl
 Leue, Stefan
 Liang, Tianyi
 Liu, Jun
 Liu, Lingyi
 Liu, Peizun
 Liu, Wanwei
 Loginov, Alexey

Logozzo, Francesco
 Lopes, Nuno
 Lopes, Nuno P.
 Luchaup, Daniel
 Luckow, Kasper
 Malik, Sharad
 Mangal, Ravi
 Manquinho, Vasco
 Markey, Nicolas
 Mauborgne, Laurent
 McCamant, Stephen
 McClurg, Jedidiah
 Mereacre, Alexandru
 Meshman, Yuri
 Meyer, Roland
 Mikucionis, Marius
 Minea, Marius
 Mitra, Sayan
 Moarref, Salar
 Monmege, Benjamin
 Morgado, Antonio
 Moses, Yoram
 Mukherjee, Rajdeep
 Mukund, Madhavan
 Myers, Andrew
 Nadel, Alexander
 Natraj, Ashutosh
 Navarro Perez, Juan Antonio
 Navas, Jorge
 Nghiem, Truong
 Nickovic, Dejan
 Niebert, Peter
 Nimkar, Kaustubh
 Norman, Gethin
 Nyman, Ulrik
 Olesen, Mads Chr.
 Omari, Adi
 Ozay, Necmiye
 Pajic, Miroslav
 Palikareva, Hristina
 Paoletti, Nicola
 Papavasileiou, Vasilis
 Parker, David
 Parkinson, Matthew
 Parlato, Gennaro

Partush, Nimrod
 Passmore, Grant
 Pavlogiannis, Andreas
 Payer, Mathias
 Perez, Guillermo
 Peter, Isabelle
 Pichon, Jean
 Piskac, Ruzica
 Podelski, Andreas
 Poetzl, Daniel
 Prabhu, Prakash
 Pradel, M.
 Pradel, Michael
 Putot, Sylvie
 Qian, Kairong
 Rabe, Markus N.
 Radhakrishna, Arjun
 Raghothaman, Mukund
 Ramachandran, Jaideep
 Raman, Vishwanath
 Ranise, Silvio
 Ratschan, Stefan
 Ravanbakhsh, Hadi
 Ray, Sandip
 Rezine, Ahmed
 Rezine, Othmane
 Rinetzky, Noam
 Rodriguez, Cesar
 Rogalewicz, Adam
 Rollini, Simone Fulvio
 Rubio-Gonzalez, Cindy
 Ruemmer, Philipp
 Rybalchenko, Andrey
 Saarikivi, Olli
 Šafránek, David
 Sagonas, Konstantinos
 Saha, Indranil
 Sanchez, Cesar
 Sangnier, Arnaud
 Sankaranarayanan, Sriram
 Sarkar, Susmit
 Schrammel, Peter
 Sezgin, Ali
 Shacham, Ohad
 Sharma, Subodh
 Sheinvald, Sarai
 Shoham, Sharon
 Siirtola, Antti Tapani
 Singhanian, Nimit
 Sinha, Rohit
 Sinha, Saurabh
 Sorrentino, Francesco
 Sosnovich, Adi
 Srba, Jiri
 Stainer, Amelie
 Stenman, Jari
 Stergiou, Christos
 Sticksel, Christoph
 Strichman, Ofer
 Sturm, Thomas
 Su, Kaile
 Sznajder, Nathalie
 Tarrach, Thorsten
 Tasiran, Serdar
 Tautschnig, Michael
 Tentrup, Leander
 Terauchi, Tachio
 Thachuk, Chris
 Tiwari, Ashish
 Tonetta, Stefano
 Topcu, Ufuk
 Torfah, Hazem
 Totla, Nishant
 Treffler, Richard
 Trinh, Cong Quy
 Tripakis, Stavros
 Trivedi, Ashutosh
 Tschantz, Michael Carl
 Tsiskaridze, Nestan
 Tsitovich, Aliaksei
 Turrini, Andrea
 Udupa, Abhishek
 Ujma, Mateusz
 Urban, Caterina
 Vafeiadis, Viktor
 Vardi, Moshe
 Veanes, Margus
 Vechev, Martin
 Villard, Jules
 Viswanathan, Mahesh

XVIII Organization

Viswanathan, Ramesh

Vizel, Yakir

Von Essen, Christian

Wachter, Björn

Widder, Josef

Wieringa, Siert

Wiltsche, Clemens

Wintersteiger, Christoph

Wintersteiger, Christoph M.

Worrell, James

Wrigstad, Tobias

Xia, Bican

Xue, Bingtian

Yi, Wang

Zheng, Feijun

Zhou, Min

Zhu, Yunyun

Zielonka, Wieslaw

Zimmermann, Martin

Zwirschmayr, Jakob

Invited Tutorials and Talks

How Do We Get Inductive Invariants?

David Monniaux

CNRS, Verimag, Grenoble, France

Verifying the correctness of loop-free programs (or of general programs, up to bounded depth) is difficult: the state space explodes exponentially as the depth increases. Yet, the difficulty increases as we allow unboundedly many execution steps; proof approaches then generally rely on finding inductive invariants (properties shown to hold initially, then to remain true by induction).

Abstract interpretation attempts finding inductive invariants within a given domain, e.g. conjunctions of linear inequalities. The classical approach iterates a transformer until the property becomes inductive. In general, this approach may not terminate; thus termination is often enforced with a “widening” operator, which attempts at generalizing the iterates into an inductive property. Unfortunately, widening operators are brittle, with non-monotonic behaviors (supplying more information about a system may result in worse analysis outcomes!). Therefore, other approaches have been developed (policy iteration,...), which avoid this pitfall.

Finally, we shall discuss possible combinations of abstract interpretation and SMT-solving.

Hardware Model Checking

Fabio Somenzi

University of Colorado at Boulder, USA

This tutorial described the state-of-the art in Hardware-Model Checking using SAT and BDD-based techniques, including a discussion of the overall architecture of modern, multi-engine model checkers.

Designing and Verifying Molecular Circuits and Systems Made of DNA

Erik Winfree

California Institute of Technology, Pasadena, CA, USA

Inspired by the information processing core of biological organisms and its ability to fabricate intricate machinery from the molecular scale up to the macroscopic scale, research in synthetic biology, molecular programming, and nucleic acid nanotechnology aims to create information-based chemical systems that carry out human-defined molecular programs that input, output, and manipulate molecules and molecular structures. For chemistry to become the next information technology substrate, we will need improved tools for designing, simulating, and analyzing complex molecular circuits and systems. Using DNA nanotechnology as a model system, I will discuss how programming languages can be devised for specifying molecular systems at a high level, how compilers can translate such specifications into concrete molecular implementations, how both high-level and low-level specifications can be simulated and verified according to behavioral logic and the underlying biophysics of molecular interactions, and how Bayesian analysis techniques can be used to understand and predict the behavior of experimental systems that, at this point, still inevitably contain many ill-characterized components and interactions.

Automated Testing

Rance Cleaveland

University of Maryland, USA

In model-based testing, (semi-)formal models of systems are used to drive the derivation of test cases to be applied to the system-under-test (SUT). The technology has long been a part of the traditional hardware-design workflows, and it is beginning to find application in embedded-software development processes also. In automotive and land-vehicle control-system design in particular, models in languages such as MATLAB(r) / Simulink(r) / Stateflow(r) are used to drive the testing of the software used to control vehicle behavior, with tools like Reactis(r), developed by a team including the speaker, providing automated test-case generation support for this endeavor.

This talk will discuss how test-case generation capabilities may also be used to help verify that models meet formal specifications of their behavior. The method we advocate, Instrumentation-Based Verification (IBV), involves the formalization of behavior specifications as models that are used to instrument the model to be verified, and the use of coverage testing of the instrumented model to search for specification violations. The presentation will discuss the foundations of IBV, the test-generation approach and other features in Reactis that are used to support IBV, and the results of several case studies involving the use of the methods.

Competition Presentations

The First Syntax-Guided Synthesis Competition (SyGuS-COMP 2014)

Rajeev Alur¹, Dana Fisman¹, Rishabh Singh², and Armando Solar-Lezama^{2,*}

¹ University of Pennsylvania

² Massachusetts Institute of Technology

Abstract. *Syntax-Guided Synthesis (SyGuS)* is the computational problem of finding an implementation f that meets both a semantic constraint given by a logical formula φ in a background theory T , and a syntactic constraint given by a grammar G , which specifies the allowed set of candidate implementations [1]. Such a synthesis problem can be formally defined in SyGuS-IF [2], a language that is built on top of SMT-LIB.

The *Syntax-Guided Synthesis Competition (SyGuS-COMP)* is an effort to facilitate, bring together and accelerate research and development of efficient solvers for SyGuS by providing a platform for evaluating different synthesis techniques on a comprehensive set of benchmarks. The benchmarks for the first competition are restricted to the theories of bit-vector and integer linear arithmetic, yet their origin spans a variety of domains including bitvector algorithms, concurrency, robotics, and invariant generation. The solvers are scored primarily on the number of benchmark solved and the solving time, and secondarily on the succinctness of the synthesized solution.

References

1. Alur, R., Bodík, R., Juniwal, G., Martin, M.M.K., Raghthaman, M., Seshia, S.A., Singh, R., Solar-Lezama, A., Torlak, E., Udupa, A.: Syntax-Guided Synthesis. In: FMCAD, pp. 1–17. IEEE (2013)
2. Raghthaman, M., Udupa, A.: Language to Specify Syntax-Guided Synthesis Problems (May 2014), <http://arxiv.org/abs/1405.5590>

* This research was supported by NSF Expeditions in Computing award CCF-1138996 and the competition awards were sponsored by Microsoft Research and FLoC.

Hardware Model Checking Competition CAV 2014 Edition

Armin Biere¹ and Keijo Heljanko²

¹ Johannes Kepler University Linz, Austria

² Aalto University, Finland

The results of the 7th International Hardware Model Checking Competition were presented at CAV 2014. Model checkers were required to produce witnesses for single safety properties. The traces were checked by the AIGSIM tool, which is part of the AIGER tools. Otherwise, the competition was run in almost the same way as in the previous two years. The competition was run on a cluster at Aalto University with exclusive access to 32 nodes of 2x Six-Core AMD Opteron 2435 2.6GHz with at least 16 GB of RAM. This meant 12 cores for each solver per benchmark, memory limit of 15 GB and time limit of 900 seconds. As fall back we had the cluster at JKU with the same characteristics as in previous years. Beside the requirement to produce witnesses, rules, input and output format did not change.

During the FLoC Olympic Games ceremony in the second week, three real silver medals were handed out to the winners of the three tracks of the competition. These three tracks in the CAV 2014 edition of the competition consisted of: the single safety, the liveness and the deep bound track. There was no multiple property track for the CAV edition. It was considered to be the technically most challenging track, particularly while moving to new hardware, and further, only three medals were available. The winner of the deep bound track received both a medal and check, sponsored again by Oski technology. The competition further relied on support by the national research network on Rigorous System Engineering (RiSE) funded by the Austrian Science Fund (FWF) and also used resources made available through the Science-IT project at Aalto University.

SYNTCOMP - Synthesis Competition for Reactive Systems

Roderick Bloem¹, Rüdiger Ehlers^{2,3}, and Swen Jacobs¹

¹ Graz University of Technology
Austria

² University of Bremen
Germany

³ DFKI GmbH
Bremen, Germany

We present results of the first competition for reactive synthesis tools. For this first iteration, we focused on safety specifications, which are given as sequential circuits in an extension of the AIGER format for and-inverter graphs [1]. In the extended format, input signals of the circuit can be declared as controllable or uncontrollable. The synthesized implementation can read the uncontrollable input signals, and uses this information to drive the controllable signals such that the circuit never emits a **true** value at its error output signal.

The setting allows to encode a wide range of synthesis problems, and benchmarks for the first competition ranged from machine and robot controllers to hardware components like on-chip bus arbiters, and translations of LTL properties in general. Liveness properties are encodable in the form of *bounded* liveness properties, and the competition featured both benchmarks that make and that do not make use of this approach.

Tools were ranked with respect to the time needed for realizability checks and the size of circuits produced. Particular focus has been put on the verification of the synthesized implementations. Tools had to output the resulting controller in a format that is suitable as input to tools from the hardware model checking competition (HWMCC), i.e., as another and-inverter-graph circuit. Solutions had to be verifiable by current model checking tools in order to count for the competition. The competition also featured a track in which only the realizability of a specification needed to be checked, i.e., whether some controller exists or not.

SYNTCOMP was part of the FLoC 2014 Olympic Games and relied on support by the Austrian national research network on Rigorous Systems Engineering (RiSE), funded by the Austrian Science Fund (FWF).

Reference

1. Jacobs, S.: Extended AIGER Format for Synthesis. arXiv:1405.5793 (May 2014)

Table of Contents

Software Verification

The Spirit of Ghost Code	1
<i>Jean-Christophe Filliâtre, Léon Gondelman, and Andrei Paskevich</i>	
SMT-Based Model Checking for Recursive Programs	17
<i>Anvesh Komuravelli, Arie Gurfinkel, and Sagar Chaki</i>	
Property-Directed Shape Analysis	35
<i>Shachar Itzhaky, Nikolaj Bjørner, Thomas Reps, Mooly Sagiv, and Aditya Thakur</i>	
Shape Analysis via Second-Order Bi-Abduction	52
<i>Quang Loc Le, Cristian Gherghina, Shengchao Qin, and Wei-Ngan Chin</i>	
ICE: A Robust Framework for Learning Invariants	69
<i>Pranav Garg, Christof Löding, P. Madhusudan, and Daniel Neider</i>	
From Invariant Checking to Invariant Inference Using Randomized Search	88
<i>Rahul Sharma and Alex Aiken</i>	
SMACK: Decoupling Source Language Details from Verifier Implementations	106
<i>Zvonimir Rakamarić and Michael Emmi</i>	

Security

Synthesis of Masking Countermeasures against Side Channel Attacks . . .	114
<i>Hassan Eldib and Chao Wang</i>	
Temporal Mode-Checking for Runtime Monitoring of Privacy Policies . . .	131
<i>Omar Chowdhury, Limin Jia, Deepak Garg, and Anupam Datta</i>	
String Constraints for Verification	150
<i>Parosh Aziz Abdulla, Mohamed Faouzi Atig, Yu-Fang Chen, Lukáš Holík, Ahmed Rezine, Philipp Rümmer, and Jari Stenman</i>	
A Conference Management System with Verified Document Confidentiality	167
<i>Sudeep Kanav, Peter Lammich, and Andrei Popescu</i>	

VAC - Verifier of Administrative Role-Based Access Control Policies	184
<i>Anna Lisa Ferrara, P. Madhusudan, Truc L. Nguyen, and Gennaro Parlato</i>	

Automata

From LTL to Deterministic Automata: A Safriless Compositional Approach	192
<i>Javier Esparza and Jan Křetínský</i>	
Symbolic Visibly Pushdown Automata	209
<i>Loris D'Antoni and Rajeev Alur</i>	

Model Checking and Testing

Engineering a Static Verification Tool for GPU Kernels	226
<i>Ethel Bardsley, Adam Betts, Nathan Chong, Peter Collingbourne, Pantazis Deligiannis, Alastair F. Donaldson, Jeroen Ketema, Daniel Liew, and Shaz Qadeer</i>	
Lazy Annotation Revisited	243
<i>Kenneth L. McMillan</i>	
Interpolating Property Directed Reachability	260
<i>Yakir Vizel and Arie Gurfinkel</i>	
Verifying Relative Error Bounds Using Symbolic Simulation	277
<i>Jesse Bingham and Joe Leslie-Hurd</i>	
Regression Test Selection for Distributed Software Histories	293
<i>Milos Gligoric, Rupak Majumdar, Rohan Sharma, Lamyaa Eloussi, and Darko Marinov</i>	
GPU-Based Graph Decomposition into Strongly Connected and Maximal End Components	310
<i>Anton Wijs, Joost-Pieter Katoen, and Dragan Bošnački</i>	
Software Verification in the Google App-Engine Cloud	327
<i>Dirk Beyer, Georg Dresler, and Philipp Wendler</i>	
The NUXMV Symbolic Model Checker	334
<i>Roberto Cavada, Alessandro Cimatti, Michele Dorigatti, Alberto Griggio, Alessandro Mariotti, Andrea Micheli, Sergio Mover, Marco Roveri, and Stefano Tonetta</i>	

Biology and Hybrid Systems

Analyzing and Synthesizing Genomic Logic Functions	343
<i>Nicola Paoletti, Boyan Yordanov, Youssef Hamadi, Christoph M. Wintersteiger, and Hillel Kugler</i>	
Finding Instability in Biological Models	358
<i>Byron Cook, Jasmin Fisher, Benjamin A. Hall, Samin Ishtiaq, Garvit Juniwal, and Nir Piterman</i>	
Invariant Verification of Nonlinear Hybrid Automata Networks of Cardiac Cells	373
<i>Zhenqi Huang, Chuchu Fan, Alexandru Mereacre, Sayan Mitra, and Marta Kwiatkowska</i>	
Diamonds Are a Girl’s Best Friend: Partial Order Reduction for Timed Automata with Abstractions	391
<i>Henri Hansen, Shang-Wei Lin, Yang Liu, Truong Khanh Nguyen, and Jun Sun</i>	
Reachability Analysis of Hybrid Systems Using Symbolic Orthogonal Projections	407
<i>Willem Hagemann</i>	
Verifying LTL Properties of Hybrid Systems with K-LIVENESS	424
<i>Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta</i>	

Games and Synthesis

Safraless Synthesis for Epistemic Temporal Specifications	441
<i>Rodica Bozianu, Cătălin Dima, and Emmanuel Filiot</i>	
Minimizing Running Costs in Consumption Systems	457
<i>Tomáš Brázdil, David Kláška, Antonín Kučera, and Petr Novotný</i>	
CEGAR for Qualitative Analysis of Probabilistic Systems	473
<i>Krishnendu Chatterjee, Martin Chmelík, and Przemysław Daca</i>	
Optimal Guard Synthesis for Memory Safety	491
<i>Thomas Dillig, Isil Dillig, and Swarat Chaudhuri</i>	
Don’t Sit on the Fence: A Static Analysis Approach to Automatic Fence Insertion	508
<i>Jade Alglave, Daniel Kroening, Vincent Nimal, and Daniel Poetzl</i>	
MCMAS-SLK: A Model Checker for the Verification of Strategy Logic Specifications	525
<i>Petr Čermák, Alessio Lomuscio, Fabio Mogavero, and Aniello Murano</i>	

Solving Games without Controllable Predecessor	533
<i>Nina Narodytska, Alexander Legg, Fahiem Bacchus, Leonid Ryzhyk, and Adam Walker</i>	

G4LTL-ST: Automatic Generation of PLC Programs	541
<i>Chih-Hong Cheng, Chung-Hao Huang, Harald Ruess, and Stefan Stattelmann</i>	

Concurrency

Automatic Atomicity Verification for Clients of Concurrent Data Structures	550
<i>Mohsen Lesani, Todd Millstein, and Jens Palsberg</i>	

Regression-Free Synthesis for Concurrency	568
<i>Pavol Černý, Thomas A. Henzinger, Arjun Radhakrishna, Leonid Ryzhyk, and Thorsten Tarrach</i>	

Bounded Model Checking of Multi-threaded C Programs via Lazy Sequentialization	585
<i>Omar Inverso, Ermenegildo Tomasco, Bernd Fischer, Salvatore La Torre, and Gennaro Parlato</i>	

An SMT-Based Approach to Coverability Analysis	603
<i>Javier Esparza, Ruslán Ledesma-Garza, Rupak Majumdar, Philipp Meyer, and Filip Nikić</i>	

LEAP: A Tool for the Parametrized Verification of Concurrent Datatypes	620
<i>Alejandro Sánchez and César Sánchez</i>	

SMT and Theorem Proving

Monadic Decomposition	628
<i>Margus Veanes, Nikolaj Bjørner, Lev Nachmanson, and Sergey Bereg</i>	

A DPLL(T) Theory Solver for a Theory of Strings and Regular Expressions	646
<i>Tianyi Liang, Andrew Reynolds, Cesare Tinelli, Clark Barrett, and Morgan Deters</i>	

Bit-Vector Rewriting with Automatic Rule Generation	663
<i>Alexander Nadel</i>	

A Tale of Two Solvers: Eager and Lazy Approaches to Bit-Vectors	680
<i>Liana Hadarean, Kshitij Bansal, Dejan Jovanović, Clark Barrett, and Cesare Tinelli</i>	

AVATAR: The Architecture for First-Order Theorem Provers	696
<i>Andrei Voronkov</i>	
Automating Separation Logic with Trees and Data	711
<i>Ruzica Piskac, Thomas Wies, and Damien Zufferey</i>	
A Nonlinear Real Arithmetic Fragment	729
<i>Ashish Tiwari and Patrick Lincoln</i>	
Yices 2.2	737
<i>Bruno Dutertre</i>	

Bounds and Termination

A Simple and Scalable Static Analysis for Bound Analysis and Amortized Complexity Analysis	745
<i>Moritz Sinn, Florian Zuleger, and Helmut Veith</i>	
Symbolic Resource Bound Inference for Functional Programs	762
<i>Ravichandhran Madhavan and Viktor Kuncak</i>	
Proving Non-termination Using Max-SMT	779
<i>Daniel Larraz, Kaustubh Nimkar, Albert Oliveras, Enric Rodríguez-Carbonell, and Albert Rubio</i>	
Termination Analysis by Learning Terminating Programs	797
<i>Matthias Heizmann, Jochen Hoenicke, and Andreas Podelski</i>	
Causal Termination of Multi-threaded Programs	814
<i>Andrey Kupriyanov and Bernd Finkbeiner</i>	

Abstraction

Counterexample to Induction-Guided Abstraction-Refinement (CTIGAR)	831
<i>Johannes Birgmeier, Aaron R. Bradley, and Georg Weissenbacher</i>	
Unbounded Scalable Verification Based on Approximate Property- Directed Reachability and Datapath Abstraction	849
<i>Suho Lee and Karem A. Sakallah</i>	
QUICr: A Reusable Library for Parametric Abstraction of Sets and Numbers	866
<i>Arlen Cox, Bor-Yuh Evan Chang, and Sriram Sankaranarayanan</i>	

Author Index	875
-------------------------------	-----