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 for Informatics, Saarbruecken, Germany

Valeria Bertacco Axel Legay (Eds.)

Hardware and Software: Verification and Testing

9th International

Haifa Verification Conference, HVC 2013

Haifa, Israel, November 5-7, 2013

Proceedings

Springer

Volume Editors

Valeria Bertacco
University of Michigan
Department of Electrical Engineering and Computer Science
BBB4645, 2260 Hayward Avenue
Ann Arbor, MI 48109-2121, USA
E-mail: valeria@umich.edu

Axel Legay
Inria Rennes, Campus de Beaulieu
263, Avenue du Général Leclerc
35042 Rennes, France
E-mail: axel.legay@inria.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-03076-0 e-ISBN 978-3-319-03077-7
DOI 10.1007/978-3-319-03077-7
Springer Cham Heidelberg New York Dordrecht London

CR Subject Classification (1998): D.2.4-5, D.3.1, F.3.1-2, D.2.11, I.2.2-3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer International Publishing Switzerland 2013

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)

Preface

This volume contains the proceedings of the 9th Haifa Verification Conference (HVC 2013). The conference was hosted by IBM Research - Haifa and took place during November 5–7, 2013. It was the ninth event in this series of annual conferences dedicated to advancing the state of the art and state of the practice in verification and testing. The conference provided a forum for researchers and practitioners from academia and industry to share their work, exchange ideas, and discuss the future directions of testing and verification for hardware, software, and complex hybrid systems. This year HVC introduced a special track on software testing. This track, which was chaired by Amiram Yehudai and Itai Segall, expands the scope of HVC and attracted 11 submissions from a broader community.

Overall, HVC 2013 attracted 49 submissions in response to the call for papers. Each submission was assigned to at least three members of the Program Committee and in many cases additional reviews were solicited from outside experts. The Program Committee conferred about the submissions, judging them on their perceived importance, originality, clarity, and appropriateness for the expected audience. The Program Committee selected 23 papers for presentation, including five from the software testing track, resulting in an acceptance rate of 47%.

Complementing the contributed papers, the conference featured five invited keynote talks: “EDA in the Cloud” by Leon Stok, “Challenges in Enabling the Next Generation Mobile Experience: Are You Ready?” by Scott Runner, “Recent Advances in Model Checking” by Robert Brayton, “Synthesis of Concurrent Programs Using Genetic Programming” by Doron Peled, and “Opportunities and Challenges for High Performance Microprocessor Designs and Design Automation” by Ruchir Puri.

The conference itself started with a tutorial day including tutorials on: “Hardware Functional Verification - Present and Future” by Yuval Caspi; “SystemVerilog Assertions for Formal Verification” by Dmitry Korchemny; “Verification and Performance Analysis of Interconnects Within the SoCs” by Mirit Fromovich; “SAT, CSP, and Proofs” by Ofer Strichman; and “The System Simulation as a Tool for Development and Validation of Complex Systems” by Racheli Kenigsbuch.

We would like to extend our appreciation and sincere thanks to Sivan Rabinovich for serving as General Chair and handling the conference details so successfully. Our thanks also go to Arkadiy Morgenshtein for arranging the tutorials day. Finally, we would like to thank our arrangements support team: Eti Jahr for managing the technical aspects of the conference, Ettie Gilead and Chani Sacharen for handling communication, Yair Harry for web design, and Tammy Dekel for graphic design. HVC 2013 received sponsorships from IBM,

Cadence, Mellanox, Jasper, Qualcomm, and Mentor Graphics. Submissions and evaluations of papers, as well as the preparation of this proceedings volume, were handled by the EasyChair conference management system.

September 2013

Valeria Bertacco
Axel Legay

Organization

Program Committee

Valeria Bertacco	University of Michigan, USA
Armin Biere	FMV
Roderick Bloem	Graz University of Technology, Austria
Hana Chockler	King's College London, UK
Myra Cohen	University of Nebraska, USA
Alexandre David	Aalborg University, Denmark
Giuseppe Di Guglielmo	Columbia University, USA
Harry Foster	Mentor Graphics
Alex Goryachev	IBM Israel
Ian Harris	University of California, Irvine, USA
Michael Hsiao	Virginia Tech, USA
Alan Hu	University of British Columbia, Canada
Axel Legay	Inria, France
Jeff Lei	The University of Texas at Arlington, USA
João Lourenço	Universidade Nova de Lisboa, Portugal
Rupak Majumdar	Max Planck Institute, Germany
Oded Maler	Verimag, Grenoble, France
Leonardo Mariani	University of Milan, Italy
Amir Nahir	IBM, Israel
Preeti Panda	IIT Delhi, India
Hiren Patel	University of Waterloo, Canada
Itai Segall	IBM, Israel
Martina Seidl	FMV, Linz, Austria
Mark Trakhtenbrot	Holon Institute of Technology, Israel
Shobha Vasudevan	University of Illinois at Urbana-Champaign, USA
Sergiy Vilkomir	East Carolina University, USA
Ilya Wagner	Intel
Li-C. Wang	University of California, Santa Barbara, USA
Elaine Weyuker	DIMACS, Rutgers University, USA
Amiram Yehudai	Tel Aviv University, Israel

Additional Reviewers

Amin, Mohamed

André, Étienne

Chen, Wen

Dimitrova, Rayna

Khalimov, Ayrat

Kloos, Johannes

Könighofer, Bettina

Lanik, Jan

Liffiton, Mark

Meller, Yael

Mens, Irini

Mishra, Prabhat

Ferrere, Thomas

Gladisch, Christoph

Heule, Marijn

Kaushik, Anirudh

Poetzl, Daniel

Prähofer, Herbert

Sharma, Namita

Shomrat, Mati

Strichman, Ofer

Tyszberowicz, Shmuel

Vale, Tiago

Keynotes

EDA in the Cloud

Leon Stok

Electronic Design Automation Technologies, IBM

Abstract. A large number of compute intensive applications are moving to the cloud at a fast pace. EDA, has been on the forefront of computing for the last 25 years and should certainly be one of them. How come this has not happened yet at a noticeable scale? In surveying the attendees to the 50th Design Automation Conference cloud and IT was certainly at the forefront of their thoughts for the future of EDA. This talk will describe why EDA has not taken off in the cloud, but why it is inevitable to happen and what needs to be done to bring real value to the design and verification teams.

Opportunities and Challenges for High Performance Microprocessor Designs and Design Automation

Ruchir Puri

IBM Research

Abstract. With end of an era of classical technology scaling and exponential frequency increases, high end microprocessor designs and design automation methodologies are at an inflection point. With power and current demands reaching breaking points, and significant challenges in application software stack, we are also reaching diminishing returns from simply adding more cores. In design methodologies for high end microprocessors, although chip physical design efficiency has seen tremendous improvements, strong indications are emerging for maturing of those gains as well. In order to continue the cost-performance scaling in systems in light of these maturing trends, we must innovate up the design stack, moving focus from technology and physical design implementation to new IP and methodologies at logic, architecture, and at the boundary of hardware and software, solving key bottlenecks through application acceleration. This new era of innovation, which moves the focus up the design stack presents new challenges and opportunities to the design and design automation communities. This talk will motivate these trends and focus on challenges for high performance microprocessor design, verification, and design automation in the years to come.

Recent Advances in Model Checking

Robert K. Brayton

University of California, Berkeley

Abstract. Model checking, either for property checking or equivalence checking, continues to advance towards shorter runtimes and the ability to handle larger problem instances. These advances have been due to:

1. improved underlying engines such as SAT solvers, BMC, and semi-formal simulation,
2. new methods such as property directed reachability - IC3/PDR,
3. improved data structures for representing logic,
4. improved synthesis methods, such as signal correspondence, retiming, reparametrization, use of isomorphism
5. improved abstraction methods, such as localization and speculation,
6. use of parallelism and general availability of multi-core servers.

This progress is partially documented by the annual hardware model checking competitions and the growing set of competition categories, such as the liveness checking and multi-output categories. These competitions have also encouraged contributions of challenging industrial examples, all of which has greatly stimulated research and development in the model checking area.

This talk will discuss the various advances of the past few years and give examples of the progress made.

Synthesis of Concurrent Programs Using Genetic Programming

Doron Peled

Bar Ilan University

Abstract. We present a method to automatically generate concurrent code using genetic programming, based on automatic verification. As the problem of constructing concurrent code is in general undecidable, the user needs to intervene by tuning various parameters and supplying specification and hints that would steer the search for correct code in the right direction. We demonstrate how various hard-to-program protocols are generated using our method and our developed tool. We show how a commonly used protocol for coordinating concurrent interactions was found to be incorrect using our tool, and was then subsequently fixed.

Challenges in Enabling the Next Generation Mobile Experience: Are You Ready?

Scott Runner

Qualcomm

Abstract. In the next decade, consumers are going to be treated to an array of new use case experiences in mobility that one can only dream of today. The HW and SW IP and systems integration that will enable these experiences are prodigious. The design and verification challenges which must be surmounted to enable such high levels of integration and functionality are daunting. And doing so in the timeframes required to satisfy the appetites of smartphone and tablet customers, while delivering to cost, power, performance and quality targets demands novel approaches. We will explore these challenges in the design of the most popular devices in the wireless world.

Table of Contents

Session 1: SAT and SMT-Based Verification

Backbones for Equality	1
<i>Michael Codish, Yoav Fekete, and Amit Metodi</i>	
PASS: String Solving with Parameterized Array and Interval Automaton	15
<i>Guodong Li and Indradeep Ghosh</i>	
Increasing Confidence in Liveness Model Checking Results with Proofs	32
<i>Tuomas Kuusmin and Keijo Heljanko</i>	
Speeding Up the Safety Verification of Programmable Logic Controller Code	44
<i>Tim Lange, Martin R. Neuhäuser, and Thomas Noll</i>	

Session 2: Software Testing I

Modeling Firmware as Service Functions and Its Application to Test Generation	61
<i>Sunha Ahn and Sharad Malik</i>	
Symbolic Model-Based Testing for Industrial Automation Software	78
<i>Sabrina von Styp and Liyong Yu</i>	

Session 3: Software Testing II

Online Testing of LTL Properties for Java Code	95
<i>Paolo Arcaini, Angelo Gargantini, and Elvinia Riccobene</i>	
Modbat: A Model-Based API Tester for Event-Driven Systems	112
<i>Cyrille Valentin Artho, Armin Biere, Masami Hagiya, Eric Platon, Martina Seidl, Yoshinori Tanabe, and Mitsuharu Yamamoto</i>	
Predictive Taint Analysis for Extended Testing of Parallel Executions	129
<i>Emmanuel Sifakis and Laurent Mounier</i>	
Continuous Integration for Web-Based Software Infrastructures: Lessons Learned on the <i>webinos</i> Project	145
<i>Tao Su, John Lyle, Andrea Atzeni, Shamal Faily, Habib Virji, Christos Ntanos, and Christos Botsikas</i>	

Session 4: Supporting Dynamic Verification

SLAM: SLice And Merge - Effective Test Generation for Large Systems	151
<i>Tali Rabetti, Ronny Morad, Alex Goryachev, Wisam Kadry, and Richard D. Peterson</i>	
Improving Post-silicon Validation Efficiency by Using Pre-generated Data	166
<i>Wisam Kadry, Anatoly Koyfman, Dmitry Krestyashyn, Shimon Landa, Amir Nahir, and Vitali Sokhin</i>	
Development and Verification of Complex Hybrid Systems Using Synthesizable Monitors	182
<i>Andreas Abel, Allon Adir, Torsten Blochwitz, Lev Greenberg, and Tamer Salman</i>	
Assertion Checking Using Dynamic Inference	199
<i>Anand Yeolekar and Divyesh Unadkat</i>	

Session 5: Specification and Coverage

Formal Specification of an Erase Block Management Layer for Flash Memory	214
<i>Jörg Pfähler, Gidon Ernst, Gerhard Schellhorn, Dominik Haneberg, and Wolfgang Reif</i>	
Attention-Based Coverage Metrics	230
<i>Shoham Ben-David, Hana Chockler, and Orna Kupferman</i>	

Keynote Presentation

Synthesizing, Correcting and Improving Code, Using Model Checking-Based Genetic Programming	246
<i>Gal Katz and Doron Peled</i>	

Session 6: Abstraction

Domain Types: Abstract-Domain Selection Based on Variable Usage ...	262
<i>Sven Apel, Dirk Beyer, Karlheinz Friedberger, Franco Raimondi, and Alexander von Rhein</i>	
Efficient Analysis of Reliability Architectures via Predicate Abstraction	279
<i>Marco Bozzano, Alessandro Cimatti, and Cristian Mattarei</i>	
Lazy Symbolic Execution through Abstraction and Sub-space Search ...	295
<i>Guodong Li and Indradeep Ghosh</i>	

SPIN as a Linearizability Checker under Weak Memory Models	311
<i>Oleg Travkin, Annika Mütze, and Heike Wehrheim</i>	

Session 7: Model Representation

Arithmetic Bit-Level Verification Using Network Flow Model	327
<i>Maciej Ciesielski, Walter Brown, and André Rossi</i>	
Performance Evaluation of Process Partitioning Using Probabilistic Model Checking	344
<i>Saddek Bensalem, Borzoo Bonakdarpour, Marius Bozga, Doron Peled, and Jean Quilbeuf</i>	
Improving Representative Computation in ExpliSAT	359
<i>Hana Chockler, Dmitry Pidan, and Sitvanit Ruah</i>	
Author Index	365