Preface

This volume contains the proceedings of the 10th Haifa Verification Conference (HVC 2014). The conference was hosted by IBM Research - Haifa and took place during November 18–20, 2014. It was the tenth 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.

Overall, HVC 2014 attracted 43 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 external experts. The Program Committee selected 21 papers for presentation.

In addition to the 21 contributed papers, the program included five invited talks by Moshe Vardi (Rice University), Bradley McCredie (IBM), Martin Vechev (ETH Zurich), Harry Foster (Mentor Graphics), and Ziv Binyamini (Cadence).

I would like to extend our appreciation and sincere thanks to Ronny Morad for serving as general chair and handling the conference details. Our thanks also go to Raviv Gal for arranging the tutorials day, and Rachel Tzoref-Brill for serving as the publicity chair. I would like to thank the Organizing Committee: Moshe Levinger, Laurent Fournier, Amir Nahir, Karen Yorav, Avi Ziv, and Sharon Keidar Barner.

Finally, I would like to thank our support team: Eti Jahr for managing the technical aspects of the conference, and Gili Aizen and Chani Sacharen handling communication.

HVC 2014 received sponsorships from IBM, Cadence, Mellanox, Mentor Graphics, Qualcomm, SanDisk, and Technion TCE.

Submissions and evaluations of papers, as well as the preparation of this proceedings volume, were handled by the EasyChair conference management system.

October 2014

Eran Yahav
Organization

Program Committee

Earl Barr  University College London, UK
Valeria Bertacco  University of Michigan, USA
Tevfik Bultan  University of California at Santa Barbara, USA
Swarat Chaudhuri  Rice University, USA
Hana Chockler  King’s College, UK
Isil Dillig  UT Austin, USA
Kerstin Eder  University of Bristol, UK
Franco Fummi  University of Verona, Italy
Patrice Godefroid  Microsoft Research
Aarti Gupta  NEC Laboratories America
Barbara Jobstmann  EPFL, Jasper DA, and CNRS-Verimag, France
Laura Kovacs  Chalmers University of Technology, Sweden
Daniel Kroening  University of Oxford, UK
Florian Letombe  Synopsys
João Lourenço  CITI - Universidade Nova de Lisboa, Portugal
Shan Lu  University of Wisconsin, Madison, USA
Rupak Majumdar  MPI-SWS
Darko Marinov  University of Illinois at Urbana-Champaign, USA

Mayur Naik  Intel Labs
Aditya Nori  MSR India
Corina Pasareanu  CMU/NASA Ames Research Center, USA
Ruzica Piskac  Yale University, USA
Itai Segall  IBM Haifa Research Labs, Israel
Martina Seidl  Johannes Kepler University Linz, Austria
Ohad Shacham  Yahoo! Labs
Sharon Shoham  Academic College of Tel Aviv Yaffo, Israel
Zhendong Su  UC Davis, USA
Rachel Tzoref  IBM Haifa Research Labs, Israel
Jan Vitek  Purdue University, USA
Heike Wehrheim  University of Paderborn, Germany

Additional Reviewers

Bocic, Ivan  Dimitrova, Rayna
Busany, Nimrod  Dragan, Ioan
Chakarov, Aleksandar  Ferreira, Bernardo
Cobb, Jake  Forejt, Vojtech
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fu, Zhoulai</td>
<td>Parikh, Ritesh</td>
</tr>
<tr>
<td>Gabmeyer, Sebastian</td>
<td>Qiu, Rui</td>
</tr>
<tr>
<td>Grumberg, Orna</td>
<td>Rinetzky, Noam</td>
</tr>
<tr>
<td>Gyori, Alex</td>
<td>Ringert, Jan Oliver</td>
</tr>
<tr>
<td>Heule, Marijn</td>
<td>Schäf, Martin</td>
</tr>
<tr>
<td>Horn, Alexander</td>
<td>Sen, Shayak</td>
</tr>
<tr>
<td>Isenberg, Tobias</td>
<td>Shi, August</td>
</tr>
<tr>
<td>Itzhaky, Shachar</td>
<td>Sun, Chengnian</td>
</tr>
<tr>
<td>Joshi, Saurabh</td>
<td>Tentrup, Leander</td>
</tr>
<tr>
<td>Karbyshev, Aleksandr</td>
<td>Torfah, Hazem</td>
</tr>
<tr>
<td>Kloos, Johannes</td>
<td>Van Delft, Bart</td>
</tr>
<tr>
<td>Konnov, Igor</td>
<td>van Den Elsen, Susanne</td>
</tr>
<tr>
<td>Kuncak, Viktor</td>
<td>Vizel, Yakir</td>
</tr>
<tr>
<td>Landsberg, David</td>
<td>Wachter, Björn</td>
</tr>
<tr>
<td>Le, Vu</td>
<td>Yahav, Eran</td>
</tr>
<tr>
<td>Legunsen, Owolabi</td>
<td>Yorav, Karen</td>
</tr>
<tr>
<td>Mangal, Ravi</td>
<td>Zhang, Xin</td>
</tr>
<tr>
<td>Maoz, Shahar</td>
<td>Ziegert, Steffen</td>
</tr>
<tr>
<td>Milicevic, Aleksandar</td>
<td>Ziv, Avi</td>
</tr>
</tbody>
</table>
Abstracts
SAT Counting and Sampling - From Theory to Practice

Moshe Vardi

Rice University

Abstract. Counting the the number of satisfying truth assignments of a given Boolean formula or sampling such assignments uniformly at random are fundamental computational problems in computer science with numerous applications. In computer-aided design, these problems come up in constrained-random verification, where test input vectors are described by means of constraints. While the theory of these problems has been thoroughly investigated in the 1980s, approximation algorithms developed by theoreticians do not scale up to industrial-sized instances. Algorithms used by the industry offer better scalability, but give up certain correctness guarantees to achieve scalability. We describe a novel approach, based on universal hashing and SMT, that scales to formulas with hundreds of thousands of variable without giving up correctness guarantees.

Joint work with Supratik Chaudhuri, Daniel Fremont, Kuldeep Meel, and Sanjit Sheshia.
Statistical Program Analysis and Synthesis

Martin Vechev

Department of Computer Science
ETH Zurich

Abstract. The increased availability of massive codebases, sometimes referred to as “Big Code”, creates a unique opportunity for new kinds of program analysis and synthesis techniques based on statistical reasoning. These approaches will extract useful information from existing codebases and will use that information to provide statistically likely solutions to problems that are difficult or impossible to solve with traditional techniques.

As an example, I will present several statistical engines developed in our lab which instantiate this vision. I will highlight the key challenges when designing such systems including the importance of carefully combining and interfacing programming language techniques (e.g. static analysis) with powerful machine learning approaches (e.g. graphical models).
Navigating the Perfect Storm: New Trends in Functional Verification

Harry Foster
Mentor Graphics

Abstract. Between 2006 and 2014, the average number of IPs integrated into an advanced SoC increased from about 30 to over 120. In the same period, the average number of embedded processors found in an advanced SoC increased from one to as many as 20. However, increased design size is only one dimension of the growing verification complexity challenge. Beyond this growing functionally phenomenon are new layers of requirements that must be verified. Many of these verification requirements did not exist ten years ago, such as multiple asynchronous clock domains, interacting power domains, security domains, and complex HW/SW dependencies. Add all these challenges together, and you have the perfect storm brewing. This talk introduces today’s trends and challenges in SoC design and then discusses emerging verification strategy to navigate the perfect storm.
# Table of Contents

Using Coarse-Grained Abstractions to Verify Linearizability on TSO Architectures ................................................................. 1  
\textit{John Derrick, Graeme Smith, Lindsay Groves, and Brijesh Dongol}

Enhancing Scenario Quality Using Quasi-Events ....................... 17  
\textit{Yoav Katz, Eitan Marcus, and Avi Ziv}

Combined Bounded and Symbolic Model Checking for Incomplete Timed Systems ................................................................. 30  
\textit{Georges Morbé, Christian Miller, Christoph Scholl, and Bernd Becker}

DynaMate: Dynamically Inferring Loop Invariants for Automatic Full Functional Verification .................................................. 48  
\textit{Juan Pablo Galeotti, Carlo A. Furia, Eva May, Gordon Fraser, and Andreas Zeller}

Generating Modulo-2 Linear Invariants for Hardware Model Checking ................................................................. 54  
\textit{Gadi Aleksandrowicz, Alexander Ivrii, Oded Margalit, and Dan Rasin}

Suraq — A Controller Synthesis Tool Using Uninterpreted Functions ... 68  
\textit{Georg Hofferek and Ashutosh Gupta}

Synthesizing Finite-State Protocols from Scenarios and Requirements ... 75  
\textit{Rajeev Alur, Milo Martin, Mukund Raghothaman, Christos Stergiou, Stavros Tripakis, and Abhishek Udupa}

Automatic Error Localization for Software Using Deductive Verification ............................................................................... 92  
\textit{Robert Könighofer, Ronald Toegl, and Roderick Bloem}

Generating JML Specifications from Alloy Expressions ................. 99  
\textit{Daniel Grunwald, Christoph Gladisch, Tianhai Liu, Mana Taghdiri, and Shmuel Tyszberowicz}

Assume-Guarantee Abstraction Refinement Meets Hybrid Systems .......... 116  
\textit{Sergiy Bogomolov, Goran Frehse, Marius Greitschus, Radu Grosu, Corina Pasareanu, Andreas Podelski, and Thomas Strump}

Handling TSO in Mechanized Linearizability Proofs .................... 132  
\textit{Oleg Travkin and Heike Wehrheim}

Partial Quantifier Elimination ..................................................... 148  
\textit{Eugene Goldberg and Panagiotis Manolios}
Formal Verification of 800 Genetically Constructed Automata Programs: A Case Study .................................................. 165
  Mikhail Lukin, Maxim Buzdalov, and Anatoly Shalyto

A Framework to Synergize Partial Order Reduction with State Interpolation ......................................................... 171
  Duc-Hiep Chu and Joxan Jaffar

Reduction of Resolution Refutations and Interpolants via Subsumption ................................................................. 188
  Roderick Bloem, Sharad Malik, Matthias Schlaipfer, and Georg Weissenbacher

Read, Write and Copy Dependencies for Symbolic Model Checking ................................................................. 204
  Jeroen Meijer, Gijs Kant, Stefan Blom, and Jaco van de Pol

Efficient Combinatorial Test Generation Based on Multivalued Decision Diagrams ..................................................... 220
  Angelo Gargantini and Paolo Vavassori

Formal Verification of Secure User Mode Device Execution with DMA .............................................................. 236
  Oliver Schwarz and Mads Dam

Supervisory Control of Discrete-Event Systems via IC3 ................................................................. 252
  Mohammad Reza Shoaei, Laura Kovács, and Bengt Lennartson

Partial-Order Reduction for Multi-core LTL Model Checking ................................................................. 267
  Alfons Laarman and Anton Wijs

A Comparative Study of Incremental Constraint Solving Approaches in Symbolic Execution ........................................ 284
  Tianhai Liu, Mateus Araújo, Marcelo d’Amorim, and Mana Taghdiri

Author Index ................................................................. 301