

*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*

Kerstin Eder João Lourenço  
Onn Shehory (Eds.)

# Hardware and Software: Verification and Testing

7th International

Haifa Verification Conference, HVC 2011

Haifa, Israel, December 6-8, 2011

Revised Selected Papers



Springer

## Volume Editors

Kerstin Eder

University of Bristol, Department of Computer Science  
Merchant Venturers Building 3.25, Woodland Road, Bristol BS8 1UB, UK  
E-mail: kerstin.eder@bristol.ac.uk

João Lourenço

NOVA University of Lisbon, Department of Computer Science and Engineering  
FCT-UNL, Quinta da Torre, 2829-516 Caparica, Portugal  
E-mail: joao.lourenco@fct.unl.pt

Onn Shehory

IBM Research Labs at Haifa  
Haifa University Campus, Mount Carmel, Haifa 31905, Israel  
E-mail: onn@il.ibm.com

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-34187-8

e-ISBN 978-3-642-34188-5

DOI 10.1007/978-3-642-34188-5

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012950042

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-Verlag Berlin Heidelberg 2012

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.

The use of general descriptive names, registered names, trademarks, 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.

*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 papers presented at the Haifa Verification Conference 2011, the 7th in the series of annual conferences dedicated to advancing the state of the art and state of the practice in verification and testing of hardware and software. HVC provides a forum for researchers and practitioners from both academia and industry to share their work, exchange ideas, and discuss challenges and future directions of testing and verification for hardware, software, and hybrid systems.

Academic research in system verification and testing is roughly divided into two major paradigms: formal verification and dynamic verification (testing). Within each paradigm, algorithms, techniques and even terminology may differ considerably between hardware-related solutions and software-related solutions. However, the common underlying goal of verification, across paradigms and system types, is to gain confidence in a system meeting its functional as well as its non-functional requirements. HVC is the only conference that brings together researchers and practitioners from all verification and testing sub-fields, thereby encouraging the migration of methods and ideas among domains. One key asset of HVC is the strong participation from industry. HVC provides a platform for the academic and industrial research communities to mix and mingle, thereby creating new opportunities for collaborative research. We are particularly proud to say that the papers selected for presentation at HVC 2011 covered a wide range of sub-fields related to testing and verification applicable to software, hardware, and hybrid systems, thus stimulating discussion within the wider verification community.

From a total of 43 submissions, the Program Committee selected 15 regular papers for full presentation, three tools papers for short presentation, and four posters for the student poster session on day one of the conference. HVC 2011 was organized in five technical sessions devoted to topics including synthesis, formal verification, software quality, testing, and coverage. The best paper selection jury considered both the quality of the technical paper as well as the presentation at the conference. The best paper prize was awarded to Marijn Heule, Oliver Kullmann, Siert Wieringa, and Armin Biere for their paper entitled “Cube and Conquer: Guiding CDCL SAT Solvers by Lookaheads.”

Granted since 2007, the HVC award recognizes the most promising academic and industrial contribution to the fields of testing and software and hardware verification from the last five years. The HVC 2011 award went to Daniel Kroening from Oxford for his contribution of CBMC, a bounded model checker for C programs. CBMC is the first and most influential industrial-strength verification engine for a non-academic programming language, and hence a major milestone in automated verification. To date, CBMC is the only verification engine that supports the full functionality of C, including precise modeling of floating-point

operations and bit-precise arithmetic. CBMC promotes the industrial adoption of formal software verification more than any other tool in existence and is therefore a significant contribution to the verification community.

The conference was hosted by IBM at the IBM Research Labs in Haifa. We would like to thank all who made HVC 2011 run smoothly and gratefully acknowledge the invaluable support by many on the IBM administrative team, without which this event could not meet its goals and match the high standards established over the years. We would like to thank the Program Committee, the HVC Award Committee, the Best Paper Prize Jury, the authors of all submissions to HVC 2011 and, of course, the presenters of the papers and posters accepted. All these contributed toward making HVC 2011 another success in the HVC conference series. We would also like to thank the tutorial presenters Avner Engel, Ofer Strichman, and Rachel Tzoref-Brill for an informative first day prior to the main conference. Special thanks are due to our invited speakers who enriched the program with insightful and inspiring presentations: Kathryn Krannen, Jasper Design Automation, Ben Liblit, University of Wisconsin-Madison, Klaus-Dieter Schubert, IBM Deutschland Research and Development GmbH, and Armin Biere, Johannes Kepler University, Linz.

Finally, we would like to thank our sponsors, IBM, Cadence, Mentor Graphics, and Jasper Design Automation, for their generous support in preparation and throughout the event.

July 2012

Kerstin Eder  
João Lourenço  
Onn Shehory

# Organization

## General Chair

Onn Shehory                      IBM Haifa Labs, Israel

## Program Chairs

Kerstin Eder                      University of Bristol, UK    (Verification Track)  
João Lourenço                  New University of Lisbon, (Software Testing Track)  
   Portugal

## Tutorials Chair

Oz HersHKovitz                IBM Haifa Labs, Israel

## Local Organization

Yair Harry                      IBM Haifa Labs, Israel    (Webmaster)  
Shirley Namer                IBM Haifa Labs, Israel    (Local Logistics)  
Onn Shehory                IBM Haifa Labs, Israel    (Coordinator)

## Program Committee

Sharon Barner                IBM Haifa Labs, Israel  
Geoff Barrett                Broadcom, UK  
Armin Biere                  Institute for Formal Models and Verification, Austria  
Eyal Bin                      IBM Haifa Labs, Israel  
Roderick Bloem              Graz University of Technology, Austria  
Michael Browne              IBM, USA  
Michael Butler              University of Southampton, UK  
Radu Calinescu              University of Aston, UK  
Hana Chockler              IBM Haifa Labs, Israel  
Kerstin Eder                University of Bristol, UK  
Eitan Farchi                IBM Haifa Labs, Israel  
Harry Foster                Mentor Graphics, USA  
Franco Fummi              University of Verona, Italy  
Ian G. Harris                University of California Irvine, USA  
Ziyad Hanna                Jasper DA, USA  
Klaus Havelund              JPL, USA  
Alan Hu                      University of British Columbia, USA  
Mika Katara                Tampere University of Technology, Finland  
Zurab Khasidashvili        Intel, Israel

## VIII Organization

Tsvi Kuflik	University of Haifa, Israel
Mark Last	Ben Gurion University, Israel
João Lourenço	New University of Lisbon, Portugal
Tom Melham	Oxford University, UK
Amir Nahir	IBM Haifa Labs, Israel
Mauro Pezze	University of Lugano, Switzerland, and University of Milano Bicocca, Italy
Orna Raz	IBM Haifa Labs, Israel
Michael S. Hsiao	VirginiaTech, USA
Wolfram Schulte	Microsoft Research, USA
Onn Shehory	IBM Haifa Labs, Israel
Armando Tacchella	University of Genova, Italy
Helen Treharne	University of Surrey, UK
Shmuel Ur	Innovations Ltd., Israel
Helmut Veith	Vienna University of Technology, Austria
Heike Wehrheim	Paderborn University, Germany

## HVC Award Committee

Shmuel Ur	Innovations Ltd., Israel (Chair)
Ian G. Harris	University of California Irvine, USA
Klaus Havelund	JPL, USA
Mika Katara	Tampere University of Technology, Finland
Ofer Strichman	Technion, Israel

## Additional Referees

Sam Bayless	Yael Meller
Christian Bird	Madanlal Musuvathi
John Colley	Ziv Nevo
Chris Derobertis	Avigail Orni
Ricardo Dias	Andrey Rybalchenko
Andrew Edmunds	Alexander Schremmer
Cindy Eisner	Carl Seger
Ranan Fraer	Martina Seidl
Jim Grundy	Dominik Steenken
Georg Hofferek	Dorian Thomas
Andreas Holzer	Rachel Tzoref-Brill
Alexander Ivrii	Heikki Virtanen
Kenneth Johnson	Matti Vuori
Antti Jääskeläinen	Sven Walther
Robert Koenighofer	Nick Wiggins
Dmitry Korchemny	Chao Yan
Anatoly Koyfman	

# Table of Contents

## Invited Talks

Preprocessing and Inprocessing Techniques in SAT .....	1
<i>Armin Biere</i>	
Pioneering the Future of Verification: A Spiral of Technological and Business Innovation .....	2
<i>Kathryn Kranen</i>	
Automated Detection and Repair of Concurrency Bugs .....	3
<i>Ben Liblit</i>	
Verification Challenges of Workload Optimized Hardware Systems .....	4
<i>Klaus-Dieter Schubert</i>	

## Synthesis

Synthesis with Clairvoyance .....	5
<i>Orna Kupferman, Dorsa Sadigh, and Sanjit A. Seshia</i>	
Generalized Reactivity(1) Synthesis without a Monolithic Strategy .....	20
<i>Matthias Schlaipfer, Georg Hofferek, and Roderick Bloem</i>	

## Formal Verification

IIS-Guided DFS for Efficient Bounded Reachability Analysis of Linear Hybrid Automata .....	35
<i>Lei Bu, Yang Yang, and Xuandong Li</i>	
Cube and Conquer: Guiding CDCL SAT Solvers by Lookaheads .....	50
<i>Marijn J.H. Heule, Oliver Kullmann, Siert Wieringa, and Armin Biere</i>	
Implicative Simultaneous Satisfiability and Applications .....	66
<i>Zurab Khasidashvili and Alexander Nadel</i>	
Liveness vs Safety – A Practical Viewpoint .....	80
<i>B.A. Krishna, Jonathan Michelson, Vigyan Singhal, and Alok Jain</i>	
Predicting Serializability Violations: SMT-Based Search vs. DPOR-Based Search .....	95
<i>Arnab Sinha, Sharad Malik, Chao Wang, and Aarti Gupta</i>	



## Software Quality

SAM: Self-adaptive Dynamic Analysis for Multithreaded Programs . . . . .	115
<i>Qichang Chen, Liqiang Wang, and Zijiang Yang</i>	
Concurrent Small Progress Measures . . . . .	130
<i>Michael Huth, Jim Huan-Pu Kuo, and Nir Piterman</i>	
Specification and Quantitative Analysis of Probabilistic Cloud Deployment Patterns . . . . .	145
<i>Kenneth Johnson, Simon Reed, and Radu Calinescu</i>	
Interpolation-Based Function Summaries in Bounded Model Checking . . . . .	160
<i>Ondrej Sery, Grigory Fedyukovich, and Natasha Sharygina</i>	
Can File Level Characteristics Help Identify System Level Fault-Proneess? . . . . .	176
<i>Thomas J. Ostrand and Elaine J. Weyuker</i>	

## Testing and Coverage

Reverse Coverage Analysis . . . . .	190
<i>Ariel Birnbaum, Laurent Fournier, Steve Mittermaier, and Avi Ziv</i>	
Symbolic Testing of OpenCL Code . . . . .	203
<i>Peter Collingbourne, Cristian Cadar, and Paul H.J. Kelly</i>	
Dynamic Test Data Generation for Data Intensive Applications . . . . .	219
<i>Allon Adir, Ronen Levy, and Tamer Salman</i>	

## Experience and Tools

Injecting Floating-Point Testing Knowledge into Test Generators . . . . .	234
<i>Merav Aharony, Emanuel Gofman, Elena Guralnik, and Anatoly Koyfman</i>	
Combining Theorem Proving and Symbolic Trajectory Evaluation in THM&STE . . . . .	242
<i>Yongjian Li, Naiju Zeng, William N.N. Hung, and Xiaoyu Song</i>	
HAVEN: An Open Framework for FPGA-Accelerated Functional Verification of Hardware . . . . .	247
<i>Marcela Šímková, Ondřej Lengál, and Michal Kajan</i>	

**Posters – Student Event**

On-Line Detection and Prediction of Temporal Patterns . . . . .	254
<i>Shlomi Dolev, Jonathan Goldfeld, and Rami Puzis</i>	
Function Summaries in Software Upgrade Checking . . . . .	257
<i>Grigory Fedyukovich, Ondrej Sery, and Natasha Sharygina</i>	
The Rabin Index of Parity Games (Extended Abstract) . . . . .	259
<i>Michael Huth, Jim Huan-Pu Kuo, and Nir Piterman</i>	
Using Computational Biology Methods to Improve Post-silicon Microprocessor Testing . . . . .	261
<i>Ron Zeira, Dmitry Korchemny, and Ron Shamir</i>	
<b>Author Index</b> . . . . .	263