

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

Armin Biere Amir Nahir Tanja Vos (Eds.)

Hardware and Software: Verification and Testing

8th International

Haifa Verification Conference, HVC 2012

Haifa, Israel, November 6-8, 2012

Revised Selected Papers



Springer

Volume Editors

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

Amir Nahir
IBM Research Laboratory, 31905 Haifa, Israel
E-mail: nahir@il.ibm.com

Tanja Vos
Universidad Politecnica de Valencia, 46022 Valencia, Spain
E-mail: tvos@dsic.upv.es

ISSN 0302-9743
ISBN 978-3-642-39610-6
DOI 10.1007/978-3-642-39611-3
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-39611-3

Library of Congress Control Number: 2013943016

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 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 Haifa Verification Conference (HVC 2012). The conference was hosted by IBM Research Haifa and took place during November 6–8, in 2012. It was the eighth event in this series of annual conferences dedicated to advancing the state of the art and state of 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. In 2012, HVC extended the traditional focus on hardware and software verification to include verification, validation, and testing (VVT) of complex hybrid systems as a part of the systems-engineering paradigm.

The Intel DTS Symposium and a meeting of the COST Action IC0901 Rich-Model Toolkit were co-located events. The conference itself started with a tutorial day including “Idiom-Based Verification of Highly Concurrent Data Structures Using Temporal Separation Logic” by Noam Rinetzky, “Three-Valued Abstraction-Refinement” by Sharon Shoham Buchbinder, “Simulating Cyber-Physical Systems Using SysML and Numerical Simulation Tools” by Eldad Palachi, and on “Improving Verification Productivity with the Dynamic Load and Reseed Methodology” by Marat Teplitsky.

The Program Committee accepted 18 regular papers out of 36 submissions, whose post-conference versions are published in this volume. The conference chairs further selected three poster presentations out of four poster submissions submitted after the notification for regular papers.

The conference featured a keynote with the title “On Behavioral Programming” by David Harel and another keynote talk on “Verifying Real-Time Software Is Not Reasonable (Today)” by Edward Lee. There were two invited talks on “Reducing Costs While Increasing Quality” by Orna Raz and on “SMT in Verification, Modeling, and Testing at Microsoft” by Nikolaj Bjorner. The last day contained a session on security verification with talks on “A Vulnerability or a Bug? What’s the Difference Anyway? Security Software Verification as Part of the Development Lifecycle” by Ofer Maor, another talk on “Formal Analysis of Security Data Paths in RTL Design” by Jamil Mazzawi, and a third presentation on “Simultaneous Information Flow Security and Circuit Redundancy in Boolean Gates” by Ryan Kastner.

The HVC Award, granted since 2007, 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 2012 Award Committee, chaired by Daniel Kroening, decided to give the 2012 award to Aaron R. Bradley of CU Boulder for the invention of the IC3 algorithm. Aaron Bradley gave the award talk on the last day of the conference.

The Best Paper was selected by the Conference Chairs and awarded to Vasco Pessanha, Ricardo Dias, and João Lourenço for their paper with entitled “Precise Detection of Atomicity Violations.”

The Conference Chairs would like to thank the members of the Program Committee for their hard work reading the papers and writing reviews under a very tight schedule during essentially one month in July and August 2012.

We are very grateful to IBM Research – Haifa for hosting and sponsoring HVC 2012.

April 2013

Armin Biere
Amir Nahir
Tanja Vos

Organization

Program Committee

Cyrille Valentin Artho	AIST, Japan
Armin Biere	Johannes Kepler University Linz, Austria
Roderick Bloem	Graz University of Technology, Austria
Radu Calinescu	Aston University, UK
Hana Chockler	IBM Research - Haifa, Israel
Kerstin Eder	University of Bristol, UK
Maria Jose Escalona	University of Seville, Spain
Eitan Farchi	IBM Research - Haifa, Israel
Harry Foster	Mentor Graphics, USA
Franco Fummi	University of Verona, Italy
Alex Goryachev	IBM Research - Haifa, Israel
Ziyad Hanna	University of Oxford, UK
Mark Harman	University College London, UK
Ian Harris	University of California Irvine, USA
Klaus Havelund	Jet Propulsion Laboratory, USA
Michael Hsiao	Virginia Tech, USA
Alan Hu	University of British Columbia, Canada
Zurab Khasidashvili	Intel, Israel
Mark Last	Ben-Gurion University, Israel
João Lourenço	CITI - Universidade Nova de Lisboa, Portugal
Ken Mcmillan	Cadence Berkeley Labs, USA
Thomas Melham	Oxford University, UK
Amir Nahir	IBM Research - Haifa, Israel
Martina Seidl	Johannes Kepler University Linz, Austria
Onn Shehory	IBM Research - Haifa, Israel
Armando Tacchella	Università di Genova, Italy
Helen Treharne	University of Surrey, UK
Shmuel Ur	Consultant, Israel
Helmut Veith	Vienna University of Technology, Austria
Tanja Vos	Researcher, Spain
Li-C Wang	University of California Santa Barbara, USA
Joachim Wegener	Berner & Mattner, Germany
Heike Wehrheim	University of Paderborn, Germany

Additional Reviewers

Baars, Arthur
Bustan, Doron
Chen, Wen
Egly, Uwe
Finkbeiner, Bernd
Heljanko, Keijo
Heule, Marijn
Hjort, Hakan
Hofferek, Georg
Ivrii, Alexander
Jacobs, Swen
Johnson, Kenneth

Kikuchi, Shinji
Koenighofer, Bettina
Koenighofer, Robert
Korchemny, Dmitry
Nadel, Alexander
Ryvchin, Vadim
Schremmer, Alexander
Sinn, Moritz
Steenken, Dominik
Timm, Nils
Vizel, Yakir
Wolfovitz, Guy

Table of Contents

On Behavioral Programming	1
<i>David Harel</i>	
Verifying Real-Time Software Is Not Reasonable (Today)	2
<i>Edward A. Lee</i>	
SMT in Verification, Modeling, and Testing at Microsoft	3
<i>Nikolaj Bjørner</i>	
Reducing Costs While Increasing Quality	4
<i>Orna Raz</i>	
Special Session on Security Verification	5
<i>Alex Goryachev</i>	
Circuit Primitives for Monitoring Information Flow and Enabling Redundancy	6
<i>Ryan Kastner</i>	
Formal Analysis of Security Data Paths in RTL Design	7
<i>Jamil Mazzawi and Ziyad Hanna</i>	
Precise Detection of Atomicity Violations	8
<i>Ricardo J. Dias, Vasco Pessanha, and João M. Lourenço</i>	
Proving Mutual Termination of Programs	24
<i>Dima Elenbogen, Shmuel Katz, and Ofer Strichman</i>	
Knowledge Based Transactional Behavior	40
<i>Saddek Bensalem, Marius Bozga, Doron Peled, and Jean Quilbeuf</i>	
Repair with On-The-Fly Program Analysis	56
<i>Robert Könighofer and Roderick Bloem</i>	
Computing Interpolants without Proofs	72
<i>Hana Chockler, Alexander Ivrii, and Arie Matsliah</i>	
MaxSAT-Based MCS Enumeration	86
<i>Antonio Morgado, Mark Liffiton, and Joao Marques-Silva</i>	
Automated Reencoding of Boolean Formulas	102
<i>Norbert Manthey, Marijn J.H. Heule, and Armin Biere</i>	

Leveraging Accelerated Simulation for Floating-Point Regression	118
<i>John Paul, Elena Guralnik, Anatoly Koyfman, Amir Nahir, and Subrat K. Panda</i>	
Coverage-Based Trace Signal Selection for Fault Localisation in Post-silicon Validation	132
<i>Charlie Shucheng Zhu, Georg Weissenbacher, and Sharad Malik</i>	
A Novel Approach for Implementing Microarchitectural Verification Plans in Processor Designs	148
<i>Yoav Katz, Michal Rimon, and Avi Ziv</i>	
Statistical Model Checking for Safety Critical Hybrid Systems: An Empirical Evaluation	162
<i>Youngjoo Kim, Moonzoo Kim, and Tai-Hyo Kim</i>	
A New Test-Generation Methodology for System-Level Verification of Production Processes	178
<i>Allon Adir, Alex Goryachev, Lev Greenberg, Tamer Salman, and Gil Shurek</i>	
Defining and Model Checking Abstractions of Complex Railway Models Using CSP B	193
<i>Faron Moller, Hoang Nga Nguyen, Markus Roggenbach, Steve Schneider, and Helen Treharne</i>	
Word Equations with Length Constraints: What's Decidable?	209
<i>Vijay Ganesh, Mia Minnes, Armando Solar-Lezama, and Martin Rinard</i>	
Environment-Friendly Safety	227
<i>Orna Kupferman and Sigal Weiner</i>	
Deterministic Compilation of Temporal Safety Properties in Explicit State Model Checking	243
<i>Kristin Yvonne Rozier and Moshe Y. Vardi</i>	
FoREnSiC– An Automatic Debugging Environment for C Programs	260
<i>Roderick Bloem, Rolf Drechsler, Görschwin Fey, Alexander Finder, Georg Hofferek, Robert Könighofer, Jaan Raik, Urmaz Repinski, and André Süßflow</i>	
Towards Beneficial Hardware Acceleration in HAVEN: Evaluation of Testbed Architectures	266
<i>Marcela Šimková and Ondřej Lengál</i>	
Using Domain Specific Languages to Support Verification in the Railway Domain	274
<i>Phillip James, Arnold Beckmann, and Markus Roggenbach</i>	

From Fault Injection to Mutant Injection: The Next Step for Safety Analysis?	276
<i>Guillermo Rodriguez-Navas, Patrick Graydon, and Iain Bate</i>	
Test Case Generation by Grammar-Based Fuzzing for Model-Driven Engineering	278
<i>Magdalena Widl</i>	
Author Index	281