Lecture Notes in Computer Science 6996

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Tevfik Bultan Pao-Ann Hsiung (Eds.)

Automated Technology for Verification and Analysis

9th International Symposium, ATVA 2011
Taipei, Taiwan, October 11-14, 2011
Proceedings

Springer

Volume Editors

Tevfik Bultan
University of California, Department of Computer Science
Santa Barbara, CA 93106-5110, USA
E-mail: bultan@cs.ucsb.edu

Pao-Ann Hsiung
National Chung Cheng University
Department of Computer Science and Information Engineering
168 University Road, Min-Hsiung, Chiayi, Taiwan–62102, ROC
E-mail: pahsiung@cs.ccu.edu.tw

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-24371-4 e-ISBN 978-3-642-24372-1
DOI 10.1007/978-3-642-24372-1
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011936735

CR Subject Classification (1998): D.2, D.1, F.3, C.2, D.3, C.2.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

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 International Symposium on Automated Technology for Verification and Analysis (ATVA) held during October 11–14, 2011 in Taipei, Taiwan. The goal of the ATVA conferences is to promote research on theoretical and practical aspects of automated analysis, verification and synthesis by providing a forum for interaction between the regional and the international research communities and industry in the field.

There were 75 papers submitted to ATVA 2011, and among these the Program Committee accepted 23 regular papers, 2 tool papers and 11 short papers. Each paper received at least three reviews which was followed by an online discussion conducted using the EasyChair system. In addition to the presentation of the accepted papers, the ATVA 2011 program included three keynote talks and tutorials by Edmund M. Clarke (Carnegie Mellon University, USA), Orna Kupferman (Hebrew University, Israel) and Daniel Kroening (Oxford University, UK), as well as two invited talks by Masahiro Fujita (University of Tokyo, Japan) and Moonzoo Kim (KAIST, Korea), resulting in an exceptionally strong technical program of the highest quality.

ATVA 2011 was co-located with the Infinity Workshop (co-chaired by Fang Yu and Chao Wang) and the Embedded Systems Week which consisted of three leading conferences: International Conference on Compilers, Architectures and Synthesis of Embedded Systems (CASES), International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), and the International Conference on Embedded Software (EMSOFT). The co-location of these events created a unique environment for interaction among many researchers from a variety of areas which contributed to the success of ATVA 2011.

We would like to acknowledge the contributions that made ATVA 2011 a successful event. First, we would like to thank all the authors who submitted their work to ATVA and we hope that they continue to submit their high-quality work to ATVA in future years. We thank the Program Committee members and the external reviewers for their hard work in providing a rigorous and fair evaluation of each submission, and providing detailed comments and feedback to help authors improve their work. We are very grateful to the keynote and invited speakers for enriching the symposium by presenting their distinguished and internationally recognized research. We would like to thank the Steering Committee members for their guidance. We would like to thank the ATVA 2011

General Chair Hsu-Chun Yen and ATVA 2011 Local Arrangements Chair Farn Wang. Their contributions were crucial in making ATVA 2011 a successful event. Finally, we would like to thank the institutions that sponsored ATVA 2011.

We are proud of the quality of the ATVA 2011 proceedings and we sincerely hope that the readers find them informative and rewarding.

July 2011

Tevfik Bultan
Pao-Ann Hsiung

Organization

General Chair

Hsu-Chun Yen	National Taiwan University, Taiwan

Program Chairs

Tevfik Bultan	University of California at Santa Barbara, USA
Pao-Ann Hsiung	National Chung Cheng University, Taiwan

Program Committee

Parosh Abdulla	Uppsala University, Sweden
Samik Basu	Iowa State University, USA
Bernard Boigelot	University of Liege, Belgium
Ahmed Bouajjani	University of Paris Diderot, France
Swarat Chaudhuri	Pennsylvania State University, USA
Alessandro Cimatti	FBK-IRST, Italy
E. Allen Emerson	University of Texas at Austin, USA
Xiang Fu	Hofstra University, USA
Masahiro Fujita	University of Tokyo, Japan
Patrice Godefroid	Microsoft Research, USA
Susanne Graf	Verimag Laboratory, France
Holger Hermanns	Saarland University, Germany
Franjo Ivancic	NEC Laboratories, USA
Jie-Hong Roland Jiang	National Taiwan University, Taiwan
Sarfraz Khurshid	University of Texas at Austin, USA
Daniel Kroening	Oxford University, UK
Orna Kupferman	Hebrew University, Israel
Insup Lee	University of Pennsylvania, USA
Jerome Leroux	CNRS, France
Rupak Majumdar	Max Planck Institute, Germany
Darko Marinov	University of Illinois at Urbana-Champaign, USA
Kedar Namjoshi	Bell Labs, USA
Madhu Parthasarathy	University of Illinois at Urbana-Champaign, USA
Corina Pasareanu	NASA Ames Research Center, USA
Doron Peled	Bar Ilan University, Israel
Abhik Roychoudhury	National University of Singapore, Singapore
Andrey Rybalchenko	Technische Universität München, Germany
Sven Schewe	University of Liverpool, UK

Prasad Sistla	University of Illinois at Chicago, USA
Yih-Kuen Tsay	National Taiwan University, Taiwan
Tomas Vojnar	Brno University of Technology, Czech Republic
Bow-Yaw Wang	Academia Sinica, Taiwan
Chao Wang	NEC Laboratories, USA
Farn Wang	National Taiwan University, Taiwan
Hsu-Chun Yen	National Taiwan University, Taiwan
Fang Yu	National Chengchi University, Taiwan
Wenhui Zhang	Chinese Academy of Sciences, China

Local Arrangements Chair

Farn Wang	National Taiwan University, Taiwan

Steering Committee

E. Allen Emerson	University of Texas at Austin, USA
Insup Lee	University of Pennsylvania, USA
Doron Peled	Bar Ilan University, Israel
Teruo Higashino	Osaka University, Japan
Farn Wang	National Taiwan University, Taiwan
Hsu-Chun Yen	National Taiwan University, Taiwan

Sponsoring Institutions

National Taiwan University, College of EE and CS, Taiwan
Academia Sinica, Institute of Information Science, Taiwan
Academia Sinica, Research Center for Information Technology Innovation, Taiwan
National Science Council, Taiwan
Ministry of Education, Taiwan

External Reviewers

Jade Alglave	Marsha Chechik
Mohamed Faouzi Atig	Sanjian Chen
Anaheed Ayoub	Yu-Fang Chen
Gogul Balakrishnan	Misty Davies
Hernan Baro Graf	Laurent Doyen
Benedikt Bollig	Michael Emmi
Marco Bozzano	Constantin Enea
David Bushnell	John Fearnley
Chia-Wei Chang	Luis María Ferrer Fioriti
Sudipta Chattopadhyay	Emmanuel Fleury

Khalil Ghorbal
Hugo Gimbert
Alberto Griggio
Olga Grinchtein
Peter Habermehl
Cheng-Shen Han
Arnd Hartmanns
Nannan He
Alexander Heussner
Lukas Holik
Chung-Hao Huang
Geng-Dian Huang
Lei Ju
Lukasz Kaiser
Andrew King
Anvesh Komuravelli
David Landsberg
Adonis Lin
Michel Ludwig
Antoine Miné
Sergio Mover
Aniello Murano
O. Olivo
Hans-Jörg Peter
Dawei Qi
Markus Rabe
Ahmed Rezine
Alexander Roederer
Kristin Rozier
Indranil Saha
Roopsha Samanta
Sriram Sankaranarayanan
Wendelin Serwe
Junaid Siddiqui
Mihaela Sighireanu
Jiri Simacek
Ales Smrcka
Michael Tautschnig
Stefano Tonetta
Ming-Hsien Tsai
Andrea Turrini
Vincent Wang
Ralf Wimmer
Jung-Hsuan Wu
Zhilin Wu
Guowei Yang
Shun-Ching Yang
Yu Yang
Lingming Zhang

Table of Contents

Invited Papers

Statistical Model Checking for Cyber-Physical Systems 1
Edmund M. Clarke and Paolo Zuliani

Max and Sum Semantics for Alternating Weighted Automata 13
Shaull Almagor and Orna Kupferman

Making Software Verification Tools Really Work 28
Jade Alglave, Alastair F. Donaldson, Daniel Kroening, and Michael Tautschnig

Synthesizing, Verifying, and Debugging SoC with FSM-Based Specification of On-Chip Communication Protocols 43
Masahiro Fujita

Automated Analysis of Industrial Embedded Software 51
Moonzoo Kim and Yunho Kim

Regular Papers

Nondeterministic Update of CTL Models by Preserving Satisfaction through Protections 60
Miguel Carrillo and David A. Rosenblueth

Type-Based Automated Verification of Authenticity in Asymmetric Cryptographic Protocols 75
Morten Dahl, Naoki Kobayashi, Yunde Sun, and Hans Hüttel

Formalization of Finite-State Discrete-Time Markov Chains in HOL 90
Liya Liu, Osman Hasan, and Sofiène Tahar

An Alternative Definition for Timed Automata Composition 105
Jean-Paul Bodeveix, Abdeldjalil Boudjadar, and Mamoun Filali

Model Checking EGF on Basic Parallel Processes 120
Hongfei Fu

Measuring Permissiveness in Parity Games: Mean-Payoff Parity Games Revisited 135
Patricia Bouyer, Nicolas Markey, Jörg Olschewski, and Michael Ummels

Algorithms for Synthesizing Priorities in Component-Based Systems 150
Chih-Hong Cheng, Saddek Bensalem, Yu-Fang Chen, Rongjie Yan, Barbara Jobstmann, Harald Ruess, Christian Buckl, and Alois Knoll

Trust Metrics for the SPKI/SDSI Authorisation Framework 168
Dominik Wojtczak

Antichain-Based QBF Solving 183
Thomas Brihaye, Véronique Bruyère, Laurent Doyen, Marc Ducobu, and Jean-Francois Raskin

A Hierarchical Approach for the Synthesis of Stabilizing Controllers for Hybrid Systems 198
Janusz Malinowski, Peter Niebert, and Pierre-Alain Reynier

Formal Analysis of Online Algorithms 213
Benjamin Aminof, Orna Kupferman, and Robby Lampert

Modal Transition Systems: Composition and LTL Model Checking 228
Nikola Beneš, Ivana Černá, and Jan Křetínský

Efficient Inclusion Checking on Explicit and Semi-symbolic Tree Automata 243
Lukáš Holík, Ondřej Lengál, Jiří Šimáček, and Tomáš Vojnar

Assembling Sessions 259
Philippe Darondeau, Loïc Hélouët, and Madhavan Mukund

Parametric Modal Transition Systems 275
Nikola Beneš, Jan Křetínský, Kim G. Larsen, Mikael H. Møller, and Jiří Srba

Policy Iteration within Logico-Numerical Abstract Domains 290
Pascal Sotin, Bertrand Jeannet, Franck Védrine, and Eric Goubault

Small Strategies for Safety Games 306
Daniel Neider

Multi-core Nested Depth-First Search 321
Alfons Laarman, Rom Langerak, Jaco van de Pol, Michael Weber, and Anton Wijs

Self-Loop Aggregation Product — A New Hybrid Approach to On-the-Fly LTL Model Checking 336
Alexandre Duret-Lutz, Kais Klai, Denis Poitrenaud, and Yann Thierry-Mieg

A Lightweight Approach for Loop Summarization 351
Mohamed Nassim Seghir

A Succinct Canonical Register Automaton Model 366
Sofia Cassel, Falk Howar, Bengt Jonsson, Maik Merten, and Bernhard Steffen

Parallel Nested Depth-First Searches for LTL Model Checking 381
Sami Evangelista, Laure Petrucci, and Samir Youcef

Evaluating LTL Satisfiability Solvers 397
Viktor Schuppan and Luthfi Darmawan

Tool Papers

McAiT – A Timing Analyzer for Multicore Real-Time Software 414
Mingsong Lv, Nan Guan, Qingxu Deng, Ge Yu, and Wang Yi

MIO Workbench: A Tool for Compositional Design with Modal Input/Output Interfaces 418
Sebastian S. Bauer, Philip Mayer, and Axel Legay

Short Papers

The Buck Stops Here: Order, Chance, and Coordination in Distributed Control 422
Gal Katz, Doron Peled, and Sven Schewe

Symbolic Verification and Test Generation for a Network of Communicating FSMs 432
Xiaoqing Jin, Gianfranco Ciardo, Tae-Hyong Kim, and Yang Zhao

Hierarchical Counterexamples for Discrete-Time Markov Chains 443
Nils Jansen, Erika Ábrahám, Jens Katelaan, Ralf Wimmer, Joost-Pieter Katoen, and Bernd Becker

Efficient Loop Navigation for Symbolic Execution 453
Jan Obdržálek and Marek Trtík

An Efficient Algorithm for Learning Event-Recording Automata 463
Shang-Wei Lin, Étienne André, Jin Song Dong, Jun Sun, and Yang Liu

Discretizing Affine Hybrid Automata with Uncertainty 473
Thao Dang and Thomas Martin Gawlitza

What's Decidable about Weighted Automata? 482
Shaull Almagor, Udi Boker, and Orna Kupferman

Widening with Thresholds for Programs with Complex Control Graphs 492
Lies Lakhdar-Chaouch, Bertrand Jeannet, and Alain Girault

Linear Hybrid System Falsification through Local Search 503
Houssam Abbas and Georgios Fainekos

Learning-Based Compositional Verification for Synchronous Probabilistic Systems 511
Lu Feng, Tingting Han, Marta Kwiatkowska, and David Parker

An Algorithmic Framework for Synthesis of Concurrent Programs 522
E. Allen Emerson and Roopsha Samanta

Author Index 531