

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

Antonín Kučera Thomas A. Henzinger
Jaroslav Nešetřil Tomáš Vojnar
David Antoš (Eds.)

Mathematical and Engineering Methods in Computer Science

8th International Doctoral Workshop, MEMICS 2012
Znojmo, Czech Republic, October 25-28, 2012
Revised Selected Papers



Springer

Volume Editors

Antonín Kučera

Masaryk University, Faculty of Informatics
Botanická 68a, 602 00 Brno, Czech Republic
E-mail: tony@fi.muni.cz

Thomas A. Henzinger

Institute of Science and Technology Austria
Am Campus 1, 3400 Klosterneuburg, Austria
E-mail: tah@ist.ac.at

Jaroslav Nešetřil

Charles University in Prague, Faculty of Mathematics and Physics
Malostranské nám. 25, 118 00 Praha 1, Czech Republic
E-mail: nesetril@kam.mff.cuni.cz

Tomáš Vojnar

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 66 Brno, Czech Republic
E-mail: vojnar@fit.vutbr.cz

David Antoš

Masaryk University, Institute of Computer Science
Botanická 68a, 602 00 Brno, Czech Republic
E-mail: antos@ics.muni.cz

ISSN 0302-9743

ISBN 978-3-642-36044-2

DOI 10.1007/978-3-642-36046-6

Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349

e-ISBN 978-3-642-36046-6

Library of Congress Control Number: 2013930169

CR Subject Classification (1998): D.2.4, C.2.0, F.2.2, G.2.2, C.2.4, K.6.3, K.6.5, K.4.4

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2013

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 proceedings of the 8th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS 2012) held in Znojmo, Czech Republic, during October 25–28, 2012.

The aim of the MEMICS workshop series is to provide an opportunity for PhD students to present and discuss their work in an international environment. The scope of MEMICS is broad and covers many fields of computer science and engineering. In 2012, submissions were invited especially in the following (though not exclusive) areas:

- Computer-aided analysis and verification
- Applications of game theory in computer science
- Networks and security
- Modern trends of graph theory in computer science
- Electronic systems design and testing
- Quantum information processing

There were 31 submissions from 9 countries. Each submission was thoroughly evaluated by at least three Program Committee members who also provided extensive feedback to the authors. Out of these submissions, 13 papers were selected for publication in these proceedings.

In addition to regular papers, MEMICS workshops also invite PhD students to submit a *presentation* of their recent research results that have already undergone a rigorous peer-review process and have been presented at a high-quality international conference or published in a recognized journal. A total of 28 presentations out of 32 submissions from 11 countries were included in the MEMICS 2012 program.

The MEMICS 2012 program was further enriched by six keynote lectures. The speakers were

- Dirk Beyer from University of Passau with a talk on “CPAchecker: The Configurable Software-Verification Platform”
- Dieter Gollmann from Technische Universität Hamburg-Harburg with a talk on “Security for Cyber-Physical Systems”
- Said Hamdioui from Delft University of Technology with a talk on “Testing Embedded Memories in the Nano-Era: From Defects to Built-In-Self Test”
- Colin McDiarmid from Corpus Christi College Oxford with a talk on “Quick-sort and Large Deviations”
- Peter Bro Miltersen from Aarhus University with a talk on “Recent Result on Howard’s Algorithm”
- Simon Perdrix from Laboratoire d’Informatique de Grenoble (LIG), CNRS and Université de Grenoble with a talk on “Graph-Based Quantum Secret Sharing”

The MEMICS tradition of *best paper awards* continued also in 2012. The best regular papers were selected at the end of the workshop by the MEMICS 2012 Best Paper Award Committee consisting of Jozef Gruska, Dušan Kolář, Mojmir Křetínský, and Tomáš Vojnar. The winners were:

- Michal Mikuš, STU Bratislava, Slovakia, for the paper “Ciphertext-Only Attack on Gentry-Halevi Implementation of Somewhat Homomorphic Scheme”
- Petr Novotný, MU Brno, Czech Republic, for the paper “Determinacy in Games with Unbounded Payoff Functions”

The awards consisted of a diploma accompanied by a financial prize of approximately 400 Euro. The money were donated by *Red Hat Czech Republic* and *Y Soft*, the MEMICS 2012 Industrial Sponsors.

The MEMICS 2012 workshop was financially supported by the doctoral grant project 102/09/H042 *Mathematical and Engineering Approaches to Developing Reliable and Secure Concurrent and Distributed Computer Systems* from the Czech Science Foundation.

We thank the Program Committee members and the external reviewers for their careful and constructive work. We thank Organizing Committee members who helped to create a unique and relaxed atmosphere which distinguishes MEMICS from other computer science meetings. We also gratefully acknowledge the support of the EasyChair system and the fine cooperation with the *Lecture Notes in Computer Science* team of Springer.

November 2012

Antonín Kučera
Thomas A. Henzinger
Jaroslav Nešetřil
Tomáš Vojnar

Organization

Workshop Organization

The 8th Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS 2012) took place in Znojmo, Czech Republic, on the premises of the Loucký Monastery during October 25–28, 2012. The workshop was attended by 115 participants from 12 countries. More information about the MEMICS workshop series is available at <http://www.memics.cz>.

General Chair

Antonín Kučera

Masaryk University, Brno, Czech Republic

Program Committee Chairs

Thomas A. Henzinger

Institute of Science and Technology, Austria

Jaroslav Nešetřil

Charles University in Prague, Czech Republic

Tomáš Vojnar

Brno University of Technology, Brno,
Czech Republic

Program Committee

Andris Ambainis

University of Latvia

Jiří Barnat

Masaryk University, Brno, Czech Republic

Jan Bouda

Masaryk University, Brno, Czech Republic

Patricia Bouyer-Decitre

CNRS, France

Sergio Cabello

University of Ljubljana, Slovenia

Krishnendu Chatterjee

Institute of Science and Technology Austria

Zdeněk Dvořák

Charles University, Prague, Czech Republic

Javier Esparza

TU München, Germany

Rusins Freivalds

University of Latvia

Görschwin Fey

Universität Bremen, Germany

Dieter Gollmann

TU Hamburg-Harburg, Germany

Erich Grädel

RWTH Aachen, Germany

Gregory Z. Gutin

Royal Holloway, University of London, UK

Peter Habermehl

LIAFA, University Paris Diderot, France

Said Hamdioui

TU Delft, The Netherlands

Petr Hanáček

Brno University of Technology, Czech Republic

Holger Hermanns

Saarland University, Germany

Petr Hliněný

Masaryk University, Brno,
Czech Republic

VIII Organization

Keijo Heljanko	Aalto University, Finland
Richard Jozsa	University of Cambridge, UK
Zdeněk Kotásek	Brno University of Technology, Brno, Czech Republic
Hana Kubátová	Czech Technical University, Prague, Czech Republic
Gerald Luttgen	University of Bamberg, Germany
Dániel Marx	Hungarian Academy of Sciences, Budapest, Hungary
Václav Matyáš	Masaryk University, Brno, Czech Republic
Luděk Matyska	Masaryk University, Brno, Czech Republic
Michal Pěchouček	Czech Technical University in Prague, Czech Republic
Jaco van de Pol	CTIT, University of Twente, The Netherlands
Joachim Posegga	University of Passau, Germany
Geraint Price	Royal Holloway, University of London, UK
Lukáš Sekanina	Brno University of Technology, Brno, Czech Republic
Martin Stanek	Comenius University Bratislava, Slovakia
Andreas Steininger	TU Vienna, Austria
Stefan Szeider	Vienna University of Technology, Vienna, Austria
Ondřej Šerý	University of Lugano, Switzerland and D3S, Charles University in Prague, Czech Republic
Shin Yoo	CREST, University College London, UK

Steering Committee

Milan Česka	Brno University of Technology, Brno, Czech Republic
Zdeněk Kotásek	Brno University of Technology, Brno, Czech Republic
Mojmír Křetínský	Masaryk University, Brno, Czech Republic
Antonín Kučera	Masaryk University, Brno, Czech Republic
Luděk Matyska	Masaryk University, Brno, Czech Republic
Tomáš Vojnar	Brno University of Technology, Brno, Czech Republic

Organizing Committee

Jan Bouda	chair, Masaryk University, Brno, Czech Republic
Milan Česka	Masaryk University, Brno, Czech Republic
Dana Komárková	Masaryk University, Brno, Czech Republic

Zbyněk Mayer	Masaryk University, Brno, Czech Republic
Ada Nazarejová	Masaryk University, Brno, Czech Republic
Adam Rambousek	Masaryk University, Brno, Czech Republic
Šimon Suchomel	Masaryk University, Brno, Czech Republic

Additional Reviewers

Miklos Bona	Mark Jones
Bastian Braun	Syab Khan
Mafalda Cortez	Jan Křetínský
Robert Crowston	Peng Liu
Mehdi Dehbashi	Ashley Montanaro
Vladimír Drábek	Rameez Naqvi
Zbyněk Falt	Arash Rafiey
Stefan Frehse	Heinz Riener
Stephan Huber	Sadia Sharmin
Jiří Jaroš	

Table of Contents

BDD-Based Software Model Checking with CPACHECKER	1
<i>Dirk Beyer and Andreas Stahlbauer</i>	
Security for Cyber-Physical Systems (Extended Abstract)	12
<i>Dieter Gollmann</i>	
Quantum Secret Sharing with Graph States	15
<i>Sylvain Gravier, Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix</i>	
Testing Embedded Memories: A Survey	32
<i>Said Hamdioui</i>	
Quicksort and Large Deviations	43
<i>Colin McDiarmid</i>	
Recent Results on Howard’s Algorithm	53
<i>Peter Bro Miltersen</i>	
Advantage of Quantum Strategies in Random Symmetric XOR Games	57
<i>Andris Ambainis, Jānis Iraids, Dmitry Kravchenko, and Madaras Virza</i>	
Verification of Liveness Properties on Closed Timed-Arc Petri Nets	69
<i>Mathias Andersen, Heine Gatten Larsen, Jiří Srba, Mathias Grund Sørensen, and Jakob Haahr Taankvist</i>	
Fast Algorithm for Rank-Width	82
<i>Martin Beyß</i>	
Determinacy in Stochastic Games with Unbounded Payoff Functions	94
<i>Tomáš Brázdil, Antonín Kučera, and Petr Novotný</i>	
Strategy Complexity of Finite-Horizon Markov Decision Processes and Simple Stochastic Games	106
<i>Krishnendu Chatterjee and Rasmus Ibsen-Jensen</i>	
Controllable-Choice Message Sequence Graphs	118
<i>Martin Chmelík and Vojtěch Řehák</i>	
A Better Way towards Key Establishment and Authentication in Wireless Sensor Networks	131
<i>Filip Jurnečka and Vashek Matyáš</i>	

Parameterized Algorithms for Stochastic Steiner Tree Problems	143
<i>Denis Kurz, Petra Mutzel, and Bernd Zey</i>	
Action Investment Energy Games	155
<i>Kim G. Larsen, Simon Laursen, and Jiří Srba</i>	
Ciphertext-Only Attack on Gentry-Halevi Implementation of Somewhat Homomorphic Scheme	168
<i>Michal Mikuš and Marek Šýs</i>	
Grover’s Algorithm with Errors	180
<i>Andris Ambainis, Artūrs Bačkurs, Nikolajs Nahimovs, and Alexander Rivosh</i>	
On WQO Property for Different Quasi Orderings of the Set of Permutations	190
<i>Sandra Ose and Juris Viksna</i>	
Towards User-Aware Multi-touch Interaction Layer for Group Collaborative Systems	200
<i>Vít Rusňák, Lukáš Ručka, and Petr Holub</i>	
Author Index	213