

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

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Luboš Brim Boudewijn Haverkort
Martin Leucker Jaco van de Pol (Eds.)

Formal Methods: Applications and Technology

11th International Workshop, FMICS 2006
and 5th International Workshop, PDMC 2006
Bonn, Germany, August 26-27, and August 31, 2006
Revised Selected Papers

Volume Editors

Luboš Brim
Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic
E-mail: brim@fi.muni.cz

Boudewijn Haverkort
University of Twente
P.O. Box 217, 7500AE Enschede, The Netherlands
E-mail: brh@cs.utwente.nl

Martin Leucker
Technische Universität München
Boltzmannstr. 3, 85748 Garching, Germany
E-mail: leucker@in.tum.de

Jaco van de Pol
Centrum voor Wiskunde en Informatica, SEN 2
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
E-mail: Jaco.van.de.Pol@cwi.nl

Library of Congress Control Number: 2007921124

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

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN	0302-9743
ISBN-10	3-540-70951-7 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-70951-0 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12021901 06/3142 5 4 3 2 1 0

Preface

These are the joint final proceedings of the 11th International Workshop on Formal Methods for Industrial Critical Systems (FMICS 2006) and the fifth International Workshop on Parallel and Distributed Methods in Verification (PDMC 2006). Both workshops were organized as satellite events of CONCUR 2006, the 17th International Conference on Concurrency Theory that was organized in Bonn, August 2006.

The FMICS workshop continued successfully the aim of the FMICS working group – to promote the use of formal methods for industrial applications, by supporting research in this area and its application in industry. The emphasis in these workshops is on the exchange of ideas between researchers and practitioners, in both industry and academia.

This year the Program Committee received a record number of submissions. The 16 accepted regular contributions and 2 accepted tool papers, selected out of a total of 47 submissions, cover formal methodologies for handling large state spaces, model-based testing, formal description and analysis techniques as well as a range of applications and case studies.

The workshop program included two invited talks, by Anna Slobodova from Intel on “Challenges for Formal Verification in an Industrial Setting” and by Edward A. Lee from the University of California at Berkeley on “Making Concurrency Mainstream.” The former full paper can be found in this volume.

Following the tradition of previous workshops, the European Association of Software Science and Technology (EASST) supported a best paper award. This award was granted to Michael Weber and Moritz Hammer for their excellent paper “‘To Store or Not To Store’ Reloaded: Reclaiming Memory on Demand.”

The primary goal of the PDMC workshop series is to present and discuss recent developments in the young area of parallel and distributed methods in verification. Several verification techniques, ranging over model checking, equivalence checking, theorem proving, constraint solving and dependability analysis are addressed by the PDMC community. Verification problems are usually very demanding tasks, especially because the systems that we build and want to verify become increasingly complex.

On the other hand, parallel and distributed computing machinery is widely available. Algorithms and tools must be developed to use this hardware optimally for our verification tasks. Traditionally, we studied algorithms for homogeneous situations, such as parallel shared-memory computers and distributed clusters of PCs. Currently, the emphasis is shifting towards heterogeneous GRIDs. But even modern desktop PCs are quite heterogeneous, consisting of multiple core processors, various memory devices and cache levels, all with their own performance characteristics.

This year's PDMC had nine submissions; six papers were selected for presentation, and four papers were accepted for publication in this volume. In addition, Luboš Brim from Masaryk University, Brno, gave an invited lecture on "Distributed Verification: Exploring the Power of Raw Computing Power." The full paper can also be found in this volume.

We would like to thank all authors for their submissions. We would also like to thank the members of both Program Committees, and the additional referees, for their timely reviewing and lively participation in the subsequent discussion—the quality of the contributions in this volume are also due to their efforts and expertise.

The organizers wish to thank CONCUR for hosting the FMICS and PDMC 2006 workshops and taking care of many administrative aspects, and ERCIM for its financial support of FMICS. Additionally, the organizers would like to thank the EASST (European Association of Software Science and Technology), the Faculty of Informatics, Masaryk University Brno and the Technical University Munich, the CWI (Center of Mathematics and Computer Science, Amsterdam) and the University of Twente for supporting these events.

December 2006

Luboš Brim
Boudewijn R. Haverkort
Martin Leucker
Jaco van de Pol

Organization

FMICS

Program Chairs

Luboš Brim
Martin Leucker

Masaryk University Brno, Czech Republic
Technical University of Munich, Germany

Program Committee

Rance Cleaveland
Wan Fokkink

University of Maryland, USA
Vrije Universiteit Amsterdam and CWI, The Netherlands

Stefania Gnesi
Susanne Graf
David Harel
Klaus Havelund
Thomas A. Henzinger
Leszek Holenderski
Stefan Kowalewski
Marta Kwiatkowska
Salvatore La Torre
Tiziana Margaria
Radu Mateescu
Doron Peled
Ernesto Pimentel
Andreas Podelski
Don Sannella
Joseph Sifakis

ISTI-CNR, Italy
VERIMAG, France
Weizmann Institute of Science, Israel
Kestrel Technology, USA
EPFL, Switzerland
Philips Research, The Netherlands
RWTH Aachen University, Germany
University of Birmingham, UK
Università degli Studi di Salerno, Italy
University of Göttingen, Germany
INRIA Rhône-Alpes and ENS Lyon, France
University of Warwick, UK
University of Malaga, Spain
Max-Planck-Institut für Informatik, Germany
University of Edinburgh, UK
VERIMAG, France

PDMC

Program Chairs

Boudewijn Haverkort
Jaco van de Pol

University of Twente, The Netherlands
CWI Amsterdam, The Netherlands

Program Committee

Gerd Behrmann
Ivana Černá
Gianfranco Ciardo
Joerg Denzinger

Aalborg University, Denmark
Masaryk University Brno, Czech Republic
University of California at Riverside, USA
University of Calgary, Canada

Hubert Garavel	INRIA Rhône-Alpes, France
Orna Grumberg	Technion, Haifa, Israel
William Knottenbelt	Imperial College, London, UK
Marta Kwiatkowska	University of Birmingham, UK
Martin Leucker	Technical University of Munich, Germany

Referees (FMICS and PDMC)

C. Artho	I. Černá	M. Kuntz	D. Parker
Y. Atir	F. Ciesinski	F. Lang	G. Parlato
R. Atkey	M. Faella	P. Lopez	G. Salaün
J. Barnat	A. Fantechi	K. MacKenzie	W. Serwe
M. ter Beek	M. Felici	P. Maier	F. Sorrentino
M. van der Bijl	A. J. Fernandez	S. Maoz	J. Tenzer
B. Bollig	M. Fruth	F. Mazzanti	A. Venet
L. Bozzelli	N. Geisweiller	R. Merom	A. Wijs
A. Bucchiarone	A. Goldberg	A. Murano	T. Willemse
D. Calvanese	A. Idani	G. Norman	V. Wolf
M. V. Cengarle	C. Joubert	M. Parente	

Table of Contents

Invited Contributions

Challenges for Formal Verification in Industrial Setting	1
<i>Anna Slobodová</i>	
Distributed Verification: Exploring the Power of Raw Computing Power	23
<i>Luboš Brim</i>	

FMICS

An Easy-to-Use, Efficient Tool-Chain to Analyze the Availability of Telecommunication Equipment	35
<i>Kai Lampka, Markus Siegle, and Max Walter</i>	
“To Store or Not To Store” Reloaded: Reclaiming Memory on Demand	51
<i>Moritz Hammer and Michael Weber</i>	
Discovering Symmetries	67
<i>Hassen Saïdi</i>	
On Combining Partial Order Reduction with Fairness Assumptions	84
<i>Luboš Brim, Ivana Černá, Pavel Moravec, and Jiří Šimša</i>	
Test Coverage for Loose Timing Annotations	100
<i>C. Helmstetter, F. Maraninchi, and L. Maillet-Contoz</i>	
Model-Based Testing of a WAP Gateway: An Industrial Case-Study . . .	116
<i>Anders Hessel and Paul Pettersson</i>	
Heuristics for ioco -Based Test-Based Modelling	132
<i>Tim A.C. Willemse</i>	
Verifying VHDL Designs with Multiple Clocks in SMV	148
<i>A. Smrčka, V. Řehák, T. Vojnar, D. Šafránek, P. Matoušek, and Z. Řehák</i>	
Verified Design of an Automated Parking Garage	165
<i>Aad Mathijssen and A. Johannes Pretorius</i>	
Evaluating Quality of Service for Service Level Agreements	181
<i>Allan Clark and Stephen Gilmore</i>	

Simulation-Based Performance Analysis of a Medical Image-Processing Architecture	195
<i>P.J.L. Cuijpers and A.V. Fyukov</i>	
BLASTing Linux Code	211
<i>Jan Tobias Mühlberg and Gerald Lüttgen</i>	
A Finite State Modeling of AFDX Frame Management Using Spin	227
<i>Indranil Saha and Suman Roy</i>	
UML 2.0 State Machines: Complete Formal Semantics Via Core State Machines	244
<i>Harald Fecher and Jens Schönborn</i>	
Automated Incremental Synthesis of Timed Automata	261
<i>Borzoo Bonakdarpour and Sandeep S. Kulkarni</i>	
SAT-Based Verification of LTL Formulas	277
<i>Wenhui Zhang</i>	
jmlc: A Tool for Executing JML Specifications Via Constraint Programming	293
<i>Ben Krause and Tim Wahls</i>	
Goanna—A Static Model Checker	297
<i>Ansgar Fehnker, Ralf Huuck, Patrick Jayet, Michel Lussenburg, and Felix Rauch</i>	
PDMC	
Parallel SAT Solving in Bounded Model Checking	301
<i>Erika Ábrahám, Tobias Schubert, Bernd Becker, Martin Fränzle, and Christian Herde</i>	
Parallel Algorithms for Finding SCCs in Implicitly Given Graphs	316
<i>Jiří Barnat and Pavel Moravec</i>	
Can Saturation Be Parallelised? – On the Parallelisation of a Symbolic State-Space Generator	331
<i>Jonathan Ezekiel, Gerald Lüttgen, and Radu Siminiceanu</i>	
Distributed Colored Petri Net Model-Checking with CYCLADES	347
<i>Christophe Pajault and Jean-François Pradat-Peyre</i>	
Author Index	363