

Lecture Notes in Computer Science

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

2399

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Holger Hermanns Roberto Segala (Eds.)

Process Algebra and Probabilistic Methods

Performance Modeling and Verification

Second Joint International Workshop PAPM-PROBMIV 2002
Copenhagen, Denmark, July 25-26, 2002
Proceedings



Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany
Juris Hartmanis, Cornell University, NY, USA
Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Holger Hermanns
University of Twente, Faculty of Computer Science
Formal Methods and Tools Group
P.O. Box 217, 7500 AE Enschede, The Netherlands
E-mail: hermanns@cs.utwente.nl

Roberto Segala
University of Verona, Department of Computer Science
Strada Le Grazie 15, 37134 Verona, Italy
E-mail: segala@sci.univr.it

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Process algebra and probabilistic methods : performance modeling and verification ; second joint international workshop ; proceedings / PAPM PROBMIV 2002, Copenhagen, Denmark, July 25 - 26, 2002. Holger Hermanns ; Roberto Segala (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2399)
ISBN 3-540-43913-7

CR Subject Classification (1998): F.3.1, F.3, D.2.4, D.3.1, C.4

ISSN 0302-9743

ISBN 3-540-43913-7 Springer-Verlag 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-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Christian Grosche, Hamburg
Printed on acid-free paper SPIN 10873586 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the second joint PAPM-PROBMIV Workshop, held at the University of Copenhagen, Denmark, July 25–26, 2002 as part of the *Federated Logic Conference* (FLoC 2002).

The PAPM-PROBMIV workshop results from the combination of two workshops: PAPM (Process Algebras and Performance Modeling) and PROBMIV (Probabilistic Methods in Verification). The aim of the joint workshop is to bring together the researchers working across the whole spectrum of techniques for the modeling, specification, analysis, and verification of probabilistic systems. Probability is widely used in the design and analysis of software and hardware systems, as a means to derive efficient algorithms (e.g. randomization), as a model for unreliable or unpredictable behavior (as in the study of fault-tolerant systems and computer networks), and as a tool to study performance and dependability properties. The topics of the workshop include specification, models, and semantics of probabilistic systems, analysis and verification techniques, probabilistic methods for the verification of non-probabilistic systems, and tools and case studies.

The first PAPM workshop was held in Edinburgh in 1993; the following ones were held in Regensburg (1994), Edinburgh (1995), Turin (1996), Enschede (1997), Nice (1998), Zaragoza (1999), and Geneva (2000). The first PROBMIV workshop was held in Indianapolis, Indiana (1998); the next one took place in Eindhoven (1999). In 2000, PROBMIV was replaced by a Dagstuhl seminar on Probabilistic Methods in Verification.

The first joint PAPM-PROBMIV was held as part of the *2001 Aachen Multi-conference on Measurement, Modeling, and Evaluation of Computer-Communication Systems*. The proceedings were published in Springer's LNCS series as Volume 2165. Joining both research areas in a single workshop was considered very fruitful, and led to the second joint event, and to this volume.

Of the 19 regular papers submitted, the program committee accepted 10 for presentation at the workshop. They are included in the present volume as *selected papers*. The volume also contains four *short abstracts* which were selected on the basis of their innovative potential for the workshop. The workshop included two invited presentations, by David Sands (Chalmers University of Technology and Göteborg University), and André Schiper (Ecole Polytechnique Fédérale de Lausanne).

We thank all the members of the program committee, and their sub-referees, for selecting the papers to be presented. Our thanks go to the Centre for Telematics and Information Technology (CTIT) of the University of Twente for generously sponsoring the workshop, and to our FLoC sponsoring conference CAV. We also thank all the authors for their help in meeting the tight deadlines which we had to set.

PROBMIV Steering Committee

Marta Kwiatkowska	(Chair, University of Birmingham)
Luca de Alfaro	(University of California, Berkeley)
Rajeev Alur	(University of Pennsylvania)
Christel Baier	(University of Mannheim)
Michael Huth	(Kansas State University)
Joost-Pieter Katoen	(University of Twente)
Prakash Panangaden	(McGill University)
Roberto Segala	(University of Verona)

PAPM Steering Committee

Ed Brinksma	(University of Twente)
Roberto Gorrieri	(University of Bologna)
Ulrich Herzog	(University of Erlangen)
Jane Hillston	(University of Edinburgh)

Program Committee

Luca de Alfaro	University of California at Santa Cruz, USA
Christel Baier	University of Bonn, D
Gianfranco Balbo	University of Turin, I
Marco Bernardo	University of Urbino, I
Pedro R. D'Argenio	University of Cordoba, ARG
Stephen Gilmore	University of Edinburgh, UK
Holger Hermanns (co-chair)	University of Twente, co-chair
Michael Huth	Imperial College, UK
Marta Kwiatkowska	University of Birmingham, UK
Prakash Panangaden	Mc Gill University, CAN
William H. Sanders	University of Illinois at Urbana-Champaign, USA
Roberto Segala (co-chair)	University of Verona, co-chair
Markus Siegle	University of Erlangen-Nürnberg, D
Manuel Silva	University of Zaragoza, ES
Scott Smolka	SUNY at Stony Brook, USA

Referees

Alessandro Aldini	Michael Huth	Alfredo Olivero
Suzana Andova	S. Purushothaman Iyer	Prakash Panangaden
Christel Baier	Bertrand Jeannot	Dave Parker
Gianfranco Balbo	Joost-Pieter Katoen	Sylvain Peyronnet
Simonetta Balsamo	Ulrich Klehmet	Tamara Rezk
Marco Bernardo	William Knottenbelt	Eike Ritter
Henrik Bohnenkamp	Matthias Kuntz	Andrei Sabelfield
Mario Bravetti	Marcos E. Kurbán	William H. Sanders
Lucia Cloth	Marta Kwiatkowska	Roberto Segala
Pedro R. D'Argenio	Kai Lampka	Markus Siegle
Massimiliano De Pierro	Rom Langerak	Manuel Silva
Susanna Donatelli	Sophie Laplante	Scott Smolka
Stephen Gilmore	Olivier Markowitch	Jeremy Sproston
Holger Hermanns	Joachim Meyer-Kayser	Eugene W. Stark
Jane Hillston	David Monniaux	Vanessa Teague
Andras Horvath	Gethin Norman	Herbert Wiklicky

Table of Contents

Invited Contributions

- Failure Detection vs Group Membership in Fault-Tolerant Distributed Systems: Hidden Trade-Offs..... 1
André Schiper
- Probability and Timing: Challenges for Secure Programming..... 16
David Sands

Selected Papers

- Security Analysis of a Probabilistic Non-repudiation Protocol..... 17
Alessandro Aldini and Roberto Gorrieri
- The Mean Value of the Maximum..... 37
Henrik Bohnenkamp and Boudewijn Haverkort
- Reduction and Refinement Strategies for Probabilistic Analysis..... 57
Pedro R. D'Argenio, Bertrand Jeannot, Henrik E. Jensen, and Kim G. Larsen
- Action Refinement for Probabilistic Processes with True Concurrency Models..... 77
Harald Fecher, Mila Majster-Cederbaum, and Jinzhao Wu
- Probabilistic Unfoldings and Partial Order Fairness in Petri Nets..... 95
Stefan Haar
- Possibilistic and Probabilistic Abstraction-Based Model Checking..... 115
Michael Huth
- Out-of-Core Solution of Large Linear Systems of Equations Arising from Stochastic Modelling..... 135
Marta Kwiatkowska and Rashid Mehmood
- Model Checking CSL until Formulae with Random Time Bounds..... 152
Marta Kwiatkowska, Gethin Norman, and António Pacheco
- Probabilistic Model Checking of the IEEE 802.11 Wireless Local Area Network Protocol..... 169
Marta Kwiatkowska, Gethin Norman, and Jeremy Sproston
- Deriving Symbolic Representations from Stochastic Process Algebras..... 188
Matthias Kuntz and Markus Siegle

Short Abstracts

A Generalization of Equational Proof Theory?	207
<i>Olivier Bournez</i>	
An Integrated Approach for the Specification and Analysis of Stochastic Real-Time Systems	209
<i>Mario Bravetti</i>	
Probabilistic Abstract Interpretation and Statistical Testing	211
<i>Alessandra Di Pierro and Herbert Wiklicky</i>	
Approximate Verification of Probabilistic Systems	213
<i>Richard Lassaigne and Sylvain Peyronnet</i>	
Author Index	215