

# Lecture Notes in Computer Science

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

1601

**Springer**

*Berlin*

*Heidelberg*

*New York*

*Barcelona*

*Hong Kong*

*London*

*Milan*

*Paris*

*Singapore*

*Tokyo*

Joost-Pieter Katoen (Ed.)

# Formal Methods for Real-Time and Probabilistic Systems

5th International AMAST Workshop, ARTS'99  
Bamberg, Germany, May 26-28, 1999  
Proceedings



Springer

Series Editors

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

Volume Editor

Joost-Pieter Katoen  
University of Erlangen-Nürnberg, Lehrstuhl für Informatik  
Martensstr. 3, D-91058 Erlangen, Germany  
E-mail: katoen@informatik.uni-erlangen.de

Currently at:

University of Twente, Formal Methods and Tools Group  
P.O. Box 217, 7500 AE Enschede, The Netherlands  
E-mail: katoen@cs.utwente.nl

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

**Formal methods for real-time and probabilistic systems :**  
proceedings / 5th International AMAST Workshop, ARTS '99,  
Bamberg, Germany, May 26 - 28, 1999. Joost-Pieter Katoen (ed.). -  
Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ;  
Milan ; Paris ; Singapore ; Tokyo : Springer, 1999  
(Lecture notes in computer science ; Vol. 1601)  
ISBN 3-540-66010-0

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

ISSN 0302-9743

ISBN 3-540-66010-0 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 1999  
Printed in Germany

Typesetting: Camera-ready by author  
SPIN 10704800 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

## Foreword

The aim of the ARTS'99 workshop is to bring together researchers and practitioners interested in the design of real-time and probabilistic systems. It is intended to cover the whole spectrum of development and application of specification, verification, analysis and construction techniques for real-time and probabilistic systems. Being a workshop under the umbrella of the AMAST movement (Algebraic Methodology And Software Technology), ARTS is intended to provide a forum for the presentation of approaches that are based on a clear mathematical basis. Aspects of real-time and probabilistic systems for the workshop include (but are not limited to): compositional construction and verification techniques, automatic and machine-supported verification, case studies, formal methods for performance analysis, semantics, algorithms and tools, and hybrid systems.

ARTS'99 was organised by the Lehrstuhl für Informatik 7 at the University of Erlangen-Nürnberg and took place at the Städtliche Volkshochschule in Bamberg (Oberfranken), Germany from May 26–28, 1999. Previous editions of ARTS workshops were organized by the University of Iowa, USA (1993), University of Bordeaux, France (1995), Brigham Young University, USA (1996), and General Systems Development, Mallorca, Spain (1997). Previous proceedings appeared as LNCS 1231 or as books in the AMAST Series of Computing.

The Program Committee selected 17 papers from a total of 33 submissions. Each submitted paper was sent to three Program Committee members, who were often assisted by sub-referees. During a one-week discussion via e-mail, the Program Committee has made the selection of the papers on the basis of the reviews. This volume contains the 17 selected papers plus 3 invited papers (in either full or abstract form).

I would like to thank the Program Committee members and the sub-referees for their efforts. I also like to thank the invited speakers for giving a talk at the workshop and for their contribution to the proceedings. Special thanks to Ulrich Herzog, Chris Moog, Teodor Rus, Diego Latella and Ruth Abraham (Springer-Verlag) for their support. Without their help, this event would not have been possible.

March 1999

Joost-Pieter Katoen  
Program Chair  
ARTS'99

## Invited Speakers

Bengt Jonsson (Uppsala University, Sweden)  
Frits W. Vaandrager (University of Nijmegen, The Netherlands)  
Moshe Y. Vardi (Rice University, USA)

## Steering Committee

Manfred Broy (Technical University of Munich, Germany)  
Edmund Clarke (Carnegie Mellon University, USA)  
Ulrich Herzog (University of Erlangen-Nürnberg, Germany)  
Zohar Manna (Stanford University, USA)  
Maurice Nivat (University of Paris 6, France)  
Amir Pnueli (Weizmann Institute of Science, Israel)  
Teodor Rus (Chair, University of Iowa, USA)

## Program Committee

Rajeev Alur (University of Pennsylvania, USA)  
Jos Baeten (Eindhoven University of Technology, The Netherlands)  
Christel Baier (University of Mannheim, Germany)  
Miquel Bertran (University of Ramon Llull, Spain)  
Antonio Cerone (University of South Australia, Australia)  
Rance Cleaveland (SUNY at Stony Brook, USA)  
Jim Davies (Oxford University, UK)  
Colin Fidge (University of Queensland, Australia)  
David de Frutos (University of Madrid, Spain)  
Hubert Garavel (INRIA Rhone-Alpes, France)  
Constance Heitmeyer (Naval Research Laboratory, USA)  
Tom Henzinger (University of Berkeley, USA)  
Jane Hillston (University of Edinburgh, UK)  
Joost-Pieter Katoen (University of Erlangen-Nürnberg, Germany, Chair)  
Rom Langerak (University of Twente, The Netherlands)  
Kim G. Larsen (Aalborg University, Denmark)  
Diego Latella (CNR-CNUCE, Italy)  
Jonathan Ostroff (University of York, Canada)  
Steve Schneider (Royal Holloway, UK)  
Roberto Segala (University of Bologna, Italy)  
Walter Vogler (University of Augsburg, Germany)

## Organising Committee

Joost-Pieter Katoen  
Chris Moog

## Referees

Luca Aceto	Luis Fernando Llana Díaz
Suzanna Andova	Gerald Lüttgen
Myla Archer	Mieke Massink
Marco Bernardo	Radu Mateescu
Elmar Bihler	Joachim Meyer-Kayser
Andrea Bondavalli	Annabelle McIver
Howard Bowman	Faron Moller
Mario Bravetti	Gethin Norman
Franck van Breugel	Manuel Núñez
Graham Clarke	Richard Paige
Alex Cowie	Prakash Panangaden
Luca de Alfaro	Adriano Peron
Pedro D'Argenio	Rob Pooley
Henrik Ejersbo Jensen	Jean-Francois Raskin
Stephen Gilmore	Michel Reniers
Holger Hermanns	Arend Rensink
Anna Ingólfssdóttir	Theo C. Ruys
Lars Jenner	Markus Siegle
Lennard Kerber	Graeme Smith
Ulrich Klehmet	Scott Smolka
Kåre Kristoffersen	Nigel Thomas
Marta Kwiatkowska	Axel Wabenhorst
Yassim Lakhnech	John Žic
Karl Lerner	Gerard Zwaan

## Sponsoring Institutions

C.N.R. Istituto CNUCE, Pisa, Italy

German Research Council (Deutsche Forschungsgemeinschaft)

# Table of Contents

## Invited Lecture

Fully Abstract Characterization of Probabilistic May Testing .....	1
<i>Bengt Jonsson and Wang Yi (Uppsala University)</i>	

## Verification of Probabilistic Systems

Quantitative Program Logic and Performance in Probabilistic Distributed Algorithms .....	19
<i>Annabelle K. McIver (Oxford University)</i>	
Establishing Qualitative Properties for Probabilistic Lossy Channel Systems: An Algorithmic Approach .....	34
<i>Christel Baier and Bettina Engelen (University of Mannheim)</i>	
Root Contention in IEEE 1394 .....	53
<i>Mariëlle Stoeltinga and Frits Vaandrager (University of Nijmegen)</i>	

## Model Checking Probabilistic Systems

Automatic Verification of Real-Time Systems with Discrete Probability Distributions .....	75
<i>Marta Kwiatkowska, Gethin Norman (University of Birmingham), Roberto Segala (University of Bologna), and Jeremy Sproston (University of Birmingham)</i>	
ProbVerus: Probabilistic Symbolic Model Checking .....	96
<i>Vicky Hartonas-Garmhausen (Carnegie Mellon University), Sergio Campos (Federal University of Minas), and Ed Clarke (Carnegie Mellon University)</i>	

## Semantics of Probabilistic Process Calculi

Process Algebra with Probabilistic Choice .....	111
<i>Suzana Andova (Eindhoven University of Technology)</i>	
An Axiomatization of Probabilistic Testing .....	130
<i>Manuel Núñez (Universidad Complutense de Madrid)</i>	

## Invited Lecture

Verification of Hybrid Systems .....	151
<i>Frits Vaandrager (University of Nijmegen)</i>	

## Semantics of Real-Time Processes

A Parallel Operator for Real-Time Processes with Predicate Transformer Semantics .....	152
<i>Karl Lerner (SVRC, University of Queensland)</i>	



Comparing the Efficiency of Asynchronous Systems ..... 172  
*Lars Jenner and Walter Vogler (University of Augsburg)*

**Real-Time Compilation**

A Formal Model of Real-Time Program Compilation ..... 192  
*Karl Lerner and Colin Fidge (SVRC, University of Queensland)*

**Stochastic Process Algebra**

Specifying Performance Measures for PEPA ..... 211  
*Graham Clark, Stephen Gilmore, and Jane Hillston  
 (LFCS, University of Edinburgh)*

Semi-numerical Solution of Stochastic Process Algebra Models ..... 228  
*Henrik C. Bohnenkamp and Boudewijn R. Haverkort (RWTH Aachen)*

Bisimulation Algorithms for Stochastic Process Algebras and Their  
 BDD-Based Implementation ..... 244  
*Holger Hermanns (University of Twente) and Markus Siegle  
 (University of Erlangen-Nürnberg)*

**Invited Lecture**

Probabilistic Linear-Time Model Checking: An Overview of the  
 Automata-Theoretic Approach ..... 265  
*Moshe Y. Vardi (Rice University)*

**Modeling and Verification of Real-Time Systems**

Formal Verification of a Power Controller Using the Real-Time Model  
 Checker UPPAAL ..... 277  
*Klaus Havelund (NASA Ames Research Center), Kim G. Larsen, and  
 Arne Skou (BRICS, Aalborg University)*

Verifying Progress in Timed Systems ..... 299  
*Stavros Tripakis (Verimag)*

Proof Assistance for Real-Time Systems Using an Interactive Theorem  
 Prover ..... 315  
*Paul Z. Kolano (University of California at Santa Barbara)*

Modelling Timeouts without Timelocks ..... 334  
*Howard Bowman (University of Kent at Canterbury)*

**Author Index** ..... 355