

Volume 23

CRM

CRM  
MONOGRAPH  
SERIES

Centre de Recherches Mathématiques  
Université de Montréal

Mathematical Techniques  
for Analyzing Concurrent  
and Probabilistic Systems

J. J. M. M. Rutten  
Marta Kwiatkowska  
Gethin Norman  
David Parker

Prakash Panangaden  
Franck van Breugel  
Editors



American Mathematical Society



# CRM MONOGRAPH SERIES

Centre de Recherches Mathématiques  
Université de Montréal

## Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems

J. J. M. M. Rutten  
Marta Kwiatkowska  
Gethin Norman  
David Parker

Prakash Panangaden  
Franck van Breugel  
Editors

The Centre de Recherches Mathématiques (CRM) of the Université de Montréal was created in 1968 to promote research in pure and applied mathematics and related disciplines. Among its activities are special theme years, summer schools, workshops, postdoctoral programs, and publishing. The CRM is supported by the Université de Montréal, the Province of Québec (FCAR), and the Natural Sciences and Engineering Research Council of Canada. It is affiliated with the Institut des Sciences Mathématiques (ISM) of Montréal, whose constituent members are Concordia University, McGill University, the Université de Montréal, the Université du Québec à Montréal, and the Ecole Polytechnique. The CRM may be reached on the Web at [www.crm.umontreal.ca](http://www.crm.umontreal.ca).



**American Mathematical Society**  
Providence, Rhode Island USA

The production of this volume was supported in part by the Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Fonds FCAR) and the Natural Sciences and Engineering Research Council of Canada (NSERC).

2000 *Mathematics Subject Classification*. Primary 68Q60; Secondary 68Q85.

---

For additional information and updates on this book, visit  
[www.ams.org/bookpages/crmm-23](http://www.ams.org/bookpages/crmm-23)

---

#### Library of Congress Cataloging-in-Publication Data

Mathematical techniques for analyzing concurrent and probabilistic systems / J.J.M.M. Rutten... [et al.]; Prakash Panangaden, Franck van Breugel, editors.

p. cm. — (CRM monograph series, ISSN 1065-8599; v. 23)

Includes bibliographical references.

ISBN 0-8218-3571-8 (alk. paper)

1. System analysis. I. Rutten, J.J.M.M. II. Panangaden, P. (Prakash). III. Breugel, Franck van, 1966– IV. Series.

QA402.M3594 2004

003–dc22

2004041069

---

**Copying and reprinting.** Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to [reprint-permission@ams.org](mailto:reprint-permission@ams.org).

© 2004 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights  
except those granted to the United States Government.

Printed in the United States of America.

⊗ The paper used in this book is acid-free and falls within the guidelines  
established to ensure permanence and durability.

This volume was submitted to the American Mathematical Society  
in camera ready form by the Centre de Recherches Mathématiques.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 09 08 07 06 05 04

# Contents

Preface	vii
<b>On Streams and Coinduction</b>	<b>1</b>
Preface	3
Acknowledgments	5
Chapter 1. Streams and Coinduction	7
1.1. Streams	7
1.2. Proofs by Coinduction	7
1.3. Definitions by Coinduction	9
1.4. Examples of Coinductive Proofs	11
1.5. Coinduction and Greatest Fixed Points	12
1.6. Other Coalgebras	13
1.7. Discussion	14
Chapter 2. Stream Calculus	15
2.1. Behavioural Differential Equations	15
2.2. Basic Stream Calculus	17
2.3. Coinduction-Up-To	21
2.4. Basic Properties	22
2.5. Infinite Sum	23
2.6. Solving Behavioural Differential Equations	25
2.7. Solving Difference Equations	28
2.8. Streams and Weighted Automata	30
2.9. Rational Streams	32
2.10. Streams and Languages	33
2.11. Discussion	34
Chapter 3. Analytical Differential Equations	37
3.1. Shuffle Product and Shuffle Inverse	37
3.2. Stream Exponentiation	39
3.3. Comparing Convolution and Shuffle Product	40
3.4. Solving Analytical Differential Equations	44
3.5. Discussion	48
Chapter 4. Coinductive Counting	51
4.1. Introduction	51
4.2. Compositions of Natural Numbers	52
4.3. Surjections	54

4.4.	Counting with Probabilities	56
4.5.	Well-Bracketed Words	56
4.6.	Streams and Continued Fractions	58
4.7.	More on Well-Bracketed Words	59
4.8.	Permutations	60
4.9.	Set Partitions	67
4.10.	Special Numbers	69
4.11.	Discussion	69
Chapter 5.	Component Connectors	73
5.1.	Introduction	73
5.2.	Timed Data Streams	74
5.3.	Basic Connectors: Channels	75
5.4.	More Channels and the Merge Connector	77
5.5.	Composing Connectors	78
5.6.	Connector Equivalence	82
5.7.	Protocol Verification	84
5.8.	Discussion	86
Appendix A.	Key Differential Equations	89
Bibliography		91
<b>Modelling and Verification of Probabilistic Systems</b>		<b>93</b>
Preface		95
Acknowledgements		95
Chapter 1.	Introduction	97
1.1.	Motivation	98
1.2.	The models	99
1.3.	Properties of Interest	100
1.4.	Probabilistic Model Checking and Other Analysis Methods	100
Chapter 2.	Discrete-Time Markov Chains	101
2.1.	Introduction	101
2.2.	Paths and Probability Measures	103
2.3.	Probabilistic Computation Tree Logic (PCTL)	104
2.4.	PCTL Model Checking	106
2.5.	Case Study: The IPv4 ZeroConf Protocol	112
2.6.	Discussion	115
Chapter 3.	Markov Decision Processes	117
3.1.	Introduction	117
3.2.	Paths and Probability Measures	118
3.3.	Probabilistic Computation Tree Logic (PCTL)	120
3.4.	PCTL Model Checking	122
3.5.	Fairness	129
3.6.	Case Study: Self-Stabilisation Algorithms	132
3.7.	Discussion	135

Chapter 4. Continuous-Time Markov Chains	137
4.1. Introduction	137
4.2. Paths and Probability Measures	139
4.3. Steady-State and Transient Behaviour	140
4.4. Continuous Stochastic Logic (CSL)	141
4.5. CSL Model Checking	142
4.6. Complexity of CSL Model Checking	148
4.7. Case Study: Dynamic Power Management	148
4.8. Discussion	153
Chapter 5. Probabilistic Timed Automata	155
5.1. Time, Clocks and Zones	155
5.2. Syntax of Probabilistic Timed Automata	156
5.3. Parallel Composition	158
5.4. Semantics of Probabilistic Timed Automata	158
5.5. Probabilistic Timed Computation Tree Logic (PTCTL)	162
5.6. Model Checking: The Region Graph Approach	164
5.7. Model Checking: The Digital Clocks Approach	169
5.8. Case Study: IEEE 1394 FireWire Root Contention	175
5.9. Discussion	180
Chapter 6. Implementation	181
6.1. Introduction	181
6.2. Sparse Matrices	182
6.3. Multi-Terminal Binary Decision Diagrams	185
6.4. Model Representation with MTBDDs	191
6.5. MTBDD-Based Model Checking	194
6.6. Discussion	200
Appendix A. Measure Theory and Probability	203
Appendix B. Iterative Solution Methods	205
B.1. The Jacobi Method	206
B.2. The Gauss–Seidel Method	206
B.3. Over-Relaxation Methods	207
Bibliography	209

*This page intentionally left blank*

## Preface

The impact of mathematics and logic on theoretical computer science has been great from its very birth. It is perhaps less widely known among general mathematicians that mathematics has had a profound impact on computer systems. It has been about 40 years since pioneers like McCarthy, Strachey, Landin, Dijkstra, Scott and deBakker, among others, provided a firm mathematical underpinning to the study of programming languages. It is also about 30 years since Robin Milner, Tony Hoare, Carl Petri and others began looking at concurrent systems from a mathematical point of view.

At this point the theory of concurrency is a very rich subject with annual conferences and journals devoted to research in concurrency theory. The first set of lectures presents a new way of thinking about concurrency; the **coalgebraic** approach. Though it was realized implicitly from the start that coalgebra plays a key role in concurrent systems, it was only made very explicit quite recently in large part because of the work of Prof. Rutten. Roughly speaking, one can say that algebra gives the syntactic structure while a coalgebra describes the behaviour or dynamics of the system. Rutten presents an elegant “calculus of streams” for reasoning coalgebraically and shows some striking formal analogies between calculus as understood in the sense of analysis and the stream calculus.

A relatively young offshoot of concurrency theory is the theory of probabilistic, concurrent systems. The second set of lectures gives an overview of modelling and analysis of such systems. In particular the focus is on **automated tools** for reasoning about the behaviour and correctness of such systems. Prof. Kwiatkowska is one of the pioneers of this area and has been the driving force behind making the transition from theory to practice with a large active group developing implementations of the reasoning tools, carrying out case studies and, of course, enriching the theory further.

Both sets of lectures are suitable for beginning graduate students and even some advanced undergraduates. This helps fill a gap which should make it easier for graduate students to gain entry into these exciting research areas. The notes were reviewed by the editors. We wish to thank the authors for being willing to take time out of their busy research schedules to write these detailed expository notes. We hope that people will enjoy reading them as much as we enjoyed listening to the lectures in Montréal.

The two sets of notes in this volume were based on lectures delivered by Prof. Jan Rutten and Prof. Marta Kwiatkowska at a workshop on “Mathematical Techniques for Analyzing Systems” held from September 30<sup>th</sup> to October 4<sup>th</sup> 2002. This workshop was part of the Année Thématique of the Centre de Recherche Mathématiques devoted to theoretical computer science and we are very grateful to the CRM and its director, Jacques Hurtubise, whose generous support made



the workshop possible. We would also like to thank the staff at CRM: Jean Le-Tourneux, André Montpetit, Louise Letendre, Louis Pelletier and Josée Laferrière who were very helpful in organizing the workshop and producing the book.

The workshop was attended by about 30 participants, including nearly a dozen students, and included several other individual lectures on the theme of the workshop. We would like to thank all the participants for their stimulating comments and the exciting atmosphere at the workshop.

Prakash Panangaden  
*McGill University*  
Montréal, Québec

Franck van Breugel  
*York University*  
Toronto, Ontario

The book consists of two sets of lecture notes devoted to slightly different methods of analysis of concurrent and probabilistic computational systems.

The first set of lectures develops a calculus of streams (a generalization of the set of natural numbers) based on the coinduction principle coming from the theory of coalgebras. It is now well understood that the interplay between algebra (for describing structure) and coalgebra (for describing dynamics) is crucial for understanding concurrent systems. There is a striking analogy between streams and formula calculus reminiscent to those appearing in quantum calculus. These lecture notes will appeal to anyone working in concurrency theory but also to algebraists and logicians.

The other set of lecture notes focuses on methods for automatically verifying probabilistic systems using techniques of model checking. The unique aspect of these lectures is the coverage of both theory and practice. The authors have been responsible for one of the most successful experimental systems for probabilistic model checking. These lecture notes are of interest to software engineers, real-time programmers, researchers in machine learning and numerical analysts who may well be interested in seeing how standard numerical techniques are used in a novel context.

Both sets of lectures are expository and suitable for graduate courses in theoretical computer science.



For additional information  
and updates on this book, visit

[www.ams.org/bookpages/crmm-23](http://www.ams.org/bookpages/crmm-23)

ISBN 0-8218-3571-8



9 780821 835715

**CRMM/23**

**AMS on the Web**  
[www.ams.org](http://www.ams.org)