ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

# Noncommutative Rational Series with Applications

JEAN BERSTEL Université Paris-Est

CHRISTOPHE REUTENAUER University of Québec, Montréal



### CAMBRIDGE UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314-321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre, New Delhi - 110025, India

103 Penang Road, #05-06/07, Visioncrest Commercial, Singapore 238467

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning and research at the highest international levels of excellence.

www.cambridge.org

Information on this title: www.cambridge.org/9780521190220

© J. Berstel and C. Reutenauer 2011

This publication is in copyright. Subject to statutory exception and to the provisions of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published 2011

A catalogue record for this publication is available from the British Library

Library of Congress Cataloging in Publication data Berstel, Jean, 1941– Noncommutative rational series with applications / Jean Berstel, Christophe Reutenauer. p. cm. – (Encyclopedia of mathematics and its applications ; 137) Includes bibliographical references and index. ISBN 978-0-521-19022-0 (hardback) 1. Machine theory. 2. Noncommutative algebras. I. Reutenauer, Christophe. II. Title. III. Series. QA267.B47 2010 511.3'5 – dc22 2010030398 ISBN 978-0-521-19022-0 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Pour Anne et Anissa

## Contents

Preface
---------

## Part I Rational series

1	Rati	ional series	3
	1.1	Semirings	3
	1.2	Formal series	4
	1.3	Topology	5
	1.4	Rational series	6
	1.5	Recognizable series	10
	1.6	Weighted automata	16
	1.7	The fundamental theorem	18
		Exercises for Chapter 1	21
		Notes to Chapter 1	26
2	Min	imization	29
	2.1	Syntactic ideals	29
	2.2	Minimal linear representations	34
	2.3	The minimization algorithm	37
		Exercises for Chapter 2	42
		Notes to Chapter 2	45
3	Seri	es and languages	47
	3.1	Kleene's theorem	47
	3.2	Series and rational languages	49
	3.3	Syntactic algebras and syntactic monoids	52
	3.4	Support	53
	3.5	Iteration	56
	3.6	Complementation	58
		Exercises for Chapter 3	61
		Notes to Chapter 3	63
		*	

page xi

viii		Contents			
4	Rati	ional expressions	65		
	4.1	Rational expressions	65		
	4.2	Rational identities over a ring	69		
	4.3	Star height	70		
	4.4	Absolute star height	77		
		Exercises for Chapter 4	78		
		Notes to Chapter 4	79		
Par	t II	Arithmetic			
5	Aut	omatic sequences and algebraic series	83		
	5.1	Regular functions	83		
	5.2	Stable submodules and operations on k-regular functions	85		
	5.3	Automatic sequences	91		
	5.4	Automatic sequences and algebraic series	93		
	5.5	Algebraic series and diagonals of rational series	97		
		Exercises for Chapter 5	102		
		Notes to Chapter 5	104		
6	Rational series in one variable				
	6.1	Rational functions	105		
	6.2	The exponential polynomial	109		
	6.3	A theorem of Pólya	114		
	6.4	A theorem of Skolem, Mahler, Lech	118		
		Exercises for Chapter 6	126		
		Notes to Chapter 6	128		
7	Cha	inging the semiring	129		
	7.1	Rational series over a principal ring	129		
	7.2	Fatou extensions	132		
	7.3	Polynomial identities and rationality criteria	136		
	7.4	Fatou ring extensions	138		
		Exercises for Chapter 7	140		
		Notes to Chapter 7	142		
8	Positive series in one variable		143		
	8.1	Poles of positive rational series	143		
	8.2	Polynomially bounded series over $\mathbb Z$ and $\mathbb N$	145		
	8.3	Characterization of $K_+$ -rational series	147		
	8.4	Star height 2	153		
		Exercises for Chapter 8	154		
		Notes to Chapter 8	158		

	Contents	ix			
Part III Applications					
9	Matrix semigroups and applications	163			
	9.1 Finite matrix semigroups and the Burnside problem	163			
	9.2 Polynomial growth	167			
	9.3 Limited languages and the tropical semiring	175			
	Exercises for Chapter 9	180			
	Notes to Chapter 9	180			
10	Noncommutative polynomials	183			
	10.1 The weak algorithm	183			
	10.2 Continuant polynomials	186			
	10.3 Inertia	190			
	10.4 Gauss's Lemma	195			
	Exercises for Chapter 10	197			
	Notes to Chapter 10	198			
11	Codes and formal series	199			
	11.1 Codes	199			
	11.2 Completeness	203			
	11.3 The degree of a code	208			
	11.4 Factorization	208			
	Exercises for Chapter 11	215			
	Notes to Chapter 11	216			
12	Semisimple syntactic algebras	217			
	12.1 Bifix codes	217			
	12.2 Cyclic languages	220			
	Appendix 1: Semisimple algebras	224			
	Appendix 2: Minimal ideals in finite monoids	225			
	Exercises for Chapter 12	230			
	Notes to Chapter 12	231			
Open problems and conjectures		233			
Ref	234				
Index of notation		242			
Index		244			

## Preface

Formal power series have long been used in all branches of mathematics. They are invaluable in algebra, analysis, combinatorics and in theoretical computer science.

Historically, the work of M.-P. Schützenberger in the algebraic theory of finite automata and the corresponding languages has led him to introduce noncommutative formal power series. This appears in particular in his work with Chomsky on formal grammars. This last point of view is at the origin of this book.

The first part of the book, composed of Chapters 1–4, is especially devoted to this aspect: Formal power series may be viewed as formal languages with coefficients, and finite automata (and more generally weighted automata) may be considered as linear representations of the free monoid. In this sense, via formal power series, algebraic theory of automata becomes a part of representation theory.

The first two chapters contain general results and discuss in particular the equality between rational and recognizable series (Theorem of Kleene–Schützenberger) and the construction of the minimal linear representation. The exposition illustrates the synthesis of linear algebra and syntactic methods inherited from automata theory.

The next two chapters are concerned with the comparison of some typical properties of rational (regular) languages, when they are transposed to rational series. First, Chapter 3 describes the relationship with the family of regular languages studied in theoretical computer science. Next, the chapter contains iteration properties for rational series, also known as pumping lemmas, which are much more involved than those for regular languages. Chapter 4 discusses rational expressions. It contains two main results: the so-called "triviality" of rational identities over a commutative ring and the characterization of the star height of a rational series and its two consequences: the star height is unbounded and the star height over an algebraically closed field is decidable. The same problem for rational languages is known to be extremely difficult.

The second part of the book, composed of Chapters 5–8, is devoted to arithmetic properties of rational series.

Chapter 5 is concerned with automatic sequences and algebraic series. Two main results are the characterization of algebraic series over a finite field by Christol, Kamae, Mendès France and Rauzy, and Fürstenberg's theorem on the diagonal of a rational function.

xii

#### Preface

Chapter 6 gives the proof of a theorem of Pólya characterizing rational series whose set of coefficients have only finitely many distinct prime divisors, and an elementary proof of a theorem of Skolem, Mahler and Lech about vanishing terms in a rational series.

Chapter 7 studies rational series over a principal ring and Fatou extensions. It contains a section on polynomial identities and rationality criteria, and a section on Fatou rings.

Chapter 8 is concerned with rational series with nonnegative coefficients. It contains a simplified proof of Soittola's theorem (Theorem 8.3.1) which is one of the most striking results on these rational series in one variable. Also the presentation of the star height (Theorem 8.4.1) is new.

The third part, composed of the remaining four chapters, is concerned with applications and with the study of important subfamilies of rational series.

Chapter 9 contains some results appearing for the first time in book form. The first section is on the Burnside problem of matrix semigroups. Section 9.2 contains a main result: Schützenberger's theorem on polynomially bounded rational series, one of the most difficult results in the area. The chapter also contains Simon's result on the Burnside problem for the matrix semigroups over the tropical semiring and limitedness of languages.

The next two chapters are devoted to the study of polynomials in noncommutative variables, and to their application to coding theory. Because of noncommutativity, the structure of polynomials is much more complex than in the case of commutativity, and the results are rather delicate to prove. We present here basic properties concerning factorizations. The main purpose of Chapter 10 is to prepare the ground for Chapter 11. The latter contains the generalization of a result of M.-P. Schützenberger concerning the factorization of a polynomial associated with a finite code.

Chapter 12 is a step towards representation theory. It gives results on semisimple syntactic algebras. Main results are the semisimplicity of the syntactic algebra of bifix codes and its converse. The syntactic algebra of a cyclic language is semisimple and its zeta function is rational. The chapter also contains a long appendix on the Rees–Suschkewitsch theorem which describes the structure of the minimal idea of a finite monoid. We included a self-contained exposition for the ease of the reader.

More than 170 exercises are provided, and also short bibliographical notes are given at the end of the chapters.

This book is issued from a previous book of the authors, entitled *Rational Series and their Languages*. The present text is an entirely rewritten and enriched version of this book. An important part of the material presented here appears for the first time in book form.

The text served for advanced courses held several times by the authors, at the University Pierre et Marie Curie, Paris and at the University of Saarbrücken. Parts of the book were also taught at several different levels at other places, such as the University of Québec at Montréal and the University of Marne-la-Vallée.

Many thanks to Sylvain Lavallée, Aaron Lauve, Martin Dagenais, Pierre Bouchard, Franco Saliola, Dominique Perrin and to Christian Mathissen for their help.

#### Preface

Note to the reader

Following usual notation, items such as sections, theorems, corollaries, etc. are numbered within a chapter. When cross-referenced the chapter number is omitted if the item is within the current chapter. Thus "Theorem 1.1" means the first theorem in the first section of the current chapter, and "Theorem 2.1.1" refers to the equivalent theorem in Chapter 2. Exercises are numbered accordingly and the section number should help the reader to find the section relevant to that exercise.