

SpringerBriefs in Computer Science

Series Editors

Stan Zdonik

Peng Ning

Shashi Shekhar

Jonathan Katz

Xindong Wu

Lakhmi C. Jain

David Padua

Xuemin Shen

Borko Furht

VS Subrahmanian

Martial Hebert

Katsushi Ikeuchi

Bruno Siciliano

For further volumes:

<http://www.springer.com/series/10028>

Nigel Boston

Applications of Algebra to Communications, Control, and Signal Processing

Nigel Boston
University of Wisconsin
Madison, WI, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
ISBN 978-1-4614-3862-5 ISBN 978-1-4614-3863-2 (eBook)
DOI 10.1007/978-1-4614-3863-2
Springer New York Heidelberg Dordrecht London

Library of Congress Control Number: 2012935583

© The Author 2012

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed. Exempted from this legal reservation are brief excerpts in connection with reviews or scholarly analysis or material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work. Duplication of this publication or parts thereof is permitted only under the provisions of the Copyright Law of the Publisher's location, in its current version, and permission for use must always be obtained from Springer. Permissions for use may be obtained through RightsLink at the Copyright Clearance Center. Violations are liable to prosecution under the respective Copyright Law.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

*This book is dedicated to my wife, Susan Ann
Boston.*

Preface

Over the years, engineers and computer scientists have increasingly begun to use mathematical tools. Currently, it is standard for students in these fields to learn some complex analysis, probability, and statistics. There has, however, been a quietly growing introduction of tools from abstract algebra. Traditionally these have been used mostly in coding theory and cryptography, but there are emerging new areas of application for abstract algebra. For example, the first Applied Algebra Days conference, co-organized by the author and Shamgar Gurevich, took place in October, attracting speakers from Berkeley, Chicago, MIT, and other eminent institutions. That same month, the SIAM Activity Group in Algebraic Geometry held its first biannual conference. Both conferences covered very new approaches to applying algebra and both attracted researchers from mathematics, electrical engineering, and computer science.

This book is based on a 2004 course given by the author for graduate students from the Departments of Mathematics, Electrical Engineering, and Computer Science at the University of Wisconsin, but also incorporates a few more recent developments. It gathers into themes some of the main tools that are used today in applications and explains how they are used. This book should appeal to mathematicians wishing to see where what they know gets applied and to engineers and computer scientists wanting to learn more useful, modern tools.

Madison, WI

Nigel Boston
January 2012

Acknowledgements

Back in 1992, while visiting the Isaac Newton Institute in Cambridge, UK, which had just opened and where the library had very few books, I read the coding theory book by Van der Geer and Van Lint and suggested to my then student, Judy Walker, that she look into the subject. There began a journey into applications of algebra that was made easier by many helpful colleagues at the University of Illinois at Urbana-Champaign, most notably Dick Blahut and Ralf Koetter, but also Alex Vardy, Pierre Moulin, and Yi Ma. Since moving to the University of Wisconsin in 2002, several others have helped me in this quest, including Rob Nowak, Yu Hen Hu, Chuck Dyer, Steve Wright, and Bob Barmish. Outside of these institutions, other colleagues including Rob Calderbank, Gary McGuire, Judy Walker, Michael Gastpar, and Joachim Rosenthal, all of whom have worked on introducing deep algebraic tools into electrical engineering, have always been of the utmost help. I thank you all.

Contents

- 1 Introduction** 1
- 2 Algebraic Tools** 5
 - 2.1 Groups 5
 - 2.2 Fields and Division Rings 7
 - 2.3 Field Construction 9
 - 2.3.1 Quadratic Fields 10
 - 2.3.2 Cyclotomic Fields 11
 - 2.4 General Field Extensions 11
 - 2.5 Curves and Function Fields 12
 - 2.5.1 Counting Points 13
 - 2.5.2 Elliptic Curves 13
 - 2.6 Quaternions as Rotations 14
 - References 16
- 3 Traditional Applications** 17
 - 3.1 Coding Theory 17
 - 3.2 Cyclic Codes 18
 - 3.3 Linear Feedback Shift Registers 20
 - 3.4 Private-Key Cryptography 20
 - 3.5 Public-Key Cryptography 21
 - References 23
- 4 Recent Applications to Communications** 25
 - 4.1 Space-Time Codes 25
 - 4.1.1 Rayleigh Flat-Fading Model 26
 - 4.1.2 Closed under Multiplication 27
 - 4.1.3 Closed under Addition 29
 - 4.2 Network Coding 30
 - 4.3 Low Discrepancy Sequences 31
 - 4.3.1 Algebraic-Geometry Codes 33

References	34
5 Emerging Applications to Signal Processing	35
5.1 Filters	35
5.1.1 Makhoul's Conjecture	36
5.1.2 Pipelining	36
5.1.3 The Belgian Chocolate Problem	37
5.2 Image Processing	39
References	41
Glossary	43

Acronyms

fpf	Fixed-point-free
LFSR	Linear feedback shift register
PSK	Phase-shift keying
SNR	Signal-to-noise ratio
STBC	Space-time block code
STTC	Space-time trellis code