

SpringerBriefs in Mathematics

Series Editors

Nicola Bellomo

Michele Benzi

Palle Jorgensen

Tatsien Li

Roderick Melnik

Otmar Scherzer

Benjamin Steinberg

Lothar Reichel

Yuri Tschinkel

George Yin

Ping Zhang

SpringerBriefs in Mathematics showcases expositions in all areas of mathematics and applied mathematics. Manuscripts presenting new results or a single new result in a classical field, new field, or an emerging topic, applications, or bridges between new results and already published works, are encouraged. The series is intended for mathematicians and applied mathematicians.

More information about this series at <http://www.springer.com/series/10030>

SBMAC SpringerBriefs

Editorial Board

Carlile Lavor

University of Campinas (UNICAMP)
Institute of Mathematics, Statistics and Scientific Computing
Department of Applied Mathematics
Campinas, Brazil

Luiz Mariano Carvalho

Rio de Janeiro State University (UERJ)
Department of Applied Mathematics
Graduate Program in Mechanical Engineering
Rio de Janeiro, Brazil

The **SBMAC SpringerBriefs** series publishes relevant contributions in the fields of applied and computational mathematics, mathematics, scientific computing, and related areas. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic.

The Sociedade Brasileira de Matemática Aplicada e Computacional (Brazilian Society of Computational and Applied Mathematics, SBMAC) is a professional association focused on computational and industrial applied mathematics. The society is active in furthering the development of mathematics and its applications in scientific, technological, and industrial fields. The SBMAC has helped to develop the applications of mathematics in science, technology, and industry, to encourage the development and implementation of effective methods and mathematical techniques for the benefit of science and technology, and to promote the exchange of ideas and information between the diverse areas of application.

<http://www.sbmac.org.br/>



Sueli I.R. Costa • Frédérique Oggier
Antonio Campello • Jean-Claude Belfiore
Emanuele Viterbo

Lattices Applied to Coding for Reliable and Secure Communications

Sueli I.R. Costa
Institute of Mathematics,
Statistics and Computer Science
University of Campinas
Campinas, São Paulo, Brazil

Frédérique Oggier
Division of Mathematical Sciences, School
of Physical and Mathematical Sciences
Nanyang Technological University
Singapore, Singapore

Antonio Campello
Department of Electrical
and Electronic Engineering
Imperial College London
London, UK

Jean-Claude Belfiore
Communications and Electronics
Department
Télécom ParisTech
Paris, France

Emanuele Viterbo
Department of Electrical and
Computer Systems Engineering
Monash University
Clayton, VIC, Australia

ISSN 2191-8198

ISSN 2191-8201 (electronic)

SpringerBriefs in Mathematics

ISBN 978-3-319-67881-8

ISBN 978-3-319-67882-5 (eBook)

<https://doi.org/10.1007/978-3-319-67882-5>

Library of Congress Control Number: 2017959367

© The Author(s) 2017

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.

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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1	Introduction	1
2	Lattices and Applications	5
2.1	Sphere Packing and Covering	11
2.1.1	Equivalent Lattices	16
2.2	Sublattices	17
2.3	The Dual of a Lattice	20
2.4	Important Lattices and Their Duals	21
2.4.1	Table of Record Lattices	24
2.5	Applications	26
2.5.1	Coding	26
2.5.2	Quantization	29
2.5.3	Computational Problems and Cryptography	30
3	Lattices from Codes	37
3.1	Construction A	37
3.2	Relevant Distances in Codes and Lattices	46
3.2.1	q -ary Lattice Decoding	53
3.3	Wiretap Coding and Theta Series	53
4	Ideal Lattices	59
4.1	Ideal Lattices from Quadratic Fields	59
4.1.1	Lattice Constructions	60
4.1.2	Some Sublattices	65
4.1.3	Coding Applications	65
4.1.4	High-Dimensional Lattices	67
4.2	Ideal Lattices for Cryptography	68
5	Lattices and Spherical Codes	73
5.1	Spherical and Geometrically Uniform Codes	73
5.2	Flat Tori	75

5.3	Commutative Group Codes, Flat Tori, and Lattices	77
5.3.1	Commutative Group Codes	77
5.3.2	Lattice Connections	79
5.3.3	Approaching the Bound: Good and Optimum Commutative Group Codes	81
5.3.4	Commutative Group Codes and Codes on Graphs	84
5.4	Spherical Codes on Layers of Tori	85
5.4.1	Codes for the Gaussian Channel	85
5.4.2	Application: Coding for Continuous Alphabet Sources	87
6	Lattices and Index Coding	93
6.1	Introduction	93
6.2	Voronoi Constellations	96
6.3	Index Coding in AWGN Channel	98
6.4	Voronoi Constellations for Index Coding: An Illustration	101
6.5	Lattice Index Codes	104
6.5.1	An Upper Bound on the Side Information Gain	107
6.6	A Construction of Lattice Index Codes Using the Chinese Remainder Theorem	109
6.7	Discussion	111
	References	113
	Index	119