Lattice Coding for Signals and Networks

A Structured Coding Approach to Quantization, Modulation and Multi-user Information Theory

Unifying information theory and digital communication through the language of lattice codes, this book provides a detailed overview for students, researchers and industry practitioners.

It covers classical work by leading researchers in the field of lattice codes and complementary work on dithered quantization and infinite constellations, and then introduces the more recent results on “algebraic binning” for side-information problems, and linear/lattice codes for networks. It shows how high-dimensional lattice codes can close the gap to the optimal information theoretic solution, including the characterization of error exponents.

The solutions presented are based on lattice codes, and are therefore close to practical implementations, with many advanced setups and techniques, such as shaping, entropy-coding, side-information and multi-terminal systems. Moreover, some of the network setups shown demonstrate how lattice codes are potentially more efficient than traditional random coding solutions, for instance when generalizing the framework to Gaussian networks.

Ram Zamir is a Professor at the Department of Electrical Engineering Systems at Tel-Aviv University, Israel. He consults in the areas of radar and communications (DSL and WiFi), and is the Chief Scientist of Celeno Communications.

Lattice Coding for Signals and Networks

A Structured Coding Approach to Quantization, Modulation and Multi-user Information Theory

RAM ZAMIR
Tel Aviv University

with contributions by

BOBAK NAZER
Boston University

and

YUVAL KOCHMAN
The Hebrew University of Jerusalem

and with illustrations by

Ilai Bistritz

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

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/9780521766982

First published 2014

Printed in the United Kingdom by Clays, St Ives plc

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

Library of Congress Cataloguing in Publication data
Zamir, Ram.
Lattice coding for signals and networks : a structured coding approach to quantization, modulation, and multiuser information theory / Ram Zamir, Tel Aviv University.
pages cm
Includes bibliographical references and index.
ISBN 978-0-521-76698-2 (hardback)
1. Coding theory. 2. Signal processing – Mathematics. 3. Lattice theory. I. Title.
TK5102.92.Z357 2014
003′.54 – dc23 2014006008

ISBN 978-0-521-76698-2 Hardback

To my parents Eti and Sasson Zamir

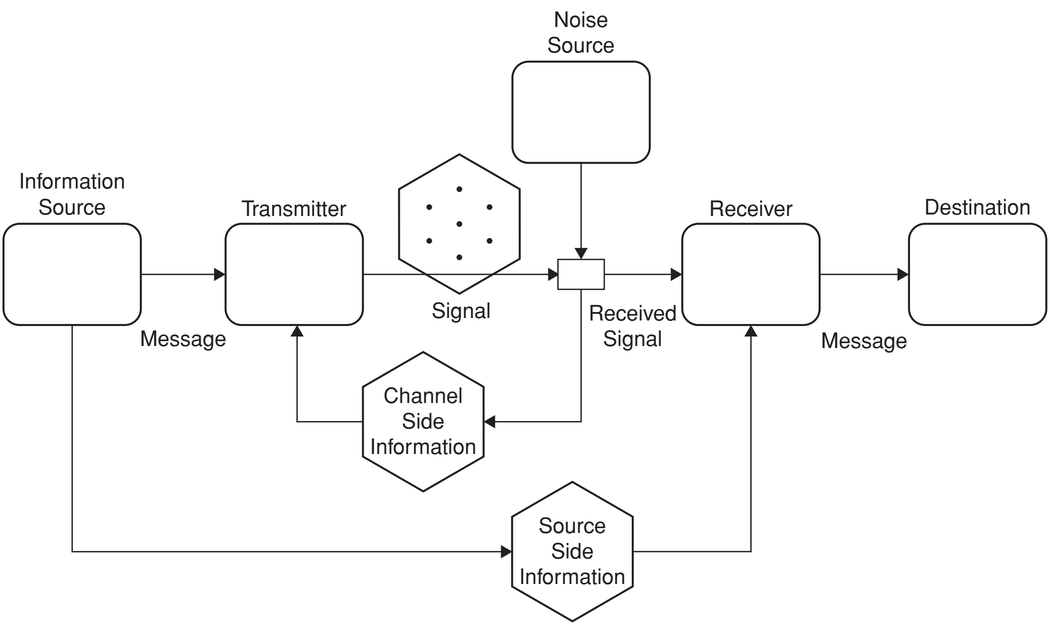
Cambridge University Press
978-0-521-76698-2 - Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multi-User Information Theory
Ram Zamir
Frontmatter
More information

Contents

Cambridge University Press
978-0-521-76698-2 - Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multi-User Information Theory
Ram Zamir
Frontmatter
More information

Preface

Digital communication and information theory talk about the same problem from very different aspects. Lattice codes provide a framework to tell their mutual story. They suggest a common view of source and channel coding, and new tools for the analysis of information network problems.



This book makes the language of quantization and modulation more accessible to the hard core information theorist. For him or her, lattices serve as a bridge from the high dimension of Shannon's theory to that of digital communication techniques. At the same time, lattices provide a useful tool for the communication engineer, whose scope is usually limited to the low – sometimes even one or two – dimensions of practical modulation schemes (e.g., QAM or PCM). She or he can "see," through the lattice framework, how signals and noise interact as the dimension increases, for example, when modulation is combined with coding. Surprisingly for both disciplines, the generalization of the lattice framework to “Gaussian networks” is not only very natural, but in some cases is more powerful than the traditional techniques.

This book is beneficial to the “Gaussian-oriented” information theorist, who wishes to become familiar with network information theory from a constructive viewpoint (as opposed to the more abstract random-coding/random-binning approach). And it is a useful tool for the communication practitioner in the industry, who prefers a “geometric” and “signal-processing oriented” viewpoint of information theory in general, and multi-user problems in particular. The algebraic coding theorist can celebrate the variety of new applications for lattice codes found in the book. The control theorist, who wishes to add communication constraints into the system, will find the linear-additive model of dithered lattice quantization useful. Other readers, like those having a background in signal processing or computer networks, can find potential challenges in the relations to linear estimation and network coding.

Ram Zamir
Tel Aviv
March 2014

Acknowledgements

In the spring of 1989 I took a data compression course with Meir Feder at Tel Aviv University, and read Jacob Ziv's 1985 article "On universal quantization." Ziv showed that the redundancy of a randomized (dithered) uniform scalar quantizer is always bounded by ≈0.754 bit; he also stated, without a proof, that if the scalar quantizer is replaced by a "good" high-dimensional lattice quantizer, then this universal bound can be reduced to half a bit – provided that Gersho's conjecture is true. In my final project – while learning about Gersho's conjecture and verifying Ziv's statement – I fell in love with the world of lattice codes.

Many people with whom I have collaborated since then have contributed to the material presented in this book. The roots of the book are in my MSc and PhD research – under Meir's supervision – about entropy-coded dithered lattice quantization (ECDQ) of signals. Tamas Linder offered rigorous proofs for some of the more technical results (and became my colleague and coauthor for many years). Two other staff members in the EE department in Tel Aviv University – Gregory Poltyrev and Simon Litsyn – while contributing from their wide knowledge about lattices, opened the way to the later applications of dithered lattice codes to signaling over the AWGN channel.

Toby Berger – my post-doctoral mentor at Cornell University in the years 1994–1995 – introduced me to the fascinating world of multi-terminal source coding. This became the first instance where randomized lattice codes were applied in network information theory. A year later, Shlomo Shamai and Sergio Verdú, with whom I communicated about systematic lossy source-channel codes, inspired me to introduce the idea of nested lattices for the Wyner–Ziv (source coding with side information) problem. This idea, which started as a toy example for a more practical systematic source-channel code, grew later into a general framework for "algebraic binning" for information networks.

Uri Erez took my first advanced information theory course in the spring of 1997; in his final project he developed an interesting technique for using channel-state information at the transmitter. His PhD research then became a fusion center of many ideas in lattice coding for noisy channels: following a pointer given to us by Shlomo Shamai to the Costa problem, Uri came up with the innovative idea of lattice pre-coding for the "dirty-paper" channel (a channel with interference known at the transmitter), using dither and Wiener estimation. Simon Litsyn helped in showing the existence of lattices which are "good for almost everything," which turned out to be a crucial element in the asymptotic optimality of nested lattice based coding schemes for general network problems. Dave Forney provided insightful comments about Uri's work, and – after noticing that the zero-interference case resolves an open question about lattice decoding of Voronoi codes – summarized his interpretations under the multiple-meaning title "Shannon meets Wiener" (2002).

Emin Martinian and Greg Wornell contributed the idea of lattice codes with variable partition (for source coding with distortion side information at the encoder) during my Sabbatical at MIT in 2002–2003.

The work in my research group during the years 2003–2010 revealed two new exciting aspects of lattice codes. Yuval Kochman developed the modulo-lattice modulation technique for joint source-channel coding, and in particular, for bandwidth conversion (an idea proposed earlier in Zvi Reznic's PhD work). Tal Philosof discovered (during his PhD research with Uri Erez and myself) that lattice codes are stronger than random codes for the "doubly dirty" multiple-access channel.

Although the material had been there for quite a few years, it took some courage and encouragement to initiate this book project. The idea was thrown into the air during my visit at Andy Loeliger and Amos Lapidoth's groups at ETH, in the summer of 2008, and suggested again by Jan Østergaard during my visit at Aalborg University a couple of months later. Dave Forney gave me important comments and suggestions in the early stages of the writing, and I thank him for that. Tom Cover, whose book with Joy Thomas was a source of inspiration for many years, was kind enough to give me a few writing-style tips during my visit at Stanford in the summer of 2009.

Our research students in Tel Aviv University provided enormous help during the writing of this book. The chapter about lattice error exponents grew from extensive discussions with Amir Ingber. Sergey Tridenski and Arie Yeredor made specific contributions to the section on error exponents for Voronoi codebooks. Or Ordentlich and Uri Erez helped me shape the material about the existence of good lattices and nested lattices. My thanks are due to Yuval Domb, Eli Haim, Anatoly Khina, Adam Mashiach, Nir and Michal Palgy, Nir Weinberger and Yair Yona for many fruitful discussions; and to the students who participated in my "Lattices in information theory" course in the fall of 2011 for the valuable feedback.

Special thanks are due to my programming assistant Ilai Bistritz, whose good advice went much beyond the numerical work, graphs and illustrations that he contributed to this book.

During the work I received help and good advice from Ofer Amrani, Benny Appelbaum, Joseph Boutrus, Shosh Brosh-Weitz, Robert Calderbank (who gave me his class notes on coded modulation), Avner Dor, Moran and Tal Gariby, Michael Gastpar, Bo'az Klartag, Frank Kschischang, Stella Achtenberg, Tamas Linder, Bobak Nazer, Jan Østergaard, Dan Rephaeli, Kenneth Rose, Yaron Shany, Anelia Somekh-Baruch and Alex Vardy. (And I have surely missed here some important people who helped along the way.) Comments on early drafts of the book were kindly provided by Ling Cong, Adam Mashiach, Jan Østergaard, Danilo Silva, Shlomo Shamai and Yaron Shani, who also provided references and pointers.

This writing project could last forever without the constant attention and professional advice of my editors at Cambridge University Press, Phil Meyler, Sarah Marsh and Mia Balashova.

I was extremely happy when Bobak Nazer agreed to join me in writing the chapter about Gaussian networks; his deep understanding of the subject and clear writing style took this part of the book to a much higher level. Also the chapter about modulo-lattice modulation greatly benefitted from the collaboration in writing with Yuval Kochman.

Last but not least, I could not have survived these four long years of writing without the infinite love and patience of my wife Ariella and three children Kessem, Shoni and Itamar.

Notation

Lattices

Λ	lattice
G	generating matrix (columns are basis vectors)
$\det(\Lambda)$	lattice determinant
$\mathcal{P}_0$	fundamental cell
$\mathcal{V}_0$, $\mathcal{V}_\lambda$	fundamental Voronoi cell, Voronoi cell of lattice point λ
$V(\Lambda)$	cell volume
$\gamma(\Lambda)$	point density
$\bmod \Lambda$, $\bmod_{\mathcal{P}_0} \Lambda$, $\mathbf{x}/\Lambda$	modulo-lattice operations
$Q_\Lambda(\cdot)$	lattice quantizer
$Q_\Lambda^{(NN)}(\cdot)$	nearest-neighbor lattice quantizer
$d_{\min}$	minimum distance
$N_\Lambda(d)$	number of lattice points at distance d from the origin
$N_\Lambda(d_{\min})$	kissing number of Λ
$r_{\text{pack}}(\Lambda)$, $r_{\text{cov}}(\Lambda)$	packing radius, covering radius
$r_{\text{eff}}(\Lambda)$	effective radius
$\rho_{\text{pack}}(\Lambda)$, $\rho_{\text{cov}}(\Lambda)$	packing and covering efficiencies
$\sigma^2(\Lambda)$	second moment
$G(\Lambda)$	normalized second moment (NSM)
$\Gamma_q(\Lambda)$, $\Gamma_s(\Lambda)$	vector-quantizer granular gain, shaping gain
$P_e(\Lambda, \sigma^2)$	error probability (in the presence of AWGN)
$\mu(\Lambda, \sigma^2)$	volume to noise ratio (VNR)
$\mu(\Lambda, P_e)$	normalized volume to noise ratio (NVNR)
$\mu_{\text{matched}}(\Lambda, \mathbf{Z}, P_e)$	noise-matched NVNR
$\mu_{\text{euclid}}(\Lambda, \mathbf{Z}, P_e)$	Euclidean (mismatched) NVNR
$\mu_{\text{mix}}(\Lambda_1, \Lambda_2, P_e, \alpha)$, $\mu_{\text{mix}}(\Lambda_1, \Lambda_2, P_e, \xi)$	mixture-noise NVNR
$\Gamma_c(\Lambda, P_e)$	coding gain (relative to cubic lattice)
$\mathbf{U}$, $\mathbf{U}_{\text{eq}}$	dither, equivalent dithered quantization noise
R_{ECDQ}	entropy rate of lattice quantizer
$R_\infty(\Lambda)$	rate per unit volume

$\mathbb{L}$	Minkowski–Hlawka–Siegel (MHS) ensemble
$N_{\mathcal{S}}(\Lambda)$	number of non-zero lattice points in $\mathcal{S}$
J	nesting matrix
$\Gamma = \Gamma(\Lambda_1, \Lambda_2)$	nesting ratio
Λ_1/Λ_2	quotient group, relative cosets
$\mathcal{C}_{\Lambda_1,\mathcal{P}_0(\Lambda_2)},\ \mathcal{C}_{\Lambda_1,\mathcal{V}_0(\Lambda_2)}$	lattice-shaped codebook, Voronoi codebook
$\mathcal{C}_{\mathbf{u},\Lambda_1,\mathcal{P}_0}$	dithered codebook
$R(\Lambda_1/\Lambda_2)$	codebook rate [bit per dimension]
$\mathbf{Z}_{\text{eq}}$	equivalent noise in mod Λ channel

Information theory

$H(X)$	regular entropy (of random variable X)
$H_B(p)$	binary entropy
$h(X)$	differential entropy
$I(X;Y)$	mutual information (between a pair of random variables)
$P_E(X)$	entropy power of a random variable ($P_E(X) = 2^{2h(X)}/2\pi e$)
C	channel capacity
C_∞	capacity per unit volume (Poltyrev's capacity)
$C^{(d)}, C^{(\text{euclid-th})}$	mismatched capacities
$R(D)$	rate-distortion function
$\mathcal{A}_\epsilon^{(n)}$	typical set
$\mathcal{C}$	codebook
$r_{\text{noise}} = \sqrt{n\sigma^2}$	typical AWGN radius

General

x, y	scalar variables
$\mathbf{x}, \mathbf{y}$	vector variables
X, Y	random variables
$\mathbf{X}, \mathbf{Y}$	random vectors (column form)
$\mathbf{X}^t$	$\mathbf{X}$ transpose (row form)
$\text{Var}(\mathbf{X})$	average variance per dimension
$\mathbb{R}^n$	Euclidean space
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$	integers
$\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$	modulo-q group
$N(\mu, \sigma^2)$	Gaussian distribution with mean μ and variance σ^2
$\mathcal{B}_r$	a ball of radius r centered about the origin
$\mathcal{B}(\mathbf{x}, r)$	a ball of radius r centered at $\mathbf{x}$
V_n	volume of a unit-radius n-dimensional ball

$\mathrm{Vol}(S)$	volume of a set S
$\doteq$	equality to the first order in the exponent
$\otimes$	binary convolution ($p \otimes q = p(1-q) + q(1-p)$)
$[x]^+$	maximum between x and zero.

Abbreviations

AWGN	additive white-Gaussian noise
BPSK	binary phase-shift keying
BSC	binary-symmetric channel
BSS	binary-symmetric source
ECDQ	entropy-coded dithered quantization
MAC	multiple-access channel
ML	maximum likelihood
MSE	mean-squared error
NN	nearest-neighbor
NSM	normalized second moment
NVNR	normalized volume to noise ratio
PAM/QAM	pulse/quadrature-amplitude modulation
PAPR	peak to average power ratio
SER	symbol error rate
SNR	signal to noise ratio
VNR	volume to noise ratio
VNER	volume to noise entropy power ratio
VRDM	variable-rate dithered modulation