Provided for non-commercial research and education use.
Not for reproduction, distribution or commercial use.

ELSEVIER

AEÜ

International Journal of Electronics and Communications

Contents

◆ www.elsevier.de/aeue

ISSN 1434-8411
Int. J. Electron. Commun. (AEÜ)
64(2010)5 · pp. 383–488

5/2010
Volume 64

This article appeared in a journal published by Elsevier. The attached copy is furnished to the author for internal non-commercial research and education use, including for instruction at the authors institution and sharing with colleagues.

Other uses, including reproduction and distribution, or selling or licensing copies, or posting to personal, institutional or third party websites are prohibited.

In most cases authors are permitted to post their version of the article (e.g. in Word or Tex form) to their personal website or institutional repository. Authors requiring further information regarding Elsevier's archiving and manuscript policies are encouraged to visit:

http://www.elsevier.com/copyright

Author's personal copy

Available online at www.sciencedirect.com
ScienceDirect

Int. J. Electron. Commun. (AEÜ) 64 (2010) 450–464

International Journal AEÜ of Electronics and Communications

www.elsevier.de/aeue

On rate and BER analysis for finite-dimensional lattice coding for the dirty paper channel

Abdellatif Zaidi[a,*], Pierre Duhamel[b]

[a]*École Polytechnique de Louvain, Université Catholique de Louvain, Louvain-la-Neuve 1348, Belgium*
[b]*Laboratoire des Signaux et Systèmes, LSS/CNRS, Supélec, 91192 Gif sur Yvette Cedex, France*

Received 17 October 2008; accepted 28 February 2009

Abstract

Costa's dirty paper coding (DPC) offers a good framework for precoding for transmission over additive Gaussian channels with additive states non-causally known at the transmitter but not at the receiver. In this paper, rate calculation, error probability analysis and code design for DPC are investigated from a practical point-of-view. Based on Monte-Carlo numerical integration and simulations, we first show that the gap to the full AWGN capacity can be partially bridged using some finite-dimensional lattices with good packing and quantizing properties. Then the difficult problem of codebook selection is addressed through some illustrative examples. Analysis sheds light on the dual roles of "packing" and "shaping" as well as on their inter-connection at finite-dimensional coding, by opposition to the asymptotic case (i.e., infinite dimension) where the two coding components are decoupled.

© 2009 Elsevier GmbH. All rights reserved.

Keywords: Dirty paper coding; Modulo channel; Lattice quantization; Capacity; Shaping and coding gains

1. Introduction

Costa's dirty paper coding (DPC) [1] offers a good framework for the design of precoding techniques for transmission over additive Gaussian channels with additive Gaussian channel state information (CSI) available non-causally at the transmitter but not at the receiver. The CSI may model an interference which is known (non-causally) to only the transmitter. Precoding techniques have been initially conceived for inter-symbol interference (ISI) cancelation in the framework of the well-known Tomlinson–Harashima precoding [2,3]. After that, there has been an extensive interest in the use of DPC techniques for interference cancelation in a variety of other applications. Examples of such applications include information embedding (IE) and watermarking [4–8,41–43] where the signal to be marked acts as interference, transmission over digital subscriber lines [9] where the crosstalk between different telephone lines handled together in their way to the central office acts as interference and coding for Gaussian dispersive (ISI) channels [10]. Another promising application is that of coding for multiple-input multiple-output (MIMO) broadcast channels (see e.g., [11–14] and references therein) where the signal sent to one user acts as interference in the eyes of other users.

Capacity of DPC-based schemes has been widely studied theoretically for various situations (e.g., see [11,15–19]). For instance, it has been shown that these schemes are able of attaining the full AWGN capacity and of completely nullifying the effect of the interference, i.e., the CSI, as if this interference were either zero or known also by the receiver. The theoretical proof is based on a random binning argument which dates back to Gel'fand and Pinsker's "coding for channels with random parameters" [20] and which is unfeasible in practice. Consequently, designing DPC-based schemes

[*] Corresponding author.
E-mail addresses: abdellatif.zaidi@uclouvain.be (A. Zaidi), Pierre.Duhamel@lss.supelec.fr (P. Duhamel).

1434-8411/$ - see front matter © 2009 Elsevier GmbH. All rights reserved.
doi:10.1016/j.aeue.2009.02.010

Author's personal copy

with manageable complexity has been a challenging problem over the last years. Existing feasible DPC schemes previously reported in literature are very often based on a modulo-reduction (i.e., quantization) operation. Quantization for coding for DPC has been first suggested in [2,21] and then carried further in [22]. For instance, it has been shown in [22] that lattice quantization [23] is capable of canceling the effect of the interference, thus achieving the full AWGN capacity. However, this is possible only asymptotically, i.e., when the dimension of the lattice used for quantization goes to infinity. In practice, finite-dimensional lattice quantization does not achieve full AWGN capacity, but it allows to partially bridge the gap to it [24,25].

In this work, we rely heavily on recent results on modulo channels [10,22] to assess the improvement brought by lattice quantization (over scalar schemes) in finite-dimensional lattice coding for DPC, mostly from a numerical point-of-view. Analysis is based on both rate and bit error rate (BER), obtained by Monte-Carlo integrations and simulations, respectively. First, we use Monte-Carlo integration techniques to numerically compute the rates allowed by the use of some finite-dimensional lattices and investigate the resulting improvement (over scalar schemes) in terms of the associated shaping gains. Then, we turn to BER computation and address the problem of optimal codebook selection. By exploiting the appealing algebraic structure of the lattice, different possible choices of lattice codes are compared, thus raising the question of an unavoidable trade-off between reliable transmission (low error rates) and high transmission rates. This allows us to identify the dual roles of coding and shaping in coding for DPC channels, numerically. Also, we emphasize the interaction between shaping and coding by presenting and discussing some low-complexity finite-dimensional illustrative implementations. We note that, though well expected, the curves presented in this paper (especially, the BER curves) have the merit of clearly showing how much (or little) one can expect from lattice quantization for DPC in practice, as classically performance are depicted for one- or two-dimensional schemes only. Also, though assessed mostly from a numerical point-of-view, many of the results, observations and discussions in this paper are useful in the design of practical implementations and reflect how difficult (or easy) is system design for DPC based on lattice coding.

The rest of this paper is organized as follows. Section 2 recalls some preliminary definitions and results from lattice theory that we will use throughout the paper. Also, it provides a brief review of some applications of DPC. Sections 3 and 4 contain numerical computation of both rates and BERs allowed by the use of some carefully tuned low-dimensional lattice codes. For BER analysis, end-to-end system design is proposed for various choices of lattice codes and the roles of shaping and coding are discussed. In Section 5 we outline the practical usefulness of the results presented in this paper and illustrate the interaction between shaping and coding at finite-dimensional lattice coding for DPC. Finally, we close with a conclusion in Section 6.

1.1. Notation

Throughout this paper, boldface fonts denote vectors and matrices. We use lowercase letters to denote vectors and uppercase letters to denote matrices. For example, a vector $\mathbf{x}$ with n elements x_i is denoted by $\mathbf{x}=(x_1, x_2, \dots, x_n)$, and a matrix $\mathbf{H}$ with n columns $\mathbf{h}_i$ is denoted by $\mathbf{H} = (\mathbf{h}_1, \mathbf{h}_2, \dots, \mathbf{h}_n)$. We use script fonts to denote sets, e.g., $\mathscr{X}$. Unless otherwise specified, vectors are assumed to be in the n-dimensional Euclidean space $(\mathbb{R}^n, \|\cdot\|)$ where $\|\cdot\|$ denotes the Euclidean norm of vectors. Notation $\mathbf{x}=(a^p, b^q, \dots, c^r)$ where $p+q+\cdots+r=n$ is used as shorthand for $\mathbf{x} = (\overbrace{a, \dots, a}^{p \text{ times}}, \overbrace{b, \dots, b}^{q \text{ times}}, \dots, \overbrace{c, \dots, c}^{r \text{ times}})$. For a random vector $\mathbf{x}$, we use $\mathbb{E}_{\mathbf{x}}[\cdot]$ to denote the expectation taken with respect to $\mathbf{x}$ and $f_{\mathbf{x}}(\cdot)$ to denote its probability density function (PDF). The Gaussian distribution with mean μ and square deviation σ^2 is denoted by $\mathscr{N}(\mu, \sigma^2)$.

2. Preliminaries on lattices and DPC

2.1. Lattices and lattice codebooks

Lattices are extensively studied in [23]. This section only provides a brief review, for reasons of completeness. Algebraically, an n-dimensional real lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$ defined as $\Lambda=\{\mathbf{\Omega}(\Lambda)\cdot\mathbf{u} : \mathbf{u} \in \mathbb{Z}^n\}$, where $\mathbf{\Omega}(\Lambda)$ is an $n\times n$ full-rank generator matrix. Geometrically, a lattice Λ is an infinite regular array that covers n-space uniformly. For example (a) the simplest n-dimensional lattice is the cubic lattice $\mathbb{Z}^n$ which consists of all n-dimensional vectors with integer coordinates, (b) the lattice family A_n, $n \in \mathbb{N}$, is defined as $A_n = \{(x_0, x_1, \dots, x_n) \in \mathbb{Z}^{n+1} : x_0+\cdots+x_n=0\}$ and (c) the lattice family D_n is defined as $D_n = \{(x_1, \dots, x_n) \in \mathbb{Z}^n : x_1+\cdots+x_n = \text{even}\}$. The fundamental Voronoi region $\mathscr{V}(\Lambda)$ of lattice Λ is the set of points $\mathbf{x} \in \mathbb{R}^n$ that are closer to $\mathbf{0}$ than to any other lattice point $\boldsymbol{\lambda} \in \Lambda$, i.e.,

$$\mathscr{V}(\Lambda) \triangleq \{\mathbf{x} : \|\mathbf{x}\| \leqslant \|\mathbf{x}-\boldsymbol{\lambda}\|, \forall \boldsymbol{\lambda} \in \Lambda\}.$$

For example, the Voronoi region of $\mathbb{Z}^n$ consists of all n-dimensional vectors that lie within a cubic region of unit volume, centered at the origin. The fundamental volume of Λ is the volume of its Voronoi region, i.e.,

$$V(\Lambda) \triangleq \int_{\mathscr{V}(\Lambda)} d\mathbf{x} = \sqrt{\det(\mathbf{\Omega}^T(\Lambda)\mathbf{\Omega}(\Lambda))}.$$

The second moment of $\mathscr{V}(\Lambda)$, or simply of Λ, is defined as

$$\sigma^2(\Lambda) \triangleq \frac{1}{nV(\Lambda)} \int_{\mathscr{V}(\Lambda)} \|\mathbf{x}\|^2 \, d\mathbf{x}$$

Author's personal copy

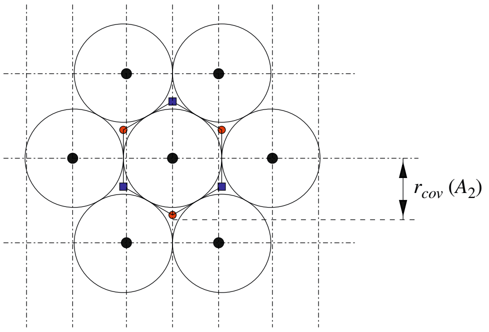

Fig. 1. Hexagonal lattice A_2 in the plane; its elements are the centers of the circles of radius $\rho(A_2)$. It has six deep holes, located at distance $r_{\rm cov}(A_2)$ from it and indicated with filled (small) squares and circles in the vertices of $\mathscr{V}(A_2)$.

and its normalized second moment is the dimensionless quantity $G(\Lambda)\triangleq V(\Lambda)^{-2/n}\sigma^2(\Lambda)$ which measures the covering efficiency of Λ. The shaping gain provided by lattice Λ is $\gamma_s(\Lambda)=1/(12G(\Lambda))$. For example, the cubic lattice $\mathbb{Z}^n$ has the largest normalized second moment, $G(\mathbb{Z}^n)=\frac{1}{12}$, and the smallest shaping gain, $\gamma_s(\mathbb{Z}^n)=0\,\mathrm{dB}$. The covering radius $r_{\rm cov}(\Lambda)$ is the radius of the smallest n-dimensional ball centered at the origin and containing $\mathscr{V}(\Lambda)$. The packing radius $\rho(\Lambda)$ is the radius of the biggest n-dimensional ball centered at the origin and contained in $\mathscr{V}(\Lambda)$. The points of $\mathbb{R}^n$ located at the vertices of $\mathscr{V}(\Lambda)$ are called "lattice deep holes". As one example, the hexagonal lattice A_2 generated with $\mathbf{\Omega}(A_2)=(-1,1,0;0,-1,1)$ [23] is shown in Fig. 1. The figure also shows the Voronoi region $\mathscr{V}(A_2)$ and the deep holes of this lattice.

Let Λ be an n-dimensional lattice. Also, let $\mathbf{a}\in\mathbb{R}^n$ be a given vector. The translated $\Lambda_{\mathbf{c}}=\mathbf{a}+\Lambda$ is also an n-dimensional lattice, and is called a *coset* of lattice Λ. The vector $\mathbf{a}$ is the *coset leader* of lattice $\Lambda_{\mathbf{c}}$. A lattice codebook $\mathscr{C}(\Lambda,\mathscr{R})$ is a finite subset of lattice Λ, and may be specified as the intersection of this lattice with an n-dimensional *support region* $\mathscr{R}$ that has non-zero volume,

$$\mathscr{C}(\Lambda,\mathscr{R})=\Lambda\cap\mathscr{R}.$$

That is, the lattice codebook $\mathscr{C}(\Lambda,\mathscr{R})$ consists of the set of points of lattice Λ that lie in $\mathscr{R}$.

$$|\mathscr{C}(\Lambda_{\mathbf{c}},\mathscr{R})|\cong V(\mathscr{R})/V(\Lambda_{\mathbf{c}}),$$

and the associated coding rate R is well approximated by

$$R\cong\frac{1}{n}\log_2[V(\mathscr{R})/V(\Lambda_{\mathbf{c}})]\text{ bits per dimension.}$$

2.2. Review of some applications

2.2.1. Information embedding as dirty paper coding

Fig. 2 depicts a block diagram of the problem of DPC. A message m, taken from some set $\mathscr{M}=\{0,1,\ldots,M-1\}$ is to be transmitted through an Gaussian channel. In addition to the noise $\mathbf{v}$, the transmission is corrupted by an interference $\mathbf{s}$ which is assumed to be known non-causally to only the transmitter, not to the receiver. In this setup, it is assumed that the interference $\mathbf{s}$ and the noise $\mathbf{v}$ are both i.i.d. Gaussian, with variances Q and N, respectively, i.e., $s_i\sim\mathscr{N}(0,Q)$ and $v_i\sim\mathscr{N}(0,N)$. Moreover, transmission is subject to some power constraint P, i.e., the channel input $\mathbf{x}$ is such that $\mathbb{E}[\mathbf{x}^2]\leqslant nP$.

It is now well known that Costa's DPC offers a good framework for the study of the problem of information embedding [6,26]. In this model, the CSI or interference $\mathbf{s}$ represents the host signal, and the message m represents the information to be hidden in it. Earlier DPC-based implementations for IE set signal $\mathbf{x}$, the embedded or transmitted signal, to be an appropriate scaled version (with some scale parameter α) of the scalar-quantization error of cover signal $\mathbf{s}$. The most prominent two schemes are the now well-known scalar Costa scheme (SCS) [5] and quantization index modulation (QIM) [4].

2.2.2. Gaussian broadcast channel

Consider the single-input vector Gaussian broadcast channel described by the model

$$\mathbf{y}_i=h_i\mathbf{x}+\mathbf{z}_i,\quad i=1,2,\ldots,M, \tag{1}$$

where M designates for the number of users. The input signal $\mathbf{x}$ is assumed to be power constrained, $\mathbf{x}_i$ and $\mathbf{y}_i$ stand for the i.i.d. Gaussian noise (with variance N_i) and the received signal for the i-th user, $i=1,2,\ldots,M$. The $(M\times 1)$ column vector $H=(h_1,h_2,\ldots,h_M)^T$ designates the vector characterizing the channel coefficients and is assumed to be known at the transmitter. We also make the assumption that the entries of the vector H are ordered according to

$$|h_1|^2/N_1\geqslant|h_2|^2/N_2\geqslant\cdots\geqslant|h_M|^2/N_M. \tag{2}$$

In this case, the broadcast channel is degraded and coding for user i, $i=1,2,\ldots,M$, can be accomplished by simply applying a DPC using $\mathbf{s}_i=\sum_{j=i+1}^{M}h_i\mathbf{x}_j$ as Gaussian CSI non-causally known at the transmitter and $h_i\sum_{j=1}^{i-1}\mathbf{x}_j+\mathbf{z}_i$ as unknown Gaussian noise (further details can be found, e.g., in [10]).

2.3. Lattice coding for Costa's DPC

The performance of the aforementioned sample-by-sample transmission schemes QIM and SCS can be improved upon using structured low-complexity lattice-based codebooks [24]. More specifically, consider the transmission scheme depicted in Fig. 3 where Λ is an n-dimensional lattice. Assume that the encoder and the decoder share some common randomness (e.g., in the form of a key $\mathbf{k}$ which is known to both the transmitter and the receiver). Through this paper, we assume that the key $\mathbf{k}$ is uniformly distributed over $\mathscr{V}(\Lambda)$.

Author's personal copy

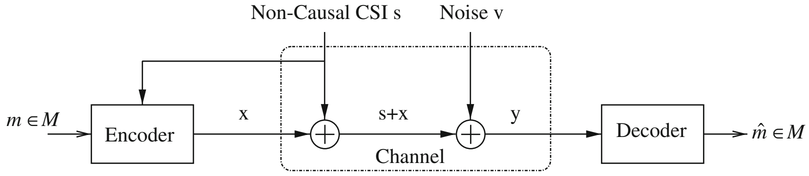

Fig. 2. Block diagram of the problem of DPC.

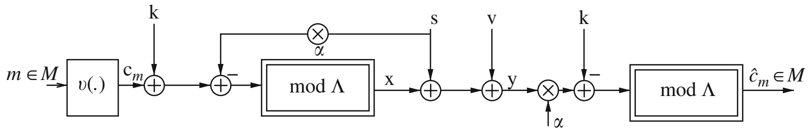

Fig. 3. Encoding/decoding for DPC based on lattice modulo-reduction.

Also, let $\imath(\cdot)$ be an indexing function which one-to-one associates each element from the set $\mathscr{M} = \{0, 1, \ldots, M-1\}$ with a vector $\mathbf{c}_m$ which is taken from some set of vectors $\mathscr{C} = \{\mathbf{c}_m : m \in \mathscr{M}\}$ that will be specified in the sequel. We assume that the vectors $\{\mathbf{c}_m\}$ lie in the fundamental region $\mathscr{V}(\Lambda)$ of lattice Λ. For each $m \in \mathscr{M}$, the vector $\imath(m) = \mathbf{c}_m$ is the *coset leader* of the coset $\Lambda_m = \mathbf{c}_m + \Lambda$ of the lattice Λ. The intersection of the lattice formed by the union of the cosets with $\mathscr{V}(\Lambda)$ gives $\mathscr{C}$, i.e.,

$$\left(\bigcup_m \Lambda_m\right) \cap \mathscr{V}(\Lambda) = \mathscr{C}. \tag{3}$$

Thus, taking $\mathscr{V}(\Lambda)$ as a support region, $\mathscr{C}$ may be viewed as a lattice codebook in the sense given in Section 2.1. This codebook is assumed to be known by both the encoder and the decoder. The key $\mathbf{k}$ may be used for security issues and also for the purpose of rate maximization [22].

In the following, we consider input signal vectors (frames) of length equal to the dimension n of lattice Λ. Also, we use the modulo-reduction operation $\bmod \Lambda$ with respect to the fundamental Voronoi region $\mathscr{V}$ of the lattice Λ, defined as $\mathbf{t} \bmod \Lambda \triangleq \mathbf{t} - \mathscr{Q}_\Lambda(\mathbf{t}) \in \mathscr{V}(\Lambda)$. The n-dimensional quantization operator $\mathscr{Q}_\Lambda(\cdot)$ is such that quantization of $\mathbf{t} \in \mathbb{R}^n$ results in the closest lattice point $\boldsymbol{\lambda} \in \Lambda$ to $\mathbf{t}$. The received signal is given by the sum of the input signal $\mathbf{x}$, the known interference $\mathbf{s}$ and the unknown noise $\mathbf{v}$, i.e.,

$$\mathbf{y} = \mathbf{x} + \mathbf{s} + \mathbf{v}. \tag{4}$$

Encoding and decoding are performed according to

$$\mathbf{x}(\mathbf{s}; m, \Lambda) = (\mathbf{c}_m + \mathbf{k} - \alpha\mathbf{s}) \bmod \Lambda, \tag{5a}$$

$$\hat{m} = \operatorname*{argmin}_{m \in \mathscr{M}} \min_{\boldsymbol{\lambda} \in \Lambda_m} \|\alpha\mathbf{y} - \mathbf{k} - \boldsymbol{\lambda}\|, \tag{5b}$$

where the scale (also called *inflation*) parameter α can be optimized according to different criteria and input is subject to power constraint $\mathbb{E}[\mathbf{x}^2] \leqslant nP$. We note that the choice $\alpha = 1$ corresponds to no scaling and is often referred to as zero-forcing DPC (ZF-DPC). Other optimization criteria for parameter α can be minimum mean-squared error (MMSE-DPC) and minimum error entropy (MEE-DPC) [24]. Also, the sample-by-sample schemes SCS and QIM mentioned previously correspond to lattice Λ being cubic, i.e., $\Lambda = \mathbb{Z}^n$.

3. Analysis of the transmission rate

Theoretical performance analysis of lattice-based codes for DPC has been provided in [10,22,27,28]. In this section, we investigate the transmission rate allowed by some finite-dimensional lattices, mostly from a numerical point-of-view, based on Monte-Carlo integration. The aim is to show how much (or little) lattice coding can improve transmission rate (w.r.t. scalar-quantization-based schemes QIM and SCS).

Consider the channel depicted in Fig. 3 and concentrate first on the case when $\alpha = 1$ (ZF-approach). In this case, the decoder computes $(\mathbf{y} - \mathbf{k} - \mathbf{c}_m) \bmod \Lambda$ for each $m \in \mathscr{M}$, with

$$\begin{aligned}(\mathbf{y} - \mathbf{k} - \mathbf{c}_m) \bmod \Lambda \\ &= ((\mathbf{c}_m + \mathbf{k} - \mathbf{s}) \bmod \Lambda + \mathbf{s} + \mathbf{v} - \mathbf{k} - \mathbf{c}_m) \bmod \Lambda \\ &= \mathbf{v} \bmod \Lambda.\end{aligned} \tag{6}$$

Thus, the modulo decoder sees the signal $\mathbf{y} - \mathbf{k} = \mathscr{Q}_\Lambda(\mathbf{y} - \mathbf{c}_m - \mathbf{k}) + \mathbf{c}_m + \tilde{\mathbf{v}}$, with the effective noise $\tilde{\mathbf{v}} = \mathbf{v} \bmod \Lambda$ being the quantization error of the initial AWGN $\mathbf{v}$ with respect to lattice Λ. Since $\mathscr{Q}_\Lambda(\mathbf{y} - \mathbf{c}_m - \mathbf{k}) \in \Lambda$, the input–output relation for the considered channel is that of a modulo lattice additive noise (MLAN) channel with input $\mathbf{c}_m$ and channel noise $\mathbf{v}$. The MLAN channel has been first considered in [29] and then in [22]. It has been shown that, in the case of infinite alphabet size and if the channel noise $\mathbf{v}$ is independent of input $\mathbf{c}_m$, the transmission rate is maximized if $\mathbf{c}_m$ is uniformly distributed over $\mathscr{V}(\Lambda)$. In this case, the channel capacity (in bits per dimension) is given by

$$R(\Lambda) = \frac{1}{n}(\log_2(V(\Lambda)) - H(\tilde{\mathbf{v}})) \leqslant \frac{1}{2}\log_2\left(1 + \frac{P}{N}\right), \tag{7}$$

Author's personal copy

Table 1. Some lattices (as defined in Section 2.1) with their important parameters.

Lattice	Name	n	Normalized second moment $G(\Lambda)$	Shaping gain $\gamma_s(\Lambda)$ (dB)	$\gamma_s(\Lambda)$ (in bit per dim.)
$\mathbb{Z}$	Integer	1	$\frac{1}{12}$	0.00	0.000
A_2	Hexagonal	2	$\frac{5}{36\sqrt{3}}$	0.17	0.028
D_4	Checkerboard	4	0.0766	0.37	0.061
E_7	E_7	7	0.0732	0.56	0.093
E_8	Gosset	8	0.0717	0.65	0.108

where $H(\cdot)$ denotes differential entropy. The right-hand side (RHS) of (7) is the capacity of an additive white Gaussian noise (AWGN) channel with $\mathrm{SNR}=10\log_{10}(P/N)\,\mathrm{dB}$. The effective noise $\tilde{\mathbf{v}}$ has probability density function given by a modularized or aliased Gaussian PDF over $\mathscr{V}(\Lambda)$. This modularized PDF can be approximated by the restriction of a Gaussian PDF over $\mathscr{V}(\Lambda)$,

$$f_{\tilde{\mathbf{v}}}(\tilde{\mathbf{v}}) \approx \begin{cases} \dfrac{1}{(2\pi N)^{n/2}} \displaystyle\sum_{\lambda\in\Lambda} \exp\left(-\dfrac{\|\tilde{\mathbf{v}}-\boldsymbol{\lambda}\|^2}{2N}\right) & \text{if } \tilde{\mathbf{v}} \in \mathscr{V}(\Lambda), \\ 0 & \text{if } \tilde{\mathbf{v}} \notin \mathscr{V}(\Lambda). \end{cases} \tag{8}$$

In general, no closed form expression for (7) can be derived and numerical integration is needed in order to evaluate the differential entropy $H(\tilde{\mathbf{v}})$.

When $\alpha \neq 1$, the receiver computes

$$\begin{aligned}\mathbf{y}' &= (\alpha\mathbf{y} - \mathbf{k}) \bmod \Lambda \\ &= (\mathbf{c}_m + \alpha\mathbf{v} - (1-\alpha)\mathbf{x}) \bmod \Lambda,\end{aligned} \tag{9}$$

where the Λ-aliased noise $\tilde{\mathbf{v}} = (\alpha\mathbf{v} - (1-\alpha)\mathbf{x}) \bmod \Lambda$ generalizes that corresponding to the ZF-approach and is statistically independent of the input $\mathbf{c}_m$ (see the *Inflated Lattice Lemma* reported in [22]). Note that this independence is satisfied even if the high resolution quantization assumption $Q \gg P$ is violated, since the key $\mathbf{k}$ is uniformly distributed over $\mathscr{V}(\Lambda)$ and, so, dithering by means of the key $\mathbf{k}$ makes $\mathbf{x}$ uniform over $\mathscr{V}(\Lambda)$ independently on the power of CSI $\mathbf{s}$. Hence, transmission over the channel in Fig. 3 is equivalent to that over an MLAN channel (modulo Λ) with input $\mathbf{c}_m$ and effective noise $\tilde{\mathbf{v}}$. However, due to the inflation parameter α, the noise $\tilde{\mathbf{v}}$ is no longer a modularized Gaussian noise over $\mathscr{V}(\Lambda)$, but the result of the convolution of a uniform self noise $(1-\alpha)\mathbf{x}$ and the ambient Gaussian noise $\alpha\mathbf{v}$. Consequently, (7) is slightly modified and the maximum transmission rate is given by the supremum of (7) over all values of parameter $\alpha \in (0, 1]$. This maximized rate is attained with a uniform input and is given by (in bits per dimension)

$$R(\Lambda) = \max_{\alpha} \frac{1}{n}(\log_2(V(\Lambda)) - H(\tilde{\mathbf{v}})). \tag{10}$$

Again, there is no closed form expression for (10) and, for finite dimension n, both computation of the differential entropy $H(\tilde{\mathbf{v}})$ and maximization over parameter α have to be done numerically. An approximation can be obtained by replacing the effective noise $\tilde{\mathbf{v}}$ by the restriction to $\mathscr{V}(\Lambda)$ of a Gaussian noise with same first and second moments. More specifically, let $\bar{\mathbf{v}}$ be the restriction to $\mathscr{V}(\Lambda)$ of the noise distributed as[1] $\mathscr{N}(0, \sigma^2)$, where $\sigma^2 = \alpha^2 N + (1-\alpha)^2 P$ and $P = G(\Lambda)V(\Lambda)^{2/n}$. The Λ-aliased Gaussian noise $\bar{\mathbf{v}}$ has density given by (8) where the variance N is replaced by σ^2. In this case, maximization in (10) (where $\tilde{\mathbf{v}}$ is replaced by $\bar{\mathbf{v}}$) reduces to minimization of the entropy$H(\bar{\mathbf{v}})$ of the Λ-aliased noise $\bar{\mathbf{v}}$. We note that computation of the entropy $H(\bar{\mathbf{v}})$ is not straightforward since it requires computation of the contribution of all points of the Gaussian distribution that are inside $\mathscr{V}(\Lambda)$ to $H(\bar{\mathbf{v}})$. From a numerical point-of-view, one difficulty here is that of generating a sufficiently long random sequence (in the n-dimensional space) which is uniformly distributed over $\mathscr{V}(\Lambda)$. We numerically compute $R(\Lambda)$ for the finite-dimensional lattices summarized below in Table 1. For each of these lattices, we proceed as follows for the generation of uniformly distributed (over $\mathscr{V}(\Lambda)$) random sequences, for the calculation of $H(\bar{\mathbf{v}})$.

(1) First, we generate n random variables uniformly distributed over [0, 1). We use independent realizations of these random variables to generate random vectors, as follows. Each realization of the n random variables gives an n-dimensional vector, say $\mathbf{u}_i$. For each vector $\mathbf{u}_i$, we use a generator matrix $\boldsymbol{\Omega}(\Lambda)$ of lattice Λ to generate the random vector $\tilde{\mathbf{u}}_i = \boldsymbol{\Omega}(\Lambda) \cdot \mathbf{u}_i$.

(2) Second, we use a lattice quantizer $\mathscr{Q}(\Lambda)$ (see the standard VQ algorithms provided in [23, Chapter 20.2]) to find the nearest lattice point to each generated vector $\tilde{\mathbf{u}}_i$. The quantization error of $\tilde{\mathbf{u}}_i$ is in the Voronoi region $\mathscr{V}(\Lambda)$ and is uniformly distributed over it.

The resulting rate curves (in bits per dimension) are plotted in Fig. 4. We defer analysis of these results until we discuss the accuracy of the above approximation (i.e., the rate-loss incurred by replacing the Λ-aliased noise $\tilde{\mathbf{v}}$ by the Λ-aliased Gaussian noise $\bar{\mathbf{v}}$). The non-Gaussiannity of $\tilde{\mathbf{v}}$ can

[1] Note that, here, for the Λ-aliased noise $\bar{\mathbf{v}}$, we neglected the effect of the *modulo loss* (due to the modulo front end at the receiver) only in the calculation of its variance σ^2, not in the computation of its PDF.

Author's personal copy

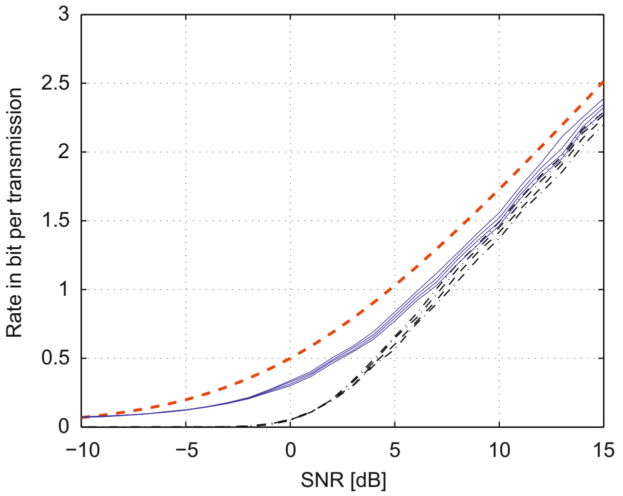

Fig. 4. Achievable rates allowed by MMSE-DPC and ZF-DPC, for various lattices over SNR $= 10\log_{10}(P/N)$. Bottom to top: $\mathbb{Z}$, A_2, D_4 and E_8 lattices. Solid: rates obtained with MMSE-DPC. Dashed-dotted: rates obtained with ZF-DPC. Dashed: AWGN capacity.

be measured as follows. Let mmse$(\tilde{\mathbf{v}}|\sqrt{\gamma}\tilde{\mathbf{v}}+\mathbf{n}_G)$ denote the minimum mean-square error in estimating $\tilde{\mathbf{v}}$ when observed through an i.i.d. Gaussian channel with unit-variance noise, $n_{G,i} \sim \mathcal{N}(0,1)$, and signal-to-noise ratio $\gamma\sigma^2$. Also, let $\tilde{\eta} = \sqrt{\gamma}\tilde{\mathbf{v}} + \mathbf{n}_G$ and $\bar{\eta} = \sqrt{\gamma}\bar{\mathbf{v}} + \mathbf{n}_G$. The differential entropy of $\tilde{\mathbf{v}}$ can be expressed as [30]

$$H(\tilde{\mathbf{v}}) = H(\bar{\mathbf{v}}) - \frac{1}{2}\int_0^{+\infty} \mathrm{mmse}(\bar{\mathbf{v}}|\bar{\eta}) - \mathrm{mmse}(\tilde{\mathbf{v}}|\tilde{\eta})\,d\gamma. \quad (11)$$

When the per-dimension SNR $= 10\log_{10}(P/N)$ is sufficiently large, the variance σ^2 becomes small and the effect of the modulo front end on the Λ-aliased Gaussian noise $\bar{\mathbf{v}}$ becomes negligible, since the points of the distribution $f_{\bar{\mathbf{v}}}(\bar{v})$ that significantly contribute to $H(\bar{\mathbf{v}})$ are then all contained in $\mathcal{V}(\Lambda)$. Hence, (11) gives

$$\begin{aligned} H(\tilde{\mathbf{v}}) &= H(\bar{\mathbf{v}}) - \frac{1}{2}\int_0^{+\infty} \frac{\sigma^2}{1+\gamma\sigma^2} - \mathrm{mmse}(\tilde{\mathbf{v}}|\tilde{\eta})\,d\gamma && (12a)\\ &= H(\bar{\mathbf{v}}) - \int_0^{+\infty} \frac{d}{d\gamma} D(\tilde{\eta}\|\bar{\eta})\,d\gamma && (12b)\\ &= H(\bar{\mathbf{v}}) - \lim_{\gamma\to+\infty} D(\tilde{\eta}\|\bar{\eta}) && (12c)\\ &= H(\bar{\mathbf{v}}) - D(\tilde{\mathbf{v}}\|\bar{\mathbf{v}}), && (12d)\end{aligned}$$

where (12a) follows since mmse$(\bar{\mathbf{v}}|\bar{\eta}) = \sigma^2/(1+\gamma\sigma^2)$, (12b) follows since [31] mmse$(\bar{\mathbf{v}}|\bar{\eta})$ − mmse$(\tilde{\mathbf{v}}|\tilde{\eta}) = 2(d/d\gamma)D(\tilde{\eta}\|\bar{\eta})$, where $D(\tilde{\eta}\|\bar{\eta})$ is the divergence of the density $f_{\tilde{\eta}}(\tilde{\eta})$ with respect to the Gaussian density $f_{\bar{\eta}}(\bar{\eta})$ with identical first and second moments, and (12d) follows since $D(\tilde{\eta}\|\bar{\eta})|_{\gamma=0} = 0$ and $\lim_{\gamma\to+\infty} D(\tilde{\eta}\|\bar{\eta}) = D(\tilde{\mathbf{v}}\|\bar{\mathbf{v}})$ [30, Lemma 7]. So, the transmission rate (10) can be rewritten as

$$\begin{aligned} R(\Lambda) &= \max_{\alpha} \frac{1}{n}(\log(V(\Lambda)) - H(\bar{\mathbf{v}}) + D(\tilde{\mathbf{v}}\|\bar{\mathbf{v}})) && (13a)\\ &\geqslant \max_{\alpha} \frac{1}{n}(\log(V(\Lambda)) - H(\bar{\mathbf{v}})). && (13b)\end{aligned}$$

From (13a), we see that rate expression includes two terms: the first term – the lower bound in (13b), is the transmission rate if the Λ-aliased noise $\tilde{\mathbf{v}}$ were Gaussian, and the other one – the term $D(\tilde{\mathbf{v}}\|\bar{\mathbf{v}})/n$, which measures how much additional rate (per dimension) is made possible by having $\tilde{\mathbf{v}}$ actually being non-Gaussian. We note that the divergence $D(\tilde{\mathbf{v}}\|\bar{\mathbf{v}})$ depends on lattice Λ (through the modulo output $\mathbf{x}$ and, thereby, the effective noise $\tilde{\mathbf{v}}$) and its computation may be not straightforward since it requires the computation of the restriction to $\mathcal{V}(\Lambda)$ of the convolution of the densities $f_{\alpha\mathbf{v}}(\cdot)$ and $f_{(1-\alpha)\mathbf{x}}(\cdot)$. Also, we mention that at large SNR $= 10\log_{10}(G(\Lambda)V(\Lambda)^{2/n}/N)$, the value of α that maximizes (10) is approximately equal to unity and, thus, the noise $\tilde{\mathbf{v}}$ is approximately equal to $\bar{\mathbf{v}}$. That is, the divergence $D(\tilde{\mathbf{v}}\|\bar{\mathbf{v}})$vanishes at large SNR.

3.1. Simulations and discussion

The results shown in Fig. 4 are obtained by maximizing numerically the RHS of (13b) over α, for each per-dimension SNR value, for some of the lattices in Table 1. It should be noted that the numerical computation of the differential entropy term $H(\bar{\mathbf{v}})$ is not straightforward. Here, we use Monte-Carlo integration. The details of the computation are omitted for brevity.

From the curves in Fig. 4, we observe that:

(1) The integer lattice $\mathbb{Z}$ provides the lowest rate. The gap to AWGN capacity is particularly large at low SNR. At low rates (below 0.1 bit/dim (bit/dimension)), a gap of about 4 dB is observed. At high SNR, this gap is already partially bridged up using lattices A_2, D_4 and E_8. The improvement brought by each of these lattices is due to the increase in the associated shaping gain $\gamma_s(\Lambda){=}1/12G(\Lambda)$ (w.r.t. $\gamma_s(\mathbb{Z}){=}0$ dB). For a given fixed rate R, such increase in $\gamma_s(\Lambda)$ translates to a reduction in the (per-dimension) average power $P = G(\Lambda)V(\Lambda)^{2/n}$ needed to transmit the set of indexes $m \in \mathcal{M}$ (i.e., to an SNR gain) by a factor $\gamma_s(\Lambda)$ (dB). Equivalently, for a given SNR, the rate R is increased by a factor $\frac{1}{2}\log_2(\gamma_s(\Lambda))$.

(2) The improvement due to shaping is particularly visible at high rates where the shaping gain $\gamma_s(\Lambda)$ becomes significant (this is consistent with the approximation $\gamma_s \approx (\pi e/6)(1-2^{-2R})$ in [32]). At low rates, however, the shaping gain is very small and the increase in rate is marginal. Note that this same behavior was also observed in [24].

Author's personal copy

4. Code design and probability of error

We now turn to evaluate the effect of lattice coding for DPC on the (per-dimension) bit error rate from a practical point-of-view. The improvement in BER due to lattice coding for DPC has been analyzed from a theoretical point-of-view in the case when the dimension of the used lattices is sufficiently high, most notably by Merhav [33] and Liu et al. [34]. In this section, probability of error obtained with lattice coding for DPC is investigated numerically, through Monte-Carlo simulations, for some finite-dimensional low-complexity lattices. Such analysis shows how much (or little) lattice codes are able of lowering BER when used for DPC in practice. Also, though carried out mostly through examples, analysis of BER in this section sheds light on the roles of shaping and coding and illustrates many practical considerations which are useful in the design of DPC-based systems.

4.1. Codebook selection

The design of an efficient lattice code $\mathscr{C}(\Lambda)$ for the channel shown in Fig. 3 depends on the target application, through the target transmission or embedding rate and the target reliability. Hence, conceiving a (good) lattice code for general DPC may be difficult in a general setting. Instead, we concentrate in this section on the design of efficient lattice codes $\mathscr{C}_m(\Lambda)$ for two different situations: (1) reliable transmission of only little information (e.g., for watermarking and information embedding type of applications where usually only few bits of information are needed) and (2) transmission of as much information as possible, for a given tolerated error. For the first situation, one is primarily concerned with reducing the probability of error; rate does not much matter. For the second situation, one is primarily concerned with rate as long as the probability of error is kept below a prescribed (relatively low) value.

For M different cosets $\{\Lambda_i\}$ of lattice Λ, one important parameter that highly influences BER is the minimum Euclidean distance between these cosets, i.e., the inter-cosets minimum-distance $d_{\min}$ given by

$$d_{\min} \triangleq \min_{0\leqslant i,j\leqslant M-1: i\neq j} \|\Lambda_i - \Lambda_j\| = \min_{(i,j):i\neq j} \min_{(\boldsymbol{\lambda_i},\boldsymbol{\lambda_j})\in\Lambda_i\times\Lambda_j} \|\boldsymbol{\lambda_i} - \boldsymbol{\lambda_j}\|. \quad (14)$$

It is precisely the choice of codebook $\mathscr{C}(\Lambda)$ that fixes both the values of $d_{\min}$ and the allowed (per-dimension) rate $R = (1/n)\log_2 M$. In the following, we give different examples of codebook selection (i.e., different choices for coset leaders $\{\mathbf{c}_m\}$) based on the geometrical structure of lattice Λ.

4.1.1. Lattice relevant deep holes

Lattice deep holes have been introduced in Section 2.1. These are the points of $\mathbb{R}^n$ that are located furthest away from Λ, i.e., at distance r_{cov} from it (see Fig. 1). The inter-cosets minimum distance $d_{\min}$ satisfies $d_{\min} \leqslant r_{\text{cov}}$ as observed in [35]. Thus, in order to maximize $d_{\min}$, these deep holes can be ideally used as coset leaders. However, as two or more of these deep holes can generate the same coset, only a subset of them can be used without causing a decoding ambiguity at the receiver. More specifically, let $\mathscr{H}(\Lambda) = \{\mathbf{h}_1, \ldots, \mathbf{h}_{N_h}\}$ be the set of the deep holes of lattice Λ. To resolve any ties when a coset of Λ has more than one minimum Euclidean norm element, we choose the smallest subset $\mathscr{H}^*(\Lambda) = \{\mathbf{h}_1, \ldots, \mathbf{h}_{N_h^*}\}$ of $\mathscr{H}(\Lambda)$, with $N_h^* \leqslant N_h$, such that

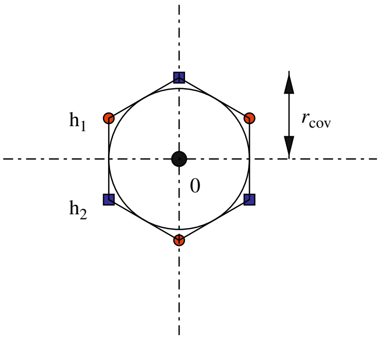

Fig. 5. Relevant deep holes of the lattice A_2 generated with $\boldsymbol{\Omega}(A_2) = (-1, 1, 0; 0, -1, 1)$. Among the holes shown in Fig. 1, only two are relevant, $\mathbf{h}_1$ and $\mathbf{h}_2$. This gives the ternary constellation $\{\mathbf{0}, \mathbf{h}_1, \mathbf{h}_2\}$.

$$\bigcup_{i\in\mathscr{H}^*(\Lambda)} \mathbf{h}_i + \Lambda = \bigcup_{i\in\mathscr{H}(\Lambda)} \mathbf{h}_i + \Lambda. \quad (15)$$

In the following, the deep holes of lattice Λ which satisfy (15) are called *relevant deep holes* of Λ. We see by inspection of (15) that a deep hole $\mathbf{h}_i$, $i \in \{1, \ldots, N_h\}$, is relevant if and only if

$$(\mathbf{h}_i - \mathbf{h}_j) \notin \Lambda \quad \text{for all } \mathbf{h}_j \in \mathscr{H}^*(\Lambda),\ j \neq i, \quad (16)$$

i.e., iff $\mathbf{h}_i$ does not belong to any of the cosets $\mathbf{h}_j + \Lambda$ where $\mathbf{h}_j \in \mathscr{H}^*(\Lambda)$ and $j \neq i$. The set $\mathscr{C} = \{\mathbf{0}, \mathbf{h}_1, \ldots, \mathbf{h}_{N_h^*}\}$ formed by the origin (the zero vector) and the relevant deep holes of lattice Λ forms a shaped constellation. Though non-optimal from a rate point-of-view (since it requires that $M \leqslant N_h^* + 1$, or equivalently that $R \leqslant (1/n)\log_2(N_h^* + 1)$), the use of this constellation is, however, optimal from a probability of error point-of-view, since it allows the largest inter-cosets Euclidean minimum distance (i.e., $d_{\min} = r_{\text{cov}}$). As a toy example, applying (16) for the hexagonal lattice A_2, we get $N_h^* = 2$. A possible choice for the resulting ternary shaped constellation $\mathscr{C}(A_2) = \{\mathbf{0}\} \cup \mathscr{H}^*(A_2)$ is shown in Fig. 5.

4.1.2. Construction A

A low-complexity efficient method for increasing transmission rate R with respect to the use of *relevant lattice deep holes* is Construction A [23]. Construction A provides means of constructing a lattice $\Lambda = C(n, k) + 2\mathbb{Z}^n$ with

Author's personal copy

minimum distance

$$d_{\min}(\Lambda) = \min(2, \sqrt{d}), \tag{17}$$

from an appropriate linear channel code $C(n,k)$ with minimum Hamming distance d. As a toy example, note that using this technique, the lattices E_7 and E_8 – which are the densest lattices in dimensions 7 and 8, respectively, can be constructed as $E_7 = (7,3,4) + 2\mathbb{Z}^7$ and $E_8 = (8,4,4) + 2\mathbb{Z}^8$. The binary linear code $(7,3,4)$ is the dual of the Hamming code $(7,4,3)$ and $(8,4,4)$ is the first order Reed–Muller code of length 8. Construction A is primarily a means of lattice construction and has already been used in [28].

(1) First, choose N_a^* binary vectors $\mathbf{a}_1, \ldots, \mathbf{a}_{N_a^*}$ inside the Hamming ball $\mathscr{B}_H(\mathbf{0}, d/2)$ centered at the origin $\mathbf{0}$ and of radius $d/2$. These vectors must be as far apart as possible and must satisfy

$$dH(\mathbf{a}_i, \mathbf{c}) \leqslant d/2, \quad \forall (i, \mathbf{c}) \in \{1, \ldots, N_a^*\} \times C(n,k), \tag{18}$$

where dH denotes the Hamming distance.

(2) Second, one-to-one map these vectors to N_a^* appropriately chosen minimum Euclidean norm points $\mathbf{c}_1, \ldots, \mathbf{c}_{N_a^*}$ located inside $\mathscr{V}(\Lambda)$ by $\mathbf{c}_i = \mathbf{a}_i + 2\mathbf{z}$, $\mathbf{z} \in \mathbb{Z}^n$ and choose codebook $\mathscr{C}$ as $\mathscr{C} = \{\mathbf{0}, \mathbf{c}_1, \ldots, \mathbf{c}_{N_a^*}\}$.

The use of deep holes for code design is more appropriate for low rate applications, since the allowed transmission rate is constrained by $(1/n)\log_2(N_h^* + 1)$ as already mentioned previously. Construction A may allow transmission at larger rates, but at the expense of lower reliability since inter-cosets minimum distance $d_{\min}$ is upper bounded as in (17). It is then more appropriate for applications where the target rate is preferably as high as possible and some (small) decoding error is tolerated at the receiver.

Discussion: Before we describe the end-to-end system design using the proposed lattice codebooks, we pause to discuss two important implications that follow from the specific choice of the constellation as specified previously. We insist on these implications as they reflect the specific structure of the employed codes and, also, explain the careful (and somewhat tedious) nature of the design that will follow in Section 4.2.

Consequence 1: The shaped constellations described so far are *non-conventional* in the sense that, spatially, their elements are spread in a way that makes mapping (for inputs labeling) not straightforward. To see that, observe, for example, that the ternary-constellation $\mathscr{C}(A_2) = \{\mathbf{0}, \mathbf{h}_1(A_2), \mathbf{h}_2(A_2)\}$ shown in Fig. 5 and obtained with the relevant holes $\mathbf{h}_1(A_2) = (-\frac{2}{3}, \frac{1}{3}, \frac{1}{3})$ and $\mathbf{h}_2(A_2) = (-\frac{1}{3}, -\frac{1}{3}, \frac{2}{3})$ of hexagonal lattice A_2 forms an equilateral triangle, geometrically, since $\|\mathbf{h}_1(A_2) - \mathbf{0}\| = \|\mathbf{h}_2(A_2) - \mathbf{0}\| = \|\mathbf{h}_1(A_2) - \mathbf{h}_2(A_2)\| = r_{\mathrm{cov}}(A_2) = \sqrt{\frac{2}{3}}$. This specific spatial localization of the elements of the constellation preclude the use of standard input labeling techniques such as Gray labeling [36].

Consequence 2: For the problem of codebook selection addressed above, we shall see the ensemble of coset leaders as the elements of a shaped constellation. When such a constellation is uncoded, the allowed transmission rate is determined by its size, i.e., the number of its elements. Hence, one important consequence is that the investigation (for comparison reasons) of the effects of coding (brought by channel coding, CC) and shaping (brought by source coding, SC) allowed by the use of different constellations is not straightforward, since different constellations (with different sizes) correspond to different rates and different rates correspond to different importance for the SC and CC [28,37]. More specifically, at a given SNR value, SC and CC unequally contribute to the "total" gain (i.e., the observed BER reduction). Some illustrative examples are given in Section 4.2. This means that when two schemes with different constellations yield different error probabilities, it might not be clear to interpret the improvement brought by one scheme over the other as being due to source coding enhancement or, instead, to channel coding enhancement. Hence, in order to isolate (for comparison reasons) the individual effects of SC and CC on the (per-dimension) BER achieved with different schemes, one has to operate at the same bit rate (i.e., the same spectral efficiency, when bandwidth is normalized to 1 Hz).

In the following section, for the design of an end-to-end DPC-based system that operates at a given target rate, we rely on channel coding which introduces redundancy in the binary stream before mapping. This allows us to compare the shaping and coding capabilities of different systems that use different constellations and discuss their efficiency. For channel coding, i.e., rate matching, we use the standard parallel concatenated codes (PCCs [38]) listed in Table 3 and also simple repetition coding.

4.2. Bit error rate analysis

In this section, we illustrate the use of some of the finite-dimensional shaped constellations described in Section 4.1 by evaluating and comparing the resulting BERs against the per-dimension per-bit SNR $= 10\log_{10}(G(\Lambda)V(\Lambda)^{2/n}/RN)$, where R stands for the operating rate. We consider two rate regimes: low rate transmission using relevant deep holes and higher rate transmission using Construction A. Our aim is to investigate the effect of shaping and coding on BER from a practical point-of-view. Though non-general (since carried out mostly through examples), analysis in this section shows how much (or little) lattice-based constellations can improve upon scalar schemes in terms of both shaping and coding, in practice. However, for that, we need careful system design (including design of appropriate mapper/de-mapper functions, vector quantizer (VQ) and coding). Though somewhat tedious, this careful design reflects the specific structure of the employed codes for each of the considered constellations.

Author's personal copy

Table 2. Labeling for transmission using the constellations $\mathscr{C}'(A_2)$ and $\mathscr{C}(D_4)$.

Labeling for the constellation $\mathscr{C}'(A_2)$				Labeling for the constellation $\mathscr{C}(D_4)$	
$(\mathbf{0}, \mathbf{0})$	000	$(\mathbf{h}_1(A_2), \mathbf{h}_1(A_2))$	110	$\mathbf{0}$	00
$(\mathbf{0}, \mathbf{h}_1(A_2))$	001	$(\mathbf{h}_1(A_2), \mathbf{h}_2(A_2))$	111	$\mathbf{h}_1(D_4)$	11
$(\mathbf{0}, \mathbf{h}_2(A_2))$	101	$(\mathbf{h}_2(A_2), \mathbf{0})$	010	$\mathbf{h}_2(D_4)$	01
$(\mathbf{h}_1(A_2), \mathbf{0})$	100	$(\mathbf{h}_2(A_2), \mathbf{h}_2(A_2))$	011	$\mathbf{h}_3(D_4)$	10

4.2.1. Design of mapper/de-mapper functions

Consider the constellation $\mathscr{C}(\Lambda) = \{\mathbf{0}\} \cup \mathscr{H}^*(\Lambda)$ formed by the origin and relevant deep holes of lattice Λ. We shall use such constellation to design end-to-end DPC schemes in Section 4.2.2. Let $\Phi(\cdot)$ be a mapper function which one-to-one associates each input binary sequence of n bits with an element of this constellation; and $\Psi(\cdot)$ the inverse de-mapper function. Input labeling is not straightforward as we mentioned previously. Two examples are discussed below for some lattices taken from Table 1.

Hexagonal lattice A_2: We consider the hexagonal lattice A_2 that we considered previously, in the example shown in Fig. 1. It has dimension $n = 2$, normalized second moment $G(A_2)=5/36\sqrt{3}$ and volume $V(A_2)=\sqrt{3}$ [23]. The uncoded but shaped constellation obtained with its relevant deep holes $\mathscr{C}(A_2)=\{\mathbf{0}, \mathbf{h}_1(A_2), \mathbf{h}_1(A_2)\}$ is shown in Fig. 5. For mapping, we group the input binary flow into binary sequences of 3 bits each (and not 2 bits, see footnote 2 for explanation). Then, to form the cosets, we map each 3-bit binary sequence onto an appropriately chosen pair of symbols from $\mathscr{C}(A_2)$.[2] We denote by $\mathscr{C}'(A_2)$ the "two symbols-by-two symbols" set

$$\begin{aligned}\mathscr{C}'(A_2) = \{&(\mathbf{0}, \mathbf{0}), (\mathbf{0}, \mathbf{h}_1(A_2)), (\mathbf{0}, \mathbf{h}_2(A_2)), (\mathbf{h}_1(A_2), \mathbf{0}),\\ &(\mathbf{h}_1(A_2), \mathbf{h}_1(A_2)), (\mathbf{h}_1(A_2), \mathbf{h}_2(A_2)),\\ &(\mathbf{h}_2(A_2), \mathbf{0}), (\mathbf{h}_2(A_2), \mathbf{h}_2(A_2))\}\end{aligned} \tag{19}$$

and loosely use the term "constellation" to refer to it (even though it is just a way of grouping the elements of constellation $\mathscr{C}(A_2)$). Then, mapping is performed by using the bits-to-symbols assignment shown in Table 2.

Checkerboard lattice D_4: The checkerboard lattice D_4 considered here is generated by the generator matrix $\mathbf{\Omega}(D_4)$ given by [23]

$$\mathbf{\Omega}(D_4) = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \tag{20}$$

It has dimension $n = 4$, second moment $G(D_4) = (\frac{1}{12} + 1/(2n(n+1)))/2^{(2/n)} = 0.0766$, volume $V(D_4) = \sqrt{\det(\Omega(D_4)^T\Omega(D_4))} = 2$, $N_h = 16$. Typical deep holes are $(\pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2}, \pm\frac{1}{2})$ and $(0, 0, 0, \pm 1)$ [23]. By applying (16), we obtain $|\mathscr{H}^*(D_4)| = 3$. A possible choice for the relevant deep holes of D_4 is: $\mathbf{h}_1(D_4) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$, $\mathbf{h}_2(D_4) = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$ and $\mathbf{h}_3(D_4) = (0, 0, 0, 1)$. Thus, we get the quaternary uncoded shaped constellation

$$\mathscr{C}(D_4) = \{\mathbf{0}, \mathbf{h}_1(D_4), \mathbf{h}_2(D_4), \mathbf{h}_3(D_4)\}, \tag{21}$$

which allows a transmission rate of $\log_2(4)/4 = 0.5\,\text{bit/dim}$. Mapping is obtained by using the bits-to-symbols assignment shown in Table 2 for constellation $\mathscr{C}(D_4)$.

4.2.2. End-to-end designed systems (based on lattices A_2 and D_4)

We now describe two end-to-end designed systems based on lattices A_2 and D_4 and compare their performance (in terms of shaping and coding capabilities) relative to the same baseline scalar scheme. We choose two values for the target operating (per-dimension) transmission rate: $R_1 = 0.5\,\text{bit/dim}$ and $R_2 = 0.25\,\text{bit/dim}$.

Hexagonal lattice A_2: The uncoded constellation given by (19) gives a rate of $(\log_2(|\mathscr{C}'(A_2)|)/2)/2 = 0.75\,\text{bit/dim}$ (note that the additional normalization per 2 is here to obtain the bit rate per channel use). For target rate $R_1 = 0.5\,\text{bit/dim}$, we use a parallel concatenated code of rate $R_{ch} = \frac{2}{3}$ and memory 2 before the shaping code (i.e., the two-dimensional vector quantizer based on lattice A_2). The constituent convolutional codes are taken in their recursive systematic form. Their generator polynomials, expressed in octal form, are $(\mathbf{g}_1^{(1)} = 007_8, \mathbf{g}_1^{(2)} = 001_8, \mathbf{g}_1^{(3)} = 004_8)$ and $(\mathbf{g}_2^{(1)} = 002_8, \mathbf{g}_2^{(2)} = 005_8, \mathbf{g}_2^{(3)} = 007_8)$. For target rate $R_2 = 0.25\,\text{bit/dim}$, we use a rate-$\frac{1}{3}$, memory $\nu = 2$ PCC, with generator polynomials $\mathbf{g}^{(1)} = 005_8$ and $\mathbf{g}^{(2)} = \mathbf{g}^{(3)} = 007_8$. The interleaver is generated pseudo-randomly and has size $L = 10\,000$. Coding parameters of the used PCCs together with their important parameters are summarized in Table 3 .

Next, we describe the end-to-end system design. The turbo-encoded L bits are grouped into sequences of 3-bits each, which are then mapped onto the corresponding (pairs of) symbols from $\mathscr{C}'(A_2)$ using the mapper shown in Table 2. We denote by P the (per-dimension) output power of the signal $\mathbf{x}$ to be transmitted in the channel. After adding the scaled interference $\alpha\mathbf{s}$ and a uniformly distributed dither

[2] Note that grouping the input bits by pairs and not by triplets (and hence directly using $\mathscr{C}(A_2)$ instead of $\mathscr{C}'(A_2)$) would cause mapping to be drastically poor. To see this, observe that in this case, one would have two different symbols (e.g., 01 and 11) constantly assigned to the same point from the constellation, thus causing larger error rates. One way to solve this problem is to group symbols by pairs as in (19). However, note that as sending one symbol from $\mathscr{C}'(A_2)$ amounts to send two symbols from $\mathscr{C}(A_2)$, rate is divided by 2 in the following.

Author's personal copy

Table 3. Coding parameters for coded constellations $\mathscr{C}(\mathbb{Z})$, $\mathscr{C}'(A_2)$ and $\mathscr{C}(D_4)$ for rates $R_1 = 0.5\,\text{bit/dim}$ and $R_2 = 0.25\,\text{bit/dim}$.

	Rate $R_1 = 0.5\,\text{bit/dim}$		Rate $R_2 = 0.25\,\text{bit/dim}$	
Integer lattice $\mathbb{Z}$	PCC	$R_{ch} = 1/2$, memory $\nu = 2$ $\mathbf{g}^{(1)} = 005_8$, $\mathbf{g}^{(2)} = 005_8$	PCC	$R_{ch} = 1/4$, memory $\nu = 2$ $\mathbf{g}^{(1)} = 005_8$, $\mathbf{g}^{(2)} = 007_8$ $\mathbf{g}^{(3)} = 007_8$, $\mathbf{g}^{(4)} = 007_8$
Hexagonal lattice A_2	PCC	$R_{ch} = 2/3$, memory $\nu = 2$ $\mathbf{g}_1^{(1)} = 007_8$, $\mathbf{g}_1^{(2)} = 001_8$, $\mathbf{g}_1^{(3)} = 004_8$ $\mathbf{g}_2^{(1)} = 002_8$, $\mathbf{g}_2^{(2)} = 005_8$, $\mathbf{g}_2^{(3)} = 007_8$	PCC	$R_{ch} = 1/3$, memory $\nu = 2$ $\mathbf{g}^{(1)} = 005_8$ $\mathbf{g}^{(2)} = \mathbf{g}^{(3)} = 007_8$
Checkerboard latticeD_4		Uncoded	PCC	$R_{ch} = 1/2$, memory $\nu = 2$ $\mathbf{g}^{(1)} = 005_8$, $\mathbf{g}^{(2)} = 007_8$ $R_{ch} = 1/2$, memory $\nu = 4$ $\mathbf{g}^{(1)} = 0023_8$, $\mathbf{g}^{(2)} = 0035_8$ $R_{ch} = 1/2$, memory $\nu = 8$ $\mathbf{g}^{(1)} = 0561_8$, $\mathbf{g}^{(2)} = 0753_8$

signal $\mathbf{k}$, the two-dimensional modulo encoder (VQ) first determines[3] the nearest point of the scaled lattice $\beta(A_2)A_2$ to the vector $(\mathbf{c} + \mathbf{k} - \alpha\mathbf{s})$ (i.e., $\mathscr{Q}_{\beta(A_2)A_2}(\mathbf{c} + \mathbf{k} - \alpha\mathbf{s})$) where $\beta(A_2) = \sqrt{P/G(A_2)V(A_2)^{2/n}}$, and then outputs the quantization error $\mathbf{x} = (\mathbf{c} + \mathbf{k} - \alpha\mathbf{s}) \bmod \beta(A_2)A_2$ which is transmitted over the channel.

In the channel, transmission is corrupted by both zero-mean white Gaussian noise with double-sided noise power spectral density $N = N_0/2$ and interference $\mathbf{s}$ (with per-dimension power Q). For the simulations, the inflation parameter α is set to $\alpha = P/(P + N)$ [1] and N_0 is chosen such that $N = P/(2R_i E_b/N_0)$, where $i = 1, 2$ and $R_1 = \frac{1}{2}(\log_2(|\mathscr{C}'(A_2)|)/2)\frac{2}{3} = 0.5\,\text{bit/dim}$ and $R_2 = \frac{1}{2}(\log_2(|\mathscr{C}'(A_2)|)/2)\frac{1}{3} = 0.25\,\text{bit/dim}$.

At the receiver, MMSE α-scaling is applied and the dither $\mathbf{k}$ is removed; the two-dimensional modulo decoder $\mathscr{Q}_{\beta(A_2)A_2}(\cdot)$ is applied and the transmitted symbol sequence is detected. Then, de-mapping is performed and the binary output is passed into a BCJR a posteriori probability decoder [39]. The BCJR uses the APP values and successively refines the estimates of the information bits (the curves in Figs. 6–8 are obtained after five iterations).

Checkerboard lattice D_4: The uncoded constellation $\mathscr{C}(D_4)$ given by (21) allows a rate of $\log_2(4)/4$=0.5 bit/dim. Thus, for our target operating rate $R_1 = 0.5\,\text{bit/dim}$, no additional CC of the information bits is required; we simply use the uncoded constellation $\mathscr{C}(D_4)$ as is. We group information bits by pairs and then map them to the corresponding cosets using the mapping in Table 2. For our target operating rate $R_2 = 0.25\,\text{bit/dim}$, however, we incorporate a rate $\frac{1}{2}$ memory-2 PCC with generator polynomials $\mathbf{g}^{(1)} = 005_8$ and $\mathbf{g}^{(2)} = 007_8$ before the shaping code (i.e., the four-dimensional VQ based on lattice D_4). The rest of the transmission scheme follows the same steps as for lattice A_2 (i.e., lattice scaling, interference and noise addition, dither removal, modulo-reduction, de-mapping and the BCJR module).

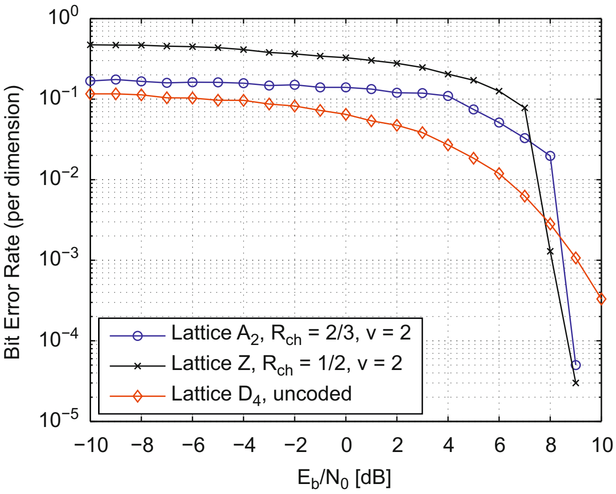

Fig. 6. BER vs. the per-bit SNR $= 10\log_{10}(E_b/N_0)$. Operating rate $R_1 = 0.5\,\text{bit/dim}$.

4.2.3. Simulation results and discussion

We consider the use of the constellation $\mathscr{C}(\mathbb{Z})$ for DPC as a baseline relative to which the above two end-to-end designed systems are compared. With the integer lattice $\mathbb{Z}$, the target operating rate $R_1 = 0.5\,\text{bit/dim}$ is obtained using PCC of rate $R_{ch} = \frac{1}{2}$; and the target operating rate $R_2 = 0.25\,\text{bit/dim}$ is obtained using either PCC of rate $R_{ch} = \frac{1}{4}$

[3] We use the standard low-complexity VQ algorithms provided in [23, Chapter 20.2].

Author's personal copy

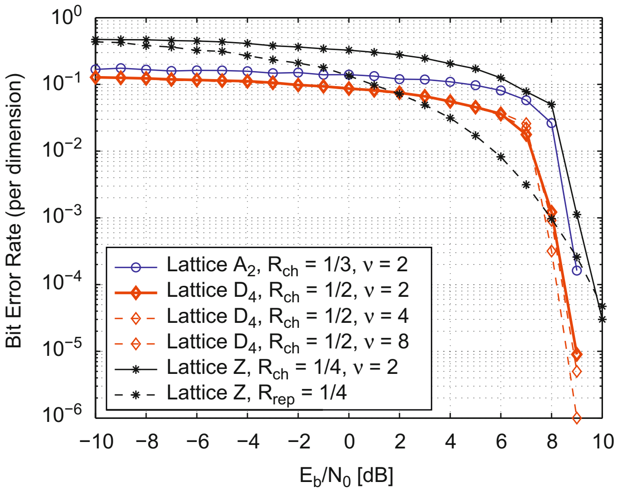

Fig. 7. BER vs. the per-bit SNR $= 10\log_{10}(E_b/N_0)$. Operating rate $R_2 = 0.25\,\text{bit/dim}$.

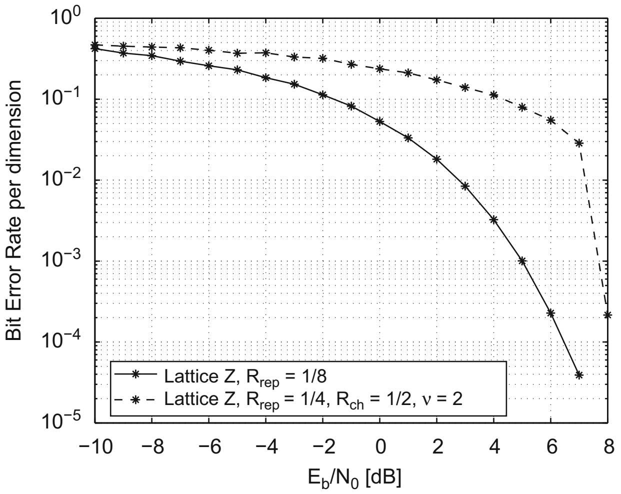

Fig. 8. BER vs. the per-bit SNR $= 10\log_{10}(E_b/N_0)$. Operating rate $R_3 = 0.125\,\text{bit/dim}$.

or simple repetition coding with repetition factor $1/R_{rep} = 4$ (details of memory length and generator polynomials for PCCs are given in Table 3). Results are shown in Figs. 6–8. We observe that:

1. At small SNR, the use of the (here coded) shaped constellation $\mathscr{C}'(A_2)$ results in some BER reduction (w.r.t. that of the binary constellation $\mathscr{C}(\mathbb{Z})$). Further improvement is obtained by use of the quaternary shaped constellation $\mathscr{C}(D_4)$ even when the latter is uncoded (see Fig. 6 for the target rate $R_1 = 0.5\,\text{bit/dim}$). For instance, that uncoded constellation $\mathscr{C}(D_4)$ improves upon coded constellations illustrates the fact that coding has only negligible effect on BER when the SNR is small. Moreover, note that the used lattices have second moments such that $G(D_4) = 13/120\sqrt{2} < G(A_2) = 5/36\sqrt{3} < G(\mathbb{Z}^n) = \frac{1}{12}$. Improvement in BER due to lattice coding for DPC at small SNR is mainly determined by how small is the second moment of the used lattice – i.e., by how large is its shaping capability; and reflects lattice efficiency as a VQ (recall that $\gamma_s(\Lambda) = 1/12G(\Lambda)$). Furthermore, we see from Fig. 7 that the latter observation is also valid for target rate $R_2 = 0.25\,\text{bit/dim}$, which illustrates that it is the effect of shaping that most matters at low SNR independently of the operating rate. This observation is consistent with prior theoretical work in [10,37].
2. At high SNR, however, the improvement brought by normalized second moment (i.e., the increase of (per-dimension) shaping gain from 0.000 dB (for $\mathbb{Z}$ to 0.028 for A_2, and to 0.061 for lattice D_4) does not counterbalance the loss in coding (incurred by using less powerful error correction channel codes). This explains why the BER curve corresponding to the integer lattice $\mathbb{Z}$ falls below those corresponding to lattices A_2 and D_4 in Fig. 6 for rate target $R_1 = 0.5\,\text{bit/dim}$. Thus, in this SNR range, it is the effect of coding that more influences BER in lattice coding for DPC (in particular, observe that the effect of memory for the rate-$\frac{1}{2}$ PCC in Fig. 7 is observed only above an SNR of about 8 dB).
3. At medium SNR (typically, 2–8 dB), the effect of shaping is still visible but is very small. On the other hand, simple repetition codes outperform powerful PCC (see Fig. 7) in this SNR range. This is also visible from Fig. 8 where repetition coding is compared to turbo coding for operating rate $R_3 = 0.125\,\text{bit/dim}$.

Remarks: We close this section by the following two remarks. Firstly, we note that the above observation as for the effect of shaping on BER should not be considered as being non-consistent with that in Section 4 relative to the increase in the transmission rate due to lattice coding which was observed especially at high SNR. Intuitively, this can be interpreted as follows. For fixed per-dimension power P, the effect of shaping can be viewed as an increase in lattice volume (in fact, in $V(\Lambda)^{2/n}$). Then, for the same information to be transmitted (i.e., at fixed rate), enlarging lattice Voronoi cell is beneficial especially when channel noise is strong (and hence can cause signal to fall outside the Voronoi cell if this cell were small). Alternatively, when noise is weak (and hence even a small Voronoi cell suffices to keep inside the input signal which has power P per-dimension), enlarging this cell may be better exploited by sending more signals, each with per-dimension power P, and each occupying a portion of this cell.

Secondly, we note that even though simulations and discussions above were carried out assuming the same bit rate (per-dimension), this was adopted for reasons of comparison of the effects of shaping and coding only; and one can definitely compare BERs provided by different schemes at different rates – just as one can compare BERs provided by

Author's personal copy

different constellations with different sizes at given per-bit SNR in classical communication (see for example comparison of M-ary constellations in terms of BER in [36, p. 311]). Of course, it is not possible to discriminate the individual effects of shaping and coding on BER in this latter case. But, this may turn out to be useful in practice, as it will be explained in Section 5.

5. Practical usefulness – interaction shaping/coding

In this section, we briefly discuss the usefulness of the approach and results presented so far in practice, for real implementations of DPC, and, also, to illustrate the interaction between shaping and coding at finite-dimensional lattice-coding for DPC.

5.1. Practical usefulness

From an application-oriented point-of-view, the following two questions are (among others) of special interest in the design of real lattice-based DPC implementations.

(1) Given a minimum target per-dimension rate R and a target operating per-dimension SNR (i.e., a power-distortion couple (P, N)), select a lattice Λ of dimensionality n and a lattice code $\mathscr{C}(\Lambda)$ such that error probability is as small as possible.

(2) Given a target operating per-dimension SNR and a maximum tolerated probability of error at this SNR, select a lattice Λ of dimensionality n and a lattice code $\mathscr{C}(\Lambda)$ such that the allowed transmission rate is as large as possible.

Insights to solve the first problem can be obtained through comparison of the BER obtained by the use of different constellations which all allow the same target per-dimension rate (rate matching can be utilized to ensure the same operating rate, as described in Section 4). For example, we see from the numerical results in Section 4.2.3 that at small SNR lattices with large shaping gain (i.e., high dimension) are more appropriate (codebook may then be built using relevant deep holes). At medium SNR, repetition coding is efficient. At high SNR, appropriate solutions are generally rate-dependent but, from the previous examples, it appears that, more than the choice of the lattice itself, it is the efficiency of the channel code used for error correction that most determines system performance (see Figs. 6–8).

Insights to solve the second problem can be obtained through comparison of the BERs obtained by the use of different constellations which, possibly, allow different rates. To illustrate this approach, Fig. 9 displays BER curves relative to different rates obtained with the use of different constellations. The two solid curves correspond to rates $\frac{1}{7}$ bit/ dim and $\frac{1}{8}$ bit/ dim obtained with the use of relevant deep holes-based uncoded constellations $\mathscr{C}(E_7) = \{\mathbf{0}, (\frac{1}{4}^6, -\frac{3}{4}^2)\}$ and $\mathscr{C}(E_8) = \{\mathbf{0}, (-\frac{1}{8}, \frac{1}{8}^6, \frac{7}{8})\}$, respectively. For the simplicity of the VQ process, the two lattices E_7 and E_8 are constructed as $E_7 = A_7 \cup ((-\frac{1}{2}^4, \frac{1}{2}^4) + A_7)$. The two dashed curves correspond to rates which are two times larger, $\frac{2}{7}$ bit/ dim and $\frac{1}{4}$ bit/ dim, and correspond to the use of Construction A to build lattices E_7 and E_8 as in the example in Section 4.1.2. The displayed numerical results suggest that Construction A may be a better choice (w.r.t. deep holes) for code design for DPC when the target rate is relatively important.

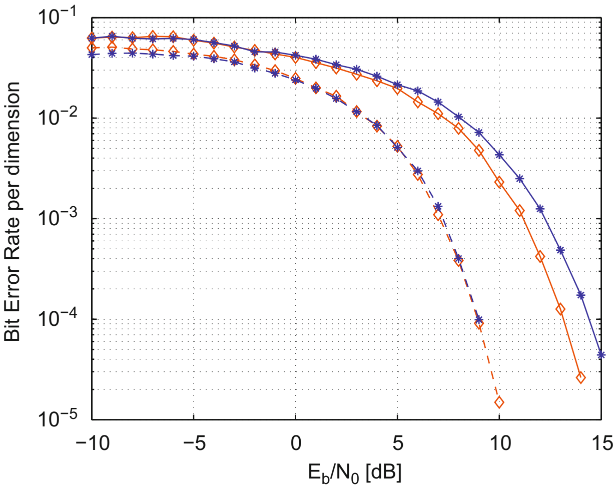

Fig. 9. BER against the per-dimension per-bit SNR $= 10\log_{10}(E_b/N_0)$ for uncoded-constellations for MMSE-DPC. The curves correspond to lattices E_7 (asterisk) and E_8 (diamond). The codebook $\mathscr{C}$ is obtained using relevant lattice deep holes (solid) and Construction A (dashed).

5.2. Interaction shaping–coding

First of all, we note that when used in conjunction with good (standard) error correction codes, lattices may provide efficient implementations for DPC, by putting together the afforded shaping efficiency and the coding efficiency provided by the employed channel code. From a theoretical point-of-view, it is even possible to take advantage from full shaping gain at small SNR along with full coding gain at high SNR (e.g., by means of nested codes as in [10]). From a practical point-of-view, however, one major difficulty in the design of such schemes is due to the interaction between shaping and coding at finite-dimensional lattice coding, by opposition to the infinite-dimensional case for which shaping and coding are decoupled [10].

At finite-dimensional lattice coding, interaction between shaping and coding can be illustrated as follows. Since the shaping gain provided by a lattice Λ depends only on its normalized second moment $G(\Lambda)$, the improvement in the per-

Author's personal copy

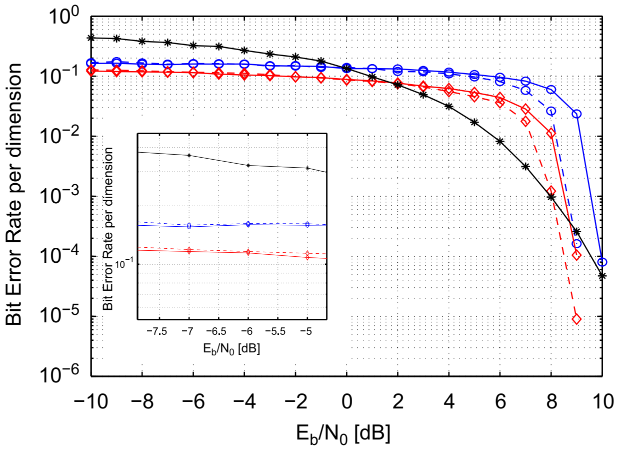

Fig. 10. Interaction shaping/coding. Scaling lattices so as to have the same volume causes coding loss at high SNR (by diminishing the inter-cosets minimum-distance $d_{\min}$). Meanwhile, only negligible improvement in shaping efficiency is observed at small SNR.

dimension per-bit $\text{SNR} = 10\log_{10} G(\Lambda)V(\Lambda)^{2/n}/RN$) due to shaping can be brought out[4] by simply scaling the lattices so as to have the same volume (e.g., that, $V(\mathbb{Z})$, of the cubic lattice $\mathbb{Z}^n$). The solid curves shown in Fig. 10 are obtained by having lattices $\mathbb{Z}$ (asterisk), A_2 (circle) and D_4 (diamond) being scaled so as to have the same volume, $V(\mathbb{Z}) = 1$. BER is measured for a target rate of $R = 0.25\,\text{bit}/\,\text{dim}$. For comparison reasons, we also reproduced the curves (dashed) obtained previously in Section 4 with the same lattices being non-scaled, for the same target rate. We observe that scaling in order to make the most of shaping at small SNR not only provides only negligible improvement at small SNR (cf. zoom in Fig. 10), but, in addition, causes coding efficiency to diminish at high SNR. We note that, that the improvement due to shaping is negligible at small SNR is consistent with the fact that the theoretical ultimate gain due to shaping, which is obtained when the employed lattice has an infinite dimension, is only $\pi e/6$, i.e., 0.255 bit/dim. However, that the BER is larger (w.r.t. no scaling) at high SNR illustrates the interaction that does exist between shaping and coding. For instance, at high SNR, the increase in the shaping capability does not counterbalance the loss caused by the decrease (due to scaling) in the inter-cosets minimum distance $d_{\min}$ (which translates to a coding loss). More specifically, scaling a lattice Λ with scale factor θ in such a way that $V(\theta\Lambda)^{2/n} = V(\mathbb{Z}^n)^{2/n}$ causes the inter-coset minimum distance $d_{\min}$ todecrease to $\theta d_{\min}$ where

$$\theta = \frac{V(\mathbb{Z})}{V(\Lambda)^{1/n}}. \tag{22}$$

Informally speaking, this brings the different cosets closer to each other and, hence, increases error probability. When $n \longrightarrow +\infty$, θ tends to unity and the decrease in the minimum distance (and thereby in coding efficiency) goes to zero. This is consistent with the fact that, asymptotically in dimension n of the employed lattice, shaping and coding are decoupled.

[4] Note that a similar approach has been used in [40] in the context of multidimensional constellations for channels with no CSI.

6. Conclusion

In this paper, we investigated how low-complexity finite-dimensional lattices can be tuned in practice for the problem of dirty paper coding. We evaluated numerically the performance allowed by some lattice-based carefully designed end-to-end systems. Rate calculation and bit error rate computation are carried out based on Monte-Carlo integration and simulation techniques. Though mostly qualitative, analysis in this paper illustrates how much (or little) finite-dimensional lattice coding can improve upon scalar schemes. Meanwhile, the problem of codebook selection is investigated through some illustrative examples using the appealing algebraic structure of the lattice. Numerical simulations for end-to-end designed systems allowed us to investigate the effects of shaping and coding (across the per-dimension per-bit signal-to-noise ratio). Finally, we illustrated the interaction between shaping and coding at finite-dimensional lattice coding for DPC and discussed the usefulness of the provided results from a practical point-of-view, in real DPC implementations.

Acknowledgments

This work was supported in part by the EU framework program ECRYPT, the French National RNRT framework program SDMO. The work of A. Zaidi was also supported in part by the Walloon Region DGTRE Nanotic-COSMOS program, in part by the EU framework program COOPCOM, and in part by the FP7 network of Excellence Newcom++.

References

[1] Costa MHM. Writing on dirty paper. IEEE Trans Inf Theory 1983;29:439–41.

[2] Tomlinson M. New automatic equalizer employing modulo arithmetic. IEEE Electron Lett 1971;7:138–9.

[3] Harashima H, Miyakawa H. Matched-transmission technique for channels with intersymbol interference. IEEE Trans Commun 1972;COM-20:774–80.

[4] Chen B, Wornell G. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans Inf Theory 2001;47:1423–43.

[5] Eggers JJ, Bäuml R, Tzschoppe R, Girod B. Scalar Costa scheme for information embedding. IEEE Trans Signal Process 2003:1003–19.

Author's personal copy

[6] Moulin P, O'Sullivan JA. Information-theoretic analysis of information hiding. IEEE Trans Inf Theory 2003;49:563–93.

[7] Zaidi A, Piantanida P, Duhamel P. Broadcast- and MAC-aware coding strategies for multiple user information embedding. IEEE Trans Signal Process 2007;55:2974–92.

[8] Zaidi A, Vandendorpe L. Coding schemes for relay-assisted information embedding. IEEE Trans Inf Secur Forensics 2009;4:70–85.

[9] Ginis G, Cioffi JM. Vectored DMT: a FEXT canceling modulation scheme for coordinating users. In: IEEE international conference on communications, Helsinki, Finland, 2001.

[10] Zamir R, Shamai (Shitz) S, Erez U. Nested linear/lattice codes for structured multi-terminal binning. IEEE Trans Inf Theory 2002;IT-48:1250–76.

[11] Caire G, Shamai (Shitz) S. On the throughput of a multi-antenna Gaussian broadcast channel. IEEE Trans Inf Theory 2003;IT-49:1691–706.

[12] Yu W, Cioffi J. Sum capacity of Gaussian vector broadcast channels. IEEE Trans Inf Theory 2004;50:1875–92.

[13] Viswanath S, Jindal N, Goldsmith A. Duality, achievable rates and sum rate capacity of Gaussian MIMO broadcast channel. IEEE Trans Inf Theory 2003;IT-49:2658–68.

[14] Viswanath P, Tse DN. Sum capacity of the vector Gaussian MIMO broadcast channel. IEEE Trans Inf Theory 2003;IT-49:1912–21.

[15] Cohen AS, Lapidoth A. The Gaussian watermarking game. IEEE Trans Inf Theory 2002;48:1639–67.

[16] Weingarten H, Steinberg Y, Shamai (Shitz) S. The capacity region of the Gaussian MIMO broadcast channel. In: Proceedings of the IEEE international symposium on information theory, Chicago, IL, June/July 2004. p. 174.

[17] Kim Y-H, Sutivong A, Sigurjonsson S. Multiple user writing on dirty paper. In: Proceedings of the IEEE international symposium on information theory, Chicago, USA, June 2004. p. 534.

[18] Zaidi A, Kotagiri S, Laneman JN, Vandendorpe L. Cooperative relaying with state available non-causally at the relay. IEEE Trans Inf Theory, December 2008, submitted for publication.

[19] Zaidi A, Vandendorpe L. Lower bounds on the capacity of the relay channel with states at the source. EURASIP J Wireless Commun Networking, 2009, accepted for publication.

[20] Gel'fand SI, Pinsker MS. Coding for channel with random parameters. Problems Control Inf Theory 1980;9:19–31.

[21] Willems FMJ. On Gaussian channels with side information at the transmitter. In: Proceedings of the nineth symposium on information theory, Benelux, The Netherlands, 1998.

[22] Erez U, Shamai (Shitz) S, Zamir R. Capacity and lattice strategies for cancelling known interference. IEEE Trans Inf Theory 2005;IT-51:3820–33.

[23] Conway JH, Sloane NJA. Sphere packing, lattices and groups. 3rd ed., New York: Wiley; 1988.

[24] Fischer RFH, The modulo-lattice channel: the key feature in precoding schemes. Int J Electron Commun 2005;October:244–53.

[25] Fischer RFH, Tzschoppe R, Bäeuml R. Lattice Costa schemes using subspace projection for digital watermarking. In: Proceedings of the ITG conference on source and channel coding (SCC), Erlangen, Germany, January 2004. p. 127–34.

[26] Cox I, Miller M, McKellips A. Watermarking as communication with side information. In: Proceedings of the international conference on multimedia computing and systems, July 1999. p. 1127–41.

[27] Erez U, Zamir R. Achieving $\frac{1}{2}\log_2(1+\mathrm{SNR})$ on the AWGN channel with lattice encoding and decoding. IEEE Trans Inf Theory 2004;IT-50:1–23.

[28] Erez U, ten Brink S. A close-to-capacity dirty paper coding scheme. IEEE Trans Inf Theory 2005;51:3417–32.

[29] Forney GD, Trott MD, Chung SY. Sphere-bound-achieving cosets codes and multilevel coset codes. IEEE Trans Inf Theory 2000;IT-46:820–50.

[30] Guo D, Shamai (Shitz) S, Verdù S. Mutual information and minimum mean-square error in Gaussian channels. IEEE Trans Inf Theory 2005;51:1261–82.

[31] Binia J. Divergence and minimum mean-square error in continuous-time additive white Gaussian noise channels. IEEE Trans Inf Theory 2006;52:1160–3.

[32] Kschischang FR, Pasupathy S. Optimal nonuniform signaling for Gaussian channels. IEEE Trans Inf Theory 1993;May:913–29.

[33] Merhav N. On random coding error exponents of watermarking systems. IEEE Trans Inf Theory 2000;46:420–30.

[34] Liu T, Moulin P, Koetter R. On error exponents of nested lattice codes for the AWGN channel. In: IEEE information theory workshop, San Antonio, Texas, October 2004. p. 348–52.

[35] Moulin P, Goteti AK, Koetter R. Optimal sparse-QIM codes for zero-rate blind watermarking. In: Proceedings of ICASSP, Canada, May 2004.

[36] Proakis JG. Digital communications. 4th ed., New York: McGraw-Hill; 2001.

[37] Xiong Z, Stanković V, Cheng S, Liveris AD, Sun Y. Source-channel coding for algebraic multiterminal binning. In: IEEE information theory workshop, ITW, USA, 2004.

[38] Berrou C, Glavieux A, Thitimajshima P. Near-Shannon limit error correcting coding and decoding: turbo-codes. In: Proceedings of the IEEE international conference on communications (ICC), Honolulu, Hawaii, May 1993. p. 1064–70.

[39] Bahl L, Cocke J, Jelink F, Raviv J. Optimal decoding of linear codes for minimizing symbol error rate. IEEE Trans Inf Theory 1974;IT-20:284–7.

[40] Forney GD, Wei LF. Multidimensional constellations – part I: introductions figures of merit, and generalized cross constellations. IEEE J Select Areas Commun 1989;7:877–92.

[41] Zaidi A, Piantanida P, Duhamel P. Scalar scheme for multiple user information embedding. In: Proceedings of the IEEE international conference on acoustics, speech and signal processing, ICASSP, Philadelphia, USA, March 2005. p. 5–8.

[42] Zaidi A, Piantanida P. MAC-aware coding strategy for multiple user information embedding. In: Proceedings of the IEEE international conference on acoustics, speech and signal processing, ICASSP, Toulouse, France, May 2006. p. 393–6.

[43] Zaidi A, Boyer R, Duhamel P. Audio watermarking under desynchronization and additive noise attacks. IEEE Trans Signal Process 2006;54:570–84.

Author's personal copy

Abdellatif Zaidi was born in Tunisia in 1978. He received the Eng. Degree in Electrical Engineering from the National School of Engineering in Advanced Technologies, ENSTA Paris-Tech, France, in 2002 and the M.Sc. degree and the Ph.D. degree both from the National School of Engineering in Telecommunications, TELECOM ParisTech, Paris, France, in 2002 and 2005, respectively. From December 2002 to December 2005, he was with the Communications an Electronics Department, TELECOM ParisTech, Paris, France, and the Signals and Systems Lab., CNRS/Supélec, France, pursuing his Ph.D. degree. He is now at École Polytechnique de Louvain, Université Catholique de Louvain, Belgium, working as a research assistant. Dr. Zaidi was "Research Visitor" at the University of Notre Dame, Indiana, USA, during fall 2007 and Spring 2008. His research interests cover a broad range of topics from signal processing for communication and multi-user information theory. Of particular interest are the problems of coding for side-informed channels, secure communication, coding and interference mitigation in multi-user channels, and relaying problems and cooperative communication with application to sensor networking and ad hoc wireless networks.

Pierre Duhamel (Fellow, IEEE, 1998) was born in France in 1953. He received the Eng. Degree in Electrical Engineering from the National Institute for Applied Sciences (INSA) Rennes, France, in 1975, the Dr. Eng. degree in 1978, and the Doctorat ès sciences degree in 1986, both from Orsay University, Orsay, France. From 1975 to 1980, he was with Thomson-CSF, Paris, France, where his research interests were in circuit theory and signal processing, including digital filtering and analog fault diagnosis. In 1980, he joined the National Research Center in Telecommunications (CNET), Issy les Moulineaux, France, where his research activities were first concerned with the design of recursive CCD filters. Later, he worked on fast algorithms for computing Fourier transforms and convolutions, and applied similar techniques to adaptive filtering, spectral analysis and wavelet transforms. From 1993 to September 2000, he has been professor at ENST, Paris (National School of Engineering in Telecommunications) with research activities focused on Signal processing for Communications. He was head of the Signal and Image processing Department from 1997 to 2000. He is now with CNRS/LSS (Laboratoire de Signaux et Systemes, Gif sur Yvette, France), where he is developing studies in Signal processing for communications (including equalization, iterative decoding, multicarrier systems, cooperation) and signal/image processing for multimedia applications, including source coding, joint source/channel coding, watermarking, and audio processing. He is currently investigating the application of recent information theory results to communication theory. Dr. Duhamel was chairman of the DSP committee from 1996 to 1998, and a member of the SP for Com committee until 2001. He was an associate Editor of the IEEE Transactions on Signal Processing from 1989 to 1991, an associate Editor for the IEEE Signal Processing Letters, and a guest editor for the special issue of the IEEE Transactions on SP on wavelets. He was distinguished lecturer, IEEE, for 1999, and was co-general chair of the 2001 International Workshop on Multimedia Signal Processing, Cannes, France. He was also co-technical chair of ICASSP 06, Toulouse, France. The paper on subspace-based methods for blind equalization, which he co-authored, received the "Best paper award" from the IEEE Transactions on SP in 1998. He was awarded the "grand prix France Telecom" by the French Science Academy in 2000. He is Fellow, EURASIP, since 2008.