The 38th Symposium on Information Theory
and its Applications (SITA2015)
Kojima, Okayama, Japan, Nov. 24–27, 2015

Generalized Voronoi Constellations

Brian M. Kurkoski *

Abstract— A lattice code construction that employs two separate lattices, a high dimension lattice for coding gain and a low-dimension lattice for shaping gain, is described. This generalizes past work on lattices codes based on self-similar Voronoi constellations.

Keywords— lattice codes

1 Introduction

Let Λ_c and Λ_s be two lattices in n-dimensional Euclidean space. If $\Lambda_\mathrm{s} \subseteq \Lambda_\mathrm{c}$, then the quotient group $\Lambda_\mathrm{c}/\Lambda_\mathrm{s}$ exists. The coset leaders of this group form a lattice code, which is useful for physical layer network coding. If Λ_c is good for coding and good for shaping, then the choice $\Lambda_\mathrm{s} = a\Lambda_\mathrm{c}$ with $a \in \mathbb{Z}$ gives a self-similar lattice code $\Lambda_\mathrm{c}/a\Lambda_\mathrm{c}$ which is useful for proving important theoretical results [1].

However, this choice is less suitable for practical implementations. It is assumed that Λ_c is a high-dimensional lattice such as a low-density lattice codes or LDPC Construction A. Such Polytrev capacity-approaching lattices Λ_c are designed to be efficiently decoded, using for example belief-propagation decoding. But performing shaping directly, that is direct construction of a self-similar lattice code is computationally difficult, and the exact shaping gain is not known. On the other hand, lattices with reasonable shaping gain and efficient shaping algorithms are known, such as E_8, Barnes-Wall and Leech lattices. In this paper, quotient groups $\Lambda_\mathrm{c}/\Lambda_\mathrm{s}$ where the lattices are not self-similar is considered.

2 Contribution

A simple necessary and sufficient conditions for $\Lambda_\mathrm{s} \subseteq \Lambda_\mathrm{c}$ is stated. Let Λ_c have n-by-n check matrix H_c (generator matrix is $G_\mathrm{c} = H_\mathrm{c}^{-1}$).

Lemma Let Λ_s have an all-integer generator matrix G_s. $\Lambda_\mathrm{s} \subseteq \Lambda_\mathrm{c}$ if and only if $H_\mathrm{c}G_\mathrm{s}$ is a matrix of integers.

This Lemma shows that it is straightforward to test if Λ_s is a sublattice of Λ_c. If this condition holds, then the quotient group $\Lambda_\mathrm{c}/\Lambda_\mathrm{s}$ exists and is a candidate for physical layer network coding.

Encoding refers to mapping information to the cosets of $\Lambda_\mathrm{c}/\Lambda_\mathrm{s}$. For self-similar lattices, $\Lambda_\mathrm{s} = a\Lambda_\mathrm{c}, a \in \mathbb{Z}$, Conway and Sloane gave a straightforward algorithm to perform encoding. When Λ_s and Λ_c are not self-similar, encoding is not obvious. Let $\mathcal{C}$ be a lattice code, given by suitably chosen coset leaders of $\Lambda_\mathrm{c}/\Lambda_\mathrm{s}$. The number of codewords $|\mathcal{C}|$ is $M = |\det \Lambda_\mathrm{s}|/|\det \Lambda_\mathrm{c}|$, the information is represented by integers $b_1, b_2, \ldots, b_n$ and the quantizer for Λ_s is Q_{Λ_s}.

Definition The lattice code $\mathcal{C}$ has a *rectangular encoding* if there exists G_c and $M_1, \ldots, M_n$ such that

$$G_\mathrm{c}\mathbf{b} - Q_{\Lambda_\mathrm{s}}(G_\mathrm{c}\mathbf{b}) \tag{1}$$

generates $\mathcal{C}$ exactly, for $b_i \in \{0, 1, \ldots, M_i - 1\}$. Clearly $M = \prod_{i=1}^n M_i$.

The definition is motivated by the desire for simple encoding schemes, that is, the range for each b_i depends only on M_i. For self-similar lattices $\Lambda_\mathrm{s} = a\Lambda_\mathrm{c}$, so $M_i = a$ and $|\mathcal{C}| = a^n$, and encoding is straightforward.

Proposition Let Λ_c have basis $G_\mathrm{c} = [\mathbf{g}_1, \ldots, \mathbf{g}_n]$ and let $M_1, \ldots, M_n$ be positive integers. If the following conditions are satisfied:

1. $M_i\mathbf{g}_i \in \Lambda_\mathrm{s}$ for $i = 1, 2, \ldots, n$ and
2. $\det(G_\mathrm{c}) \prod_{i=1}^n M_i = \det(\Lambda_\mathrm{s})$,

then these G_c and M_i can be used for a rectangular encoding.

Generally speaking, the given basis G_c for Λ_c (for example, the inverse of the sparse LDLC H matrix) may not satisfy this condition. It is desired to find a basis G'_c which does satisfy this condition. Replace one vector in column t with an unknown column vector $\mathbf{q}$. For example, if $t = n$ then the basis has the form:

$$G'_\mathrm{c} = \begin{bmatrix} \frac{\mathbf{g}_1}{m_1} & \frac{\mathbf{g}_2}{m_2} & \cdots & \frac{\mathbf{g}_{n-1}}{m_{n-1}} & \mathbf{q} \end{bmatrix}. \tag{2}$$

The basis transformation is:

$$G'_\mathrm{c} = G_\mathrm{c}W \tag{3}$$

where W is a unitary matrix with integer entries. The vector $\mathbf{q}$ is determined by finding W that satisfies those conditions. The n-by-n matrix W has $n \times (n-1)$ entries that are linearly dependent, and n entries $r_1, r_2, \ldots, r_n$ that are unknowns. The equation

$$\det W = 1 \tag{4}$$

results in a single linear diophantine equation in these unknowns. In numerical investigations thus far, this equation usually has many solutions. But finding the "best" solution remains an open problem.

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer-Verlag, 1999, ISBN 0-387-98585-9.

* Japan Advanced Institute of Science and Technology, Nomi, Ishikawa. kurkoski@jaist.ac.jp. This work was supported by JSPS Kakenhi Grant Number 26289119