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

However, this choice is less suitable for practical implementations. It is assumed that \( \Lambda_c \) is a high-dimensional lattice such as \( \Lambda_c = \text{LDPC Construction } \Lambda \). Such Polytrey capacity-approaching lattices \( \Lambda_c \) 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 \( \mathbb{E}_8 \), Barnes-Wall and Leech lattices. In this paper, quotient groups \( \Lambda_c/\Lambda_s \) where the lattices are not self-similar is considered.

2 Contribution

A simple necessary and sufficient conditions for \( \Lambda_s \subseteq \Lambda_c \) is stated. Let \( \Lambda_c \) have \( n \)-by-\( n \) check matrix \( H_c \) (generator matrix is \( G_c = H_c^{-1} \)).

Lemma Let \( \Lambda_s \) have an all-integer generator matrix \( G_s \). \( \Lambda_s \subseteq \Lambda_c \) if and only if \( H_c G_s \) is a matrix of integers.

This Lemma shows that it is straightforward to test if \( \Lambda_s \) is a sublattice of \( \Lambda_c \). If this condition holds, then the quotient group \( \Lambda_c/\Lambda_s \) exists and is a candidate for physical layer network coding.

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

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

\[
G_c b - Q_{\Lambda_c}(G_c b) = 0 \tag{1}
\]
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 \( \Lambda_s = a\Lambda_c \), so \( M_i = a \) and \( |\mathcal{C}| = a^n \), and encoding is straightforward.

Proposition Let \( \Lambda_c \) have basis \( G_c = [g_1, \ldots, g_n] \) and let \( M_1, \ldots, M_n \) be positive integers. If the following conditions are satisfied:

1. \( M_i g_i \in \Lambda_s \) for \( i = 1, 2, \ldots, n \)
2. \( \det(G_c) \prod_{i=1}^{n} M_i = \det(\Lambda_s) \),

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

Generally speaking, the given basis \( G_c \) for \( \Lambda_c \) (for example, the inverse of the sparse LDPC matrix \( H \) 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 \( q \). For example, if \( t = n \) then the basis has the form:

\[
G'_c = \left[ \begin{array}{c} g_1' \\ m_1 \\ g_2' \\ m_2 \\ \vdots \\ g_{n-1}' \\ m_{n-1} \\ q \end{array} \right] \tag{2}
\]
The basis transformation is:

\[
G'_c = G_c W \tag{3}
\]
where \( W \) is a unitary matrix with integer entries. The vector \( q \) 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