Multilevel constructions: coding, packing and geometric uniformity

Maiara F. Bollauf, Ram Zamir and Sueli I. R. Costa

Abstract

Lattice and special nonlattice multilevel constellations constructed from binary codes, such as Construction C, have relevant applications in mathematics (sphere packing) and communication problems (multi-stage decoding and efficient vector quantization). In this work, we explore some properties of Construction C, in particular its geometric uniformity. We then propose a new multilevel construction, motivated by bit interleaved coded modulation, that we call Construction $C^{\star}$. We explore the geometric uniformity and minimum distance properties of Construction $C^{\star}$, and discuss its potential superior packing efficiency with respect to Construction C.

Index Terms

Lattice constructions, Construction C, Construction $C^{\star}$, geometrically uniform constellation, minimum distance.

I. Introduction

Constructing lattices based on linear codes is an active topic of study which has been stimulated by the comprehensive approach in Conway and Sloane [6]. Construction C, or multi-level construction by a Code-Formula [9], [10], based on L binary codes $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L$ of length n, is an efficient constellation in $\mathbb{R}^n$ which is not always a lattice.

M. F. Bollauf is with the Institute of Mathematics, Statistics and Computer Science, University of Campinas as a Ph.D student (e-mail: maiarabollauf@ime.unicamp.br).

R. Zamir is with Department of Electrical Engineering-Systems in Tel Aviv University (e-mail: zamir@eng.tau.ac.il).

S. I. R. Costa with the Institute of Mathematics, Statistics and Computer Science, University of Campinas (e-mail: sueli@ime.unicamp.br).

Partial and preliminary results of this paper were presented at IEEE International Symposium on Information Theory, Barcelona, Spain, 2016 [3] and at International Zurich Seminar, Zurich, Switzerland, 2018 [4].

When we consider a single level ($L = 1$) with a linear code, Construction C reduces to the well known lattice Construction A [6]. For multilevel constructions, however, the resulting construction is not always a lattice, even if the component codes are linear. A recent work of Kositwattanarerk and Oggier [13] explored the relation between Construction C and the lattice Construction D. They showed that if we consider a family of nested linear binary codes $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$, where this chain is closed under Schur product, then both constructions coincide and we obtain a lattice. An example of a lattice construction originating from Construction C, uses as underlying codes a family of Reed-Muller codes and generates the Barnes-Wall lattice [9], [10].

Through multi-stage decoding, Construction C can achieve the high SNR uniform-input capacity of an AWGN channel asymptotically as the dimension n goes to infinity [12]. Moreover, if the underlying codes of this construction are linear, then all points in this constellation have the same minimum distance [6], but not necessarily the same kissing number (see Example 3).

Another application of nonlattice construction is presented by Agrell and Eriksson in [1], who proved that the "D_n+" tessellation [6] (which is a $2-$level Construction C) exhibits a lower normalized second moment (an then a better quantization efficiency) than any known lattice tessellation in dimensions 7 and 9.

Our first goal in this paper is to study the properties of a general Construction C, and to find out how close to a lattice can this construction be, in case it does not satisfy the condition required in [13]. We show that a two-level ($L = 2$) Construction C is geometrically uniform (a result that can be deduced from [11]), however for three levels or more ($L \geq 3$) the distance spectrum may vary between points of the constellation.

A recent coded modulation scheme, which is the *bit interleaved coded modulation* (BICM), motivates our second (and) main contribution of this paper: the proposal and study of a new construction which we call Construction $C^\star$.

The BICM, first introduced by Zehavi [19], requires mainly to have: a $nL-$dimensional binary code $\mathcal{C}$, an interleaver π and a one-to-one binary labeling map $\tilde{\mu} : \{0,1\}^L \to \mathcal{X}$, where $\mathcal{X}$ is a signal set $\mathcal{X} = \{0, 1, \ldots, 2^L - 1\}$ in order to construct a constellation Γ_{BICM} in $\mathcal{X}^n \subseteq \mathbb{R}^n$. The code and interleaveled bit sequence $c \in \mathcal{C}$ is partitioned into L subsequences c_i of length n :

$$c = (c_1, \ldots, c_L), \quad \text{with} \quad c_i = (c_{i1}, c_{i2}, \ldots, c_{in}). \tag{1}$$

The bits c_j are mapped at a time index j to a symbol x_j chosen from the 2^L-ary signal constellation $\mathcal{X}$ according to the binary labeling map $\tilde{\mu}$. Hence, for a $nL-$binary code $\mathcal{C}$ to encode all bits, then we have the scheme below:

$$\boxed{\text{codeword } (c)} \rightarrow \boxed{\text{interleaver } \pi} \rightarrow \boxed{\text{partitioning into L subsequences of length n}} \rightarrow \boxed{\text{mapping } \tilde{\mu}} \rightarrow \boxed{x_j = \tilde{\mu}(c_{1j}, \ldots, c_{Lj}),\ j = 1, \ldots, n}$$

In the general case, defining the natural labeling $\mu : \mathcal{C} \rightarrow \mathcal{X}^n$ as $\mu(c_1, c_2, , \ldots, c_L) = c_1 + 2c_2 + \cdots + 2^{L-1}c_L$ and assuming $\pi(\mathcal{C}) = \mathcal{C}$, it is possible to define an extended BICM constellation in a way very similar to the well known multilevel Construction C, that we call Construction $C^\star$.

The constellation produced via Construction $C^\star$ is always a subset of the associated constellation produced via Construction C for the same projection codes and it does not usually produce a lattice. We explore here this new construction presenting a necessary and sufficient condition that makes it a lattice, and also describe the Leech lattice Λ_{24} via Construction $C^\star$. Besides that, we study some properties of Construction $C^\star$, such as geometric uniformity and minimum distance, in order to analyze and compare packing efficiencies of Construction $C^\star$ and Construction C.

This paper is organized as follows: Section II is devoted to preliminary concepts and results; in Section III we point out known properties of Construction C and present a detailed discussion about its geometric uniformity; in Section IV we exhibit general geometrically uniform constellations and as consequence, an alternative proof to the geometric uniformity of a $L = 2$ Construction C; in Section V we introduce Construction $C^\star$, illustrate it with examples and also show how to describe the Leech lattice using this construction; in Section VI we investigate properties of Construction $C^\star$ such as geometric uniformity and latticeness; Section VII is devoted to the study of minimum distance in a constellation defined by Construction $C^\star$ and packing density relations between Constructions C and $C^\star$; Section VIII brings a comparison in terms of packing efficiency of Construction C and a hybrid Construction $C^\star/C$ and finally Section IX concludes the paper.

II. Fundamental concepts

This section is devoted to present some basic concepts, results and notations to be used in the next sections.

We will denote by $+$ the real addition and by $\oplus$ the sum in $\mathbb{F}_2$, i.e., $x \oplus y = (x + y) mod\ 2$.

A *linear binary code* $\mathcal{C}$ of length n and rank k (2^k codewords) is a linear subspace of dimension k over the vector space $\mathbb{F}_2^n$. It can also be written as the image of an injective linear transformation $\phi : \mathbb{F}_2^k \to \mathbb{F}_2^n$, $(a_1, \ldots, a_k) \mapsto G \cdot (a_1, \ldots, a_k)^T$, where $G \in \mathbb{F}_2^{n \times k}$ is a *generator matrix* of $\mathcal{C}$.

The *Hamming distance* between two elements $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ is the number of different symbol in two codewords,

$$d_H(x, y) \quad = \quad |\{i : x_i \neq y_i, 1 \leq i \leq n\}|. \tag{2}$$

The minimum distance of a code $\mathcal{C}$ is the minimum Hamming distance between all distinct codewords, i.e.,

$$d_H(\mathcal{C}) = d_{min}(\mathcal{C}) = \min\{d_H(x, y) : x, y \in \mathcal{C}, x \neq y\}. \tag{3}$$

A code of length n, containing M codewords and with minimum distance $d = d_{min}(\mathcal{C})$ is said to be an $(n, M, d)-$code. The *rate* of such a code is

$$R = \frac{1}{n} \log_2 M = \frac{k}{n} \log_2 2 = \frac{k}{n} \text{ bits/symbol.} \tag{4}$$

The *Hamming weight* $\omega(c)$ is the minimum number of nonzero elements in a codeword $c \in \mathcal{C}$.

A *lattice* $\Lambda \subset \mathbb{R}^N$ is a set of integer linear combinations of independent vectors $v_1, v_2, \ldots, v_n \in \mathbb{R}^N$, with $n \leq N$. In other words, a lattice is a discrete additive subgroup of $\mathbb{R}^n$. We consider here only full rank $(n = N)$ lattices.

For a lattice $\Lambda \subseteq \mathbb{R}^n$, the minimum distance is the smallest Euclidean distance between any two lattice points

$$d_E(\Lambda) = d_{min}(\Lambda) = \inf\{||x - y|| : x, y \in \Lambda, x \neq y\}. \tag{5}$$

The *Voronoi region* $\mathcal{V}(\lambda)$ of a lattice $\Lambda \subset \mathbb{R}^n$ is the subset of $\mathbb{R}^n$ containing all points nearer to lattice point λ than to any other lattice point. The closure of a Voronoi region tesselates $\mathbb{R}^n$ by translations given by lattice points.

The *packing radius* ρ of a lattice Λ is half of the minimum distance between lattice points and the *packing density* $\Delta(\Lambda)$ is the fraction of space that is covered by balls $\mathcal{B}(\lambda, \rho)$ of radius ρ in $\mathbb{R}^n$ centered at lattice points, i.e.,

$$\Delta(\Lambda) = \frac{vol \ B(0, \rho)}{vol(\Lambda)}, \tag{6}$$

where $vol(\Lambda) = |\det(G)| = vol(V(\lambda))$.

The *packing efficiency* is defined as $\chi(\Lambda) = (\Delta(\Lambda))^{1/n}$.

A constellation $\Gamma \in \mathbb{R}^n$ is said to be *geometrically uniform* if for any two codewords $c, c' \in \Gamma$ there exists a distance-preserving transformation T such that $c' = T(c)$ and $T(\Gamma) = \Gamma$.

Every lattice Λ is geometrically uniform, due to the fact that any translation $\Lambda + x$ by a lattice point $x \in \Lambda$ is just Λ and this implies that every point of the lattice has the same number of neighbors at each distance and all Voronoi regions are congruent.

From linear codes is possible to derive lattice constellations using the well known Construction A and D [6].

Definition 1. *(Construction A) Let $\mathcal{C}$ be an (n, k, d) linear binary code. We define Construction A from $\mathcal{C}$ as*

$$\Lambda_A = \mathcal{C} + 2\mathbb{Z}^n. \tag{7}$$

Definition 2. *(Construction D) Let $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$ be a family of nested linear binary codes. Let $k_i = \dim(\mathcal{C}_i)$ and let $b_1, b_2, \ldots, b_n$ be a basis of $\mathbb{F}_2^n$ such that $b_1, \ldots, b_{k_i}$ span $\mathcal{C}_i$. The lattice Λ_D consists of all vectors of the form*

$$\Lambda_D = \sum_{i=1}^{L} 2^{i-1} \sum_{j=1}^{k_i} \alpha_j^i b_j + 2^L z \tag{8}$$

where $\alpha_j^i \in \{0, 1\}$, $z \in \mathbb{Z}^n$.

Another well studied construction, that in general does not produce lattice constellation, even when the underlying codes are linear, is Construction C, defined below as in [9] (more details and applications also in [1]). Observe that in this definition the minimum distance conditions imposed in [6, pp. 150] are not being considered.

Definition 3. *(Construction C) Consider L binary codes $\mathcal{C}_1, \ldots, \mathcal{C}_L \subseteq \mathbb{F}_2^n$, not necessarily nested or linear. The infinite constellation Γ_C in $\mathbb{R}^n$, called Construction C is defined as:*

$$\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + \cdots + 2^{L-1}\mathcal{C}_L + 2^L\mathbb{Z}^n, \tag{9}$$

or equivalently

$$\Gamma_C \;\; := \;\; \{c_1 + 2c_2 + \cdots + 2^{L-1}c_L + 2^L z : c_i \in \mathcal{C}_i, i = 1, \ldots, L, \; z \in \mathbb{Z}^n\}. \tag{10}$$

Note that if $L = 1$, i.e., if we consider a single level with a linear code, then this construction reduces to lattice Construction A.

Example 1. *Consider $\mathcal{C}_1 = \{(0,0),(1,1)\}$ and $\mathcal{C}_2 = \{(0,0)\}$. The $2-$level Construction C from theses codes is given by $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathbb{Z}^2$. Geometrically, we can see this constellation in Figure 5 and clearly Γ_C is not a lattice.*

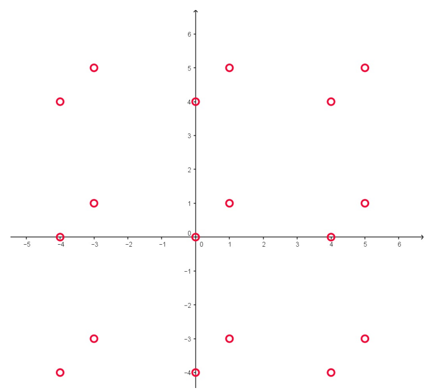

Fig. 1. 2- level Construction C from $\mathcal{C}_1 = \{(0,0),(1,1)\}$ and $\mathcal{C}_2 = \{(0,0)\}$.

Definition 4. *(Schur product) For $x = (x_1,\ldots,x_n)$ and $y = (y_1,\ldots,y_n) \in \mathbb{F}_2^n$, we define $x * y = (x_1y_1,\ldots,x_ny_n)$.*

See that, for $x, y \in \mathbb{F}_2^n$,

$$x + y = x \oplus y + 2(x * y). \tag{11}$$

Denote by Λ_C the smallest lattice that contains Γ_C. Kositwattanarerk and Oggier [13] give a condition that if satisfied guarantees that Construction C will provide a lattice which coincides with Construction D.

Theorem 1. *[13] (Lattice condition for Constructions C) Given a family of nested binary linear codes $\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$, then the following statements are equivalent:*

1. *Γ_C is a lattice.*
2. *$\mathcal{C}_1 \subseteq \cdots \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$ is closed under Schur product.*
3. *$\Gamma_C = \Lambda_D$,*

Example 2. *The D_n+ tessellation [6] could be conceived as a $2-$ level Construction C if we consider $\mathcal{C}_1$ as the $(n,2,n)-$ repetition code and $\mathcal{C}_2$ as the $(n,n-1,2)-$even parity check code. Note that for n even, this construction represents a lattice, because we would have nested linear codes that are closed under Schur product. Otherwise, when n is odd, we obtain a nonlattice* *constellation which coincides with our Construction C. In particular, for dimensions* $n = 7$ *and* 9 *it was proved that* D_n+ *has a lower normalized second moment than any known lattice tessellation [1].*

III. Properties of Construction C

There are some known properties of Construction C already explored in the literature, such as

A. Minimum distance

If the underlying codes of Construction C are linear, then the squared minimum distance can be expressed as

$$d^2_{min}(\Gamma_C) = \min\{d_H(\mathcal{C}_1), 2^2 d_H(\mathcal{C}_2), \ldots, 2^{2(L-1)} d_H(\mathcal{C}_L), 2^{2L}\}.$$

Indeed, observe that sets defined as $\Gamma_{\mathcal{C}_i} = 0 + 2 \cdot 0 + \cdots + 2^{i-1} c_i + \cdots + 2^{L-1} \cdot 0 + 2^L \cdot 0$, where $0 \in \mathbb{R}^n$, are subsets of Γ_C, i.e., $\Gamma_{\mathcal{C}_i} \subseteq \Gamma_C$ for all $i = 1, \ldots, L$, then it follows that $d^2_{E_{min}}(\Gamma_C) \leq \min\{d_H(\mathcal{C}_1), 2^2 d_H(\mathcal{C}_2), \ldots, 2^{2(L-1)} d_H(\mathcal{C}_L), 2^{2L}\}$.

From the other hand, according to the discussion in [6, pp. 150], if the first codeword in which two elements in Γ_C differ in the $i-$th component, i.e., consider $x, y \in \Gamma_C$, where

$$x = c_1 + 2c_2 + \cdots + 2^{i-1} c_i + \cdots + 2^{L-1} c_L + 2^L z \tag{12}$$

$$y = c_1 + 2c_2 + \cdots + 2^{i-1} \tilde{c}_i + \cdots + 2^{L-1} \tilde{c}_L + 2^L \tilde{z}, \tag{13}$$

where $\tilde{c}_j \neq c_j, j = i, \ldots L$. Thus, their squared distance vary by at least $2^{2(i-1)}$ in at least $d_H(\mathcal{C}_i)$ coordinates. Hence, $d^2_{E_{min}}(\Gamma_C) \geq \min\{2^{2(i-1)} d_H \mathcal{C}_i, 2^{2L}\}$ for all $i = 1, \ldots, L$ and $d^2_{E_{min}}(\Gamma_C) \geq \min\{d_H(\mathcal{C}_1), 2^2 d_H(\mathcal{C}_2), \ldots, 2^{2(L-1)} d_H(\mathcal{C}_L), 2^{2L}\}$. It justifies the formula in Equation (12).

From the formula for the squared minimum distance, it also follows that all points in this constellation have the same minimum distance to other constellations points.

B. Kissing number

The kissing number (number of nearest neighbors) of an element of Construction C may vary between the elements even when the underlying codes are linear, as it can be seen in our following Example 3, where the kissing number of an element varies between 1 and 2.

C. Geometric uniformity

The geometric uniformity of a two level ($L = 2$) Construction C can be deduced from the work of D. Forney [11] if we consider a $2-$level Construction C as group code with isometric labeling over $\mathbb{Z}/4\mathbb{Z}$ (i.e., a $2-$level binary coset code over $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}$). He proved that this type of construction produces a geometrically uniform generalized coset code. In Section IV, we provide an alternative proof, based on explicit isometric transformation (as a special case of a general class of geometric uniform constellations).

D. Equi-distance spectrum and geometric uniformity for $L \geq 3$

Geometric uniformity implies, in particular, that all points have the same set of Euclidean distances to their neighbors.

Definition 5. *(Distance spectrum) For a discrete constellation $\Gamma \subseteq \mathbb{R}^n$, the distance spectrum is*

$N(c, d) =$ *number of points in the constellation at a Euclidean distance d from an element c in the constellation.*

Definition 6. *(Equi-distance spectrum) A constellation Γ is said to have equi-distance spectrum (EDS) if $N(c, d)$ is the same for all $c \in \Gamma$.*

Geometric uniformity implies equi-distance spectrum for $L = 2$ levels in Construction C, i.e., $N(c, d) = N(0, d)$ for all $c \in \Gamma_C$.

However for $L \geq 3$ the equi-distance spectrum and hence the geometric uniformity property does not hold in general, as we will see in the next examples.

Example 3. *Consider the following linear codes, with $n = 1$ and $L = 3$:*

$$\mathcal{C}_1 = \{0, 1\}, \quad \mathcal{C}_2 = \{0, 1\}, \quad \mathcal{C}_3 = \{0\}.$$

Observe that some numbers obtained via Construction C, i.e., $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathcal{C}_3 + 8\mathbb{Z}^3$ are represented in Figure 2 and $N(2, 1) = 2 \neq 1 = N(0, 1)$. Therefore, this constellation does not have equi-distance spectrum and it cannot be geometrically uniform.

Example 4. *Consider an $(n = 2, L = 3)$ Construction C with the following three component linear codes:*

$$\mathcal{C}_1 = \mathcal{C}_2 = \{(0, 0), (1, 1)\}, \mathcal{C}_3 = \{(0, 0)\}. \tag{14}$$

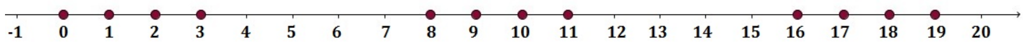

Fig. 2. Some elements of Construction C, with $\mathcal{C}_1 = \mathcal{C}_2 = \{0, 1\}$ and $\mathcal{C}_3 = \{0\}$.

We can write $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + 4\mathcal{C}_3 + 8\mathbb{Z}^3$ *(Figure 3) in this case as*

$$\Gamma_C = \{(8k_1 + j, 8k_2 + j) : k_1, k_2 \in \mathbb{Z}, j = 0, 1, 2, 3\}. \tag{15}$$

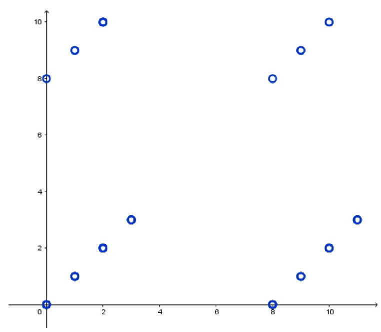

Fig. 3. Some elements of Construction C, with $\mathcal{C}_1 = \mathcal{C}_2 = \{(0, 0), (1, 1)\}$ and $\mathcal{C}_3 = \{(0, 0)\}$.

Note that $N((3, 3), \sqrt{2}) = 1 \neq 2 = N((1, 1), \sqrt{2})$, *so it is not geometrically uniform.*

IV. General geometrically uniform constellations

The next theorem presents a way to construct a geometrically uniform constellation, from which we can derive the particular case of geometric uniformity of Construction C for $L = 2$.

Theorem 2. *(Geometric uniformity of* $\Lambda + \mathcal{C}$*) If* Λ *is a lattice which has symmetry with respect to all coordinate axes and* $\mathcal{C} \subseteq \mathbb{F}_2^n$ *is a linear binary code, then* $\Gamma = \Lambda + \mathcal{C}$ *is geometrically uniform.*

Proof. Given $x = \lambda_1 + c_1 \in \Gamma$, where $\lambda_1 \in \Lambda$ and $c_1 \in \mathcal{C}$, consider the linear map $T_{c_1} : \mathbb{R}^n \to \mathbb{R}^n$, $T_{c_1}(z) = [T_{c_1}] \cdot z$ (z in the column format), where $[T_{c_1}]$ is defined as

$$[T_{c_1}] = \begin{pmatrix} (-1)^{c_{11}} & 0 & \dots & 0 \\ 0 & (-1)^{c_{12}} & \dots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & (-1)^{c_{1n}} \end{pmatrix}_{(n \times n)}, \tag{16}$$

$c_1 = (c_{11}, c_{12}, \dots, c_{1n})$. Observe that T_{c_1} is an isometry and ${T_{c_1}}^{-1} = T_{c_1}$.

The map $F_x : \mathbb{R}^n \to \mathbb{R}^n$, $F_x(y) = T_{c_1}(y - x)$ is an isometry and we show next that its restriction $F_x|_\Gamma : \Gamma \to \Gamma$ is also an isometry with $F_x(x) = 0$.

First, note that for $c_1, c_2 \in \mathcal{C}$ is valid that $T_{c_1}(c_2 - c_1) = c_1 \oplus c_2$. In fact,

$$(T_{c_1}(c_2 - c_1))_i = \begin{cases} 0, & \text{if } (c_{1i}, c_{2i}) = (0,0) \\ 1, & \text{if } (c_{1i}, c_{2i}) = (1,0) \\ 1, & \text{if } (c_{1i}, c_{2i}) = (0,1) \\ 0, & \text{if } (c_{1i}, c_{2i}) = (1,1) \end{cases} \tag{17}$$

which implies $T_{c_1}(c_2 - c_1) = c_1 \oplus c_2$.

Given $y \in \Gamma = \Lambda + \mathcal{C}$, $y = \lambda_2 + c_2$,

$$\begin{aligned} F_x(y) = T_{c_1}(y - x) &= T_{c_1}(\lambda_2 - \lambda_1 + c_2 - c_1) = T_{c_1}(\lambda_2 - \lambda_1) + T_{c_1}(c_2 - c_1) \\ &= \lambda_3 + (c_1 \oplus c_2) \in \Gamma = \Lambda + \mathcal{C}, \end{aligned} \tag{18}$$

since Λ is axes-symmetric. Therefore, $F_x(\Gamma) \subseteq \Gamma$.

As F_x is injective, it remains to prove that for any $w = \tilde{\lambda} + \tilde{c} \in \Gamma$ there exists $y \in \Gamma$ such that $w = F_x(y)$. By straightforward calculation we can see that

$$\begin{aligned} F_x(y) = \tilde{\lambda} + \tilde{c} &\Rightarrow T_{c_1}(y - (\lambda_1 + c_1)) = \tilde{\lambda} + \tilde{c} \Rightarrow T_{c_1}(T_{c_1}(y - (\lambda_1 + c_1))) = T_{c_1}(\tilde{\lambda} + \tilde{c}) \\ &\Rightarrow y = T_{c_1}(\tilde{\lambda}) + \lambda_1 + T_{c_1}(\tilde{c}) + c_1 = T_{c_1}(\tilde{\lambda}) + \lambda_1 + T_{c_1}(\tilde{c} + 0 - c_1) \\ &\Rightarrow y = T_{c_1}(\tilde{\lambda}) + \lambda_1 + T_{c_1}(\tilde{c} - c_1) = \underbrace{T_{c_1}(\tilde{\lambda}) + \lambda_1}_{\in \Lambda} + \underbrace{\tilde{c} \oplus c_1}_{\in \mathcal{C}} \in \Gamma. \end{aligned} \tag{19}$$

To conclude the proof, given any $x \in \Gamma$ and $w \in \Gamma$, we can consider the isometry

$$F : \Gamma \to \Gamma, \quad F = F_w \circ F_x, \tag{20}$$

for which we have $F(x) = F_w^{-1}(F_x(x)) = F_w^{-1}(0) = w$. $\square$

Corollary 1. *(Special geometrically uniform Construction C) If a $L-$level Construction C has just two nonzero linear codes C_i and C_L, $i \in \{1, \ldots, L-1\}$ then $\Gamma_C = 2^{i-1}\mathcal{C}_i + 2^{L-1}\mathcal{C}_L + 2^L\mathbb{Z}^n$ is geometrically uniform.*

Proof. We can write

$$\Gamma_C = 2^{i-1}(\mathcal{C}_i + 2^{L-i}(\mathcal{C}_L + 2\mathbb{Z}^n)). \tag{21}$$

Since the Construction A lattice $\mathcal{C}_L + 2\mathbb{Z}^n$ is axes-symmetric also its expansion by 2^{L-i} is. From Theorem 2, it follows that $\mathcal{C}_i + 2^{L-i}(\mathcal{C}_{L-1} + 2\mathbb{Z}^n)$, $i = 1, \ldots, L-1$ is geometrically uniform and this also holds for the scaled version. □

Remark 1. *The fact that a $2-$level Construction C is geometrically uniform (Subsection III-C) is a special case of the above Corollary 1 for $L = 2$ and $i = 1$.*

V. Construction $C^\star$: an inter-level coded version of Construction C

This section is devoted to the introduction of a new method of constructing constellations from binary codes: Construction $C^\star$.

Definition 7. *(Construction $C^\star$) Let $\mathcal{C}$ be a code in $\mathbb{F}_2^{nL}$. Then Construction $C^\star \in \mathbb{R}^n$ is defined as*

$$\begin{aligned} \Gamma_{C^\star} \;\; := \;\; & \{c_1 + 2c_2 + \cdots + 2^{L-1}c_L + 2^L z : (c_1, c_2, \ldots, c_L) \in \mathcal{C}, \\ & c_i \in \mathbb{F}_2^n, i = 1, \ldots, L, z \in \mathbb{Z}^n\}. \end{aligned} \tag{22}$$

Definition 8. *(Projection codes) Let $c = (c_1, c_2, ..., c_L)$ be a partition of a codeword $c = (c_{11}, \ldots, c_{1n}, ..., c_{L1}, \ldots, c_{Ln}) \in \mathcal{C}$ into length$-n$ subvectors $c_i = (c_{i1}, ..., c_{in})$, $i = 1, \ldots, L$. Then, a projection code $\mathcal{C}_i$ consists of all subvectors c_i that appear as we scan through all possible codewords $c \in \mathcal{C}$. Note that if $\mathcal{C}$ is linear, then every projection code $\mathcal{C}_i, i = 1, \ldots, L$ is also linear.*

Definition 9. *(Associated Construction C) Given a Construction $C^\star$ defined by a linear binary code $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$, we call the associated Construction C the constellation defined as*

$$\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + \cdots + 2^{L-1}\mathcal{C}_L + 2\mathbb{Z}^n, \tag{23}$$

such that $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L \in \mathbb{F}_2^n$ are the projection codes of $\mathcal{C}$ as in Definition 8.

Remark 2. *If $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$ then Construction $C^\star$ coincides with Construction C, because the projection codes are independent. However, in general, not all combinations of elements of projection codes compose a codeword in the main code $\mathcal{C}$, so we get a subset of the associated Construction C., i.e., $\Gamma_{C^\star} \subseteq \Gamma_C$.*

Example 5. *Consider a linear binary code $\mathcal{C}$ with length $nL = 4$, ($L = n = 2$), where $\mathcal{C} = \{(0,0,0,0),\ (1,0,0,1),(1,0,1,0),\ (0,0,1,1)\} \subseteq \mathbb{F}_2^4$. Thus, an element $x(c,z) \in \Gamma_{C^\star}$, $c \in \mathcal{C}, z \in \mathbb{Z}^2$ can be written as*

$$x(c,z) = c_1 + 2c_2 + 4z \ \in \Gamma_{C^\star}, \tag{24}$$

for some $(c_1, c_2) \in \mathcal{C}$ and $z \in \mathbb{Z}^2$. Geometrically, the resulting constellation is given by the blue points represented in Figure 4. Note that $\Gamma_{C^\star}$ is not a lattice. However, if we consider the associated Construction C with codes $\mathcal{C}_1 = \{(0,0),(1,0)\}$ and $\mathcal{C}_2 = \{(0,0),(1,1),(0,1),(1,0)\}$, we have a lattice (pink points in Figure 4), because $\mathcal{C}_1$ and $\mathcal{C}_2$ satisfy the condition given by Theorem 1.

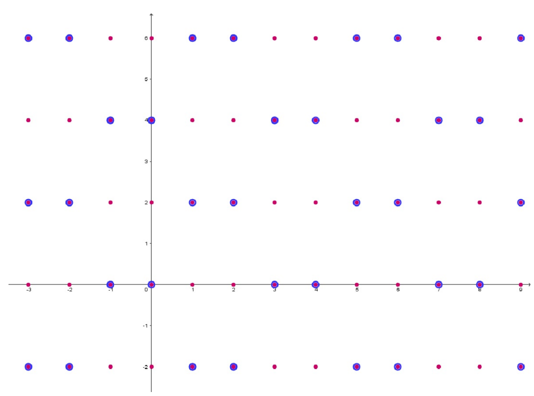

Fig. 4. (Nonlattice) Construction $C^\star$ constellation in blue and its associated (lattice) Construction C constellation in pink.

The next example presents a case where both Constructions $C^\star$ and C are lattices, but they are not equal.

Example 6. *Let a linear binary code $\mathcal{C} = \{(0,0,0,0),\ (0,0,1,0),(1,0,0,1),(1,0,1,1)\} \subseteq \mathbb{F}_2^4$ ($nL = 4,\ L = n = 2$), so the projection codes are $\mathcal{C}_1 = \{(0,0),(1,0)\}$ and $\mathcal{C}_2 = \{(0,0),(1,0),$*

$(0,1),(1,1)\}$. *An element* $w \in \Gamma_{C^\star}$ *can be described as*

$$x(c,z) = \begin{cases} (0,0)+4z, & \text{if } c_1=(0,0) \text{ and } c_2=(0,0) \\ (1,2)+4z, & \text{if } c_1=(1,0) \text{ and } c_2=(0,1) \\ (2,0)+4z, & \text{if } c_1=(0,0) \text{ and } c_2=(1,0) \\ (3,2)+4z, & \text{if } c_1=(1,0) \text{ and } c_2=(1,1), \end{cases} \tag{25}$$

for all $c \in \mathcal{C}$ *and* $z \in \mathbb{Z}^2$. *This construction is represented by black points in Figure 5. Note that* $\Gamma_{C^\star}$ *is a lattice and* $\mathcal{C} \neq \mathcal{C}_1 \times \mathcal{C}_2$, *which implies that* $\Gamma_{C^\star} \neq \Gamma_C$. *Nevertheless, the associated Construction C is also a lattice (Figure 5).*

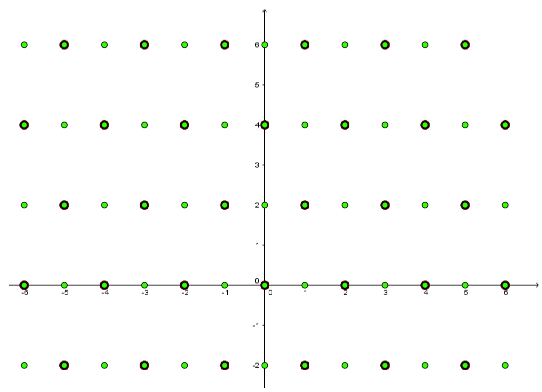

Fig. 5. (Lattice) Construction $C^\star$ constellation in black and its associated (lattice) Construction C constellation in green.

To appreciate the advantage of $\Gamma_{C^\star}$ *over the associated* Γ_C *in this case, one can notice that the packing densities are, respectively* $\Delta_{\Gamma_{C^\star}} = \frac{\Pi}{4} \approx 0.7853$ *and* $\Delta_{\Gamma_C} = \frac{\Pi}{8} \approx 0.3926$.

We can also describe the densest lattice in dimension 24, the Leech lattice Λ_{24}, in terms of Construction $C^\star$ constellation with $L=3$ levels.

Example 7. *Based on the construction given by Conway and Sloane [6] (pp. 131-132) and Amrani et al [2], we start by considering three special linear binary codes*

- $\mathcal{C}_1 = \{(0,\ldots,0),(1,\ldots,1)\} \subseteq \mathbb{F}_2^{24}$;
- $\mathcal{C}_2$ *as a Golay code* $\mathcal{C}_{24} \subset \mathbb{F}_2^{24}$ *achieved by adding a parity bit to the original* $[23,12,7]-$*binary Golay code* $\mathcal{C}_{23}$, *which consists in a quadratic residue code of length 23;*

- $\mathcal{C}_3 = \tilde{\mathcal{C}}_3 \cup \overline{\mathcal{C}}_3 = \mathbb{F}_2^{24}$, *where* $\tilde{\mathcal{C}}_3 = \{(x_1, \ldots, x_{24}) \in \mathbb{F}_2^{24} : \sum_{i=1}^{24} x_1 \equiv 0 \mod 2\}$ *and* $\overline{\mathcal{C}}_3 = \{(y_1, \ldots, y_{24}) \in \mathbb{F}_2^{24} : \sum_{i=1}^{24} y_1 \equiv 1 \mod 2\}$.

Observe that $\mathcal{C}_1, \mathcal{C}_2$ *and* $\mathcal{C}_3$ *are linear codes. Consider a code* $\mathcal{C} \subseteq \mathbb{F}_2^{72}$ *whose codewords are described in one of two possible ways:*

$$\mathcal{C} = \{(0, \ldots, 0, \underbrace{a_1, \ldots, a_{24}}_{\in \mathcal{C}_{24}}, \underbrace{x_1, \ldots, x_{24}}_{\in \tilde{\mathcal{C}}_3}), (1, \ldots, 1, \underbrace{a_1, \ldots, a_{24}}_{\in \mathcal{C}_{24}}, \underbrace{y_1, \ldots, y_{24}}_{\in \overline{\mathcal{C}}_3})\}. \tag{26}$$

Thus, we can define the Leech lattice Λ_{24} *as a* $3-$*level Construction* $C^\star$ *given by*

$$\Lambda_{24} = \Gamma_{C^\star} = \{c_1 + 2c_2 + 4c_3 + 8z : (c_1, c_2, c_3) \in \mathcal{C}, z \in \mathbb{Z}^{24}\}. \tag{27}$$

Observe that $\Gamma_{C^\star} \neq \Gamma_C$ *and in this case, the associated Construction C has packing density* $\Delta_{\Gamma_C} \approx 0.00012 < 0.001929 \approx \Delta_{\Gamma_{C^\star}}$, *which is the packing density of* Λ_{24}, *the best known packing density in dimension* 24 *[5].*

VI. Geometric uniformity and latticeness of Construction $\mathcal{C}^\star$

We verified previously that a $2-$level Construction C $\Gamma_C = \mathcal{C}_1 + 2\mathcal{C}_2 + \mathbb{Z}^n$, where $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_2^n$ are linear codes, is geometrically uniform even in the case it is not a lattice. Another question that emerges is: is a 2-level Construction $C^\star$ also geometrically uniform? As we show below, the answer is affirmative.

Theorem 3. *(Geometric uniformity of* $2-$*level Construction* $C^\star$*) Consider the binary linear code* $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$. *Then,* $\Gamma_{C^\star} = \{c_1 + 2c_2 + 4z : (c_1, c_2) \in \mathcal{C}, z \in \mathbb{Z}^n\}$ *is geometrically uniform.*

Proof. It uses analogue arguments to the geometric uniformity of Construction C, assuming the same isometry given by Equation (16). In summary, fixed $x = c_1 + 2c_2 + 4z \in \Gamma_{C^\star}$, with $(c_1, c_2) \in \mathcal{C}$ and given $y = \tilde{c}_1 + 2\tilde{c}_2 + 4\tilde{z} \in \Gamma_{C^\star}$, $(\tilde{c}_1, \tilde{c}_2) \in \mathcal{C}$, it is true that $T_{c_1}(y - x) = ((\tilde{c}_1 - c_1) \mod 2) + 2((\tilde{c}_2 - c_2) \mod 2) + 4z'$, where z' is suitably chosen according to the value of the difference in each coordinate. Clearly, $((\tilde{c}_1 - c_1) \mod 2, (\tilde{c}_2 - c_2) \mod 2) \in \mathcal{C}$, then $T_{c_1}(y - x) \in \Gamma_{C^\star}$. To prove that $T_{c_1}(\Gamma_{C^\star} - x) = \Gamma_{C^\star}$, we still need to show the reverse statement, i.e., that for each $y \in \Gamma_{C^\star}$ there exists $y' \in \Gamma_{C^\star}$ such that $T_{c_1}(y' - x) = y$. However, this fact follows from the above derivation because $T_{c_1}(y - x)$ is an isometry (as a function of y). Therefore, we can conclude that for $L = 2$, $\Gamma_{C^\star}$ is geometrically uniform. $\square$

As we have seen in Example 3, Construction C is not geometrically uniform for general $L \geq 3$. If we consider $\mathcal{C} \subseteq \mathbb{F}_2^3$, as the product $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \mathcal{C}_3$, we get in this particular example, $\Gamma_C = \Gamma_{C^star}$ and therefore, not geometrically uniform in general for $L \geq 3$.

The work in [13] motivated our search for a condition to guarantee latticeness of Construction $C^\star$. Note that, the approach in [13] consisted to compare Construction C with the lattice Construction D and in our case, there is no known lattice to be compared, which requires a different strategy. In the upcoming discussion, we will present a condition for $\Gamma_{C^\star}$ to be a lattice.

Definition 10. *(Antiprojection) The antiprojection (inverse image of a projection)* $\mathcal{S}_i(c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_L)$ *consists of all vectors* $c_i \in \mathcal{C}_i$ *that appear as we scan through all possible codewords* $c \in \mathcal{C}$*, while keeping* $c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_L$ *fixed:*

$$\mathcal{S}_i(c_1, ..., c_{i-1}, c_{i+1}, ..., c_L) = \{c_i \in \mathcal{C}_i : (c_1, \ldots, \underbrace{c_i}_{i\text{-th posititon}}, \ldots, c_L) \in \mathcal{C}\}. \tag{28}$$

Example 8. *In Example 6, we can define the antiprojection*

$$\mathcal{S}_2(c_1) = \{c_2 \in \mathcal{C}_2 : (c_1, c_2) \in \mathcal{C}\}. \tag{29}$$

For $c_1 = (0,0) \in \mathcal{C}_1$ *we have* $\mathcal{S}_2(c_1) = \{(0,0),(1,0)\}$ *and for* $c_1 = (1,0) \in \mathcal{C}_1$, $\mathcal{S}_2(c_1) = \{(0,1),(1,1)\}$.

We next introduce the following auxiliary result:

Lemma 1. *(Sum in* $\Gamma_{C^\star}$*) Let* $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ *be a binary linear code. If* $x, y \in \Gamma_{C^\star}$ *are such that*

$$x = c_1 + 2c_2 + \cdots + 2^{L-1}c_L + 2^L z \tag{30}$$

$$y = \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{L-1}\tilde{c}_L + 2^L \tilde{z}, \tag{31}$$

with $(c_1, c_2, \ldots, c_L), (\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_L) \in \mathcal{C}$ *and* $z, \tilde{z} \in \mathbb{Z}^n$*, then*

$$x + y = c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + +2^{L-1}(s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) + 2^L(s_L^\star + z + \tilde{z}), \tag{32}$$

where $s_i \in \mathbb{F}_2^n$ *is the "carry" from level* i *to level* $i+1$*, given by*

$$s_i = (c_i * \tilde{c}_i) \oplus r_i^1 \oplus r_i^2 \oplus \cdots \oplus r_i^{i-1} = (c_i * \tilde{c}_i) \bigoplus_{j=1}^{i-1} r_i^j,$$
$$r_i^1 = (c_i \oplus \tilde{c}_i) * (c_{i-1} * \tilde{c}_{i-1}), \quad r_i^j = r_i^{j-1} * r_{i-1}^{j-1},$$
$$2 \leq j \leq i-1, i = 2, \ldots, L-1 \tag{33}$$

$s_0 = (0, \ldots, 0)$ and $s_1 = c_1 * \tilde{c}_1$ and the formula for $s_L^\star$ is the same for s_i but with real sum instead of modulo-2 sum.

Proof. Through induction in the number L of levels:

Base case: For $L = 1$ level, $\mathcal{C} \subseteq \mathbb{F}_2^n$ has only one subcode $\mathcal{C}_1$. Consider $x, y \in \Gamma_{C^\star}$ such that $x = c_1 + 2z$ and $y = \tilde{c}_1 + 2\tilde{z}$. Then

$$x + y = c_1 + \tilde{c}_1 + 2(z + \tilde{z}) = c_1 \oplus \tilde{c}_1 + 2(\underbrace{c_1 * \tilde{c}_1}_{s_1 \in \mathbb{Z}^n} + z + \tilde{z}) \tag{34}$$

and the result is valid.

Induction step: Assume that the formula in Equation (32) is valid for $L = k-1$, where the main code $\tilde{\mathcal{C}} \in \mathbb{F}_2^{n(k-1)}$ has subcodes $\mathcal{C}_1, \ldots, \mathcal{C}_{k-1} \in \mathbb{F}_2^n$. Therefore, our induction hypothesis affirms that for $x, y \in \Gamma_{C^\star}$ such that

$$x = c_1 + 2c_2 + \cdots + 2^{k-2}c_{k-1} + 2^{k-1}z \tag{35}$$

$$y = \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{k-2}\tilde{c}_{k-1} + 2^{k-1}\tilde{z}, \tag{36}$$

with $z, \tilde{z} \in \mathbb{Z}^n$, is true that

$$\begin{aligned} x + y &= c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + 2^{k-2}(s_{k-2} \oplus (c_{k-1} \oplus \tilde{c}_{k-1})) \\ &+ 2^{k-1}(s_{k-1}^\star + z + \tilde{z}), \end{aligned} \tag{37}$$

where $s_{k-1}^\star$ is s_{k-1} and $s_i, i = 1, \ldots, L$ as in Equation (33).

We aim to prove that the formula presented in Equation (32) is also satisfied for $L = k$. So, consider the main code $\mathcal{C} \in \mathbb{F}_2^{nk}$ with subcodes $\mathcal{C}_1, \ldots, \mathcal{C}_{k-1}, \mathcal{C}_k \in \mathbb{F}_2^n$. Suppose $\overline{x}, \overline{y} \in \Gamma_{C^\star}$ such that

$$\overline{x} = c_1 + 2c_2 + \cdots + 2^{k-2}c_{k-1} + 2^{k-1}c_k + 2^k z \tag{38}$$

$$\overline{y} = \tilde{c}_1 + 2\tilde{c}_2 + \cdots + 2^{k-2}\tilde{c}_{k-1} + 2^{k-1}\tilde{c}_k + 2^k \tilde{z}. \tag{39}$$

So we can write, applying the induction hypothesis

$$\begin{aligned} \overline{x} + \overline{y} &= c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + 2^{k-2}(s_{k-2} \oplus (c_{k-1} \oplus \tilde{c}_{k-1})) + \\ & \quad 2^{k-1}(s_{k-1}^\star + c_k + \tilde{c}_k) + 2^k(z + \tilde{z}), \end{aligned} \tag{40}$$

where $s^\star_{k-1}$ is s_{k-1} with the real sum instead of modulo-2 sum. By doing all the decompositions to change the real sum $s^\star_{k-1} + c_k + \tilde{c}_k$ to $s_{k-1} \oplus c_k \oplus \tilde{c}_k$ we have

$$\begin{aligned}\overline{x} + \overline{y} \;\; = \;\; & c_1 \oplus \tilde{c}_1 + 2(s_1 \oplus (c_2 \oplus \tilde{c}_2)) + \cdots + 2^{k-2}(s_{k-2} \oplus (c_{k-1} \oplus \tilde{c}_{k-1})) + \\ & 2^{k-1}(s_{k-1} \oplus (c_k \oplus \tilde{c}_k)) + 2^k(\underbrace{(c_k * \tilde{c}_k) + r_k^1 + r_k^2 + \cdots + r_k^{k-1}}_{s^\star_k} + z + \tilde{z}). \qquad (41)\end{aligned}$$

This formula is exactly as we expected and it concludes the proof. □

The mathematical intuition behind the necessary and sufficient condition to guarantee that $\Gamma_{C^\star}$ is a lattice lies in the fact that since $a + b = a \oplus b + 2(a * b)$ for $a, b \in \mathbb{F}_2^n$, when adding two points in Γ_C or $\Gamma_{C^\star}$, each level $i \geq 2$ has the form of $c_i \oplus \tilde{c}_i \oplus carry_{(i-1)}$, where $carry_{(i-1)}$ is the "carry" term from the addition in the lower level. Since the projection code $\mathcal{C}_i$ is linear, $c_i \oplus \tilde{c}_i$ is a codeword in the $i-$th level. Hence, closeness of $\Gamma_{C^\star}$ under addition amounts to the fact that $carry_{(i-1)}$ is also a codeword in $\mathcal{C}_i$, which is essentially the condition of the theorem. Formally,

Theorem 4. *(Lattice condition for $\Gamma_{C^\star}$) Let $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ be a linear binary code that generates $\Gamma_{C^\star}$ and let the set $\mathcal{S} = \{(0, s_1, \ldots, s_{L-1})\} \subseteq \mathbb{F}_2^{nL}$ defined for all pairs $c, \tilde{c} \in \mathcal{C}$ (including the case $c = \tilde{c}$), where*

$$\begin{gathered} s_i = (c_i * \tilde{c}_i) \oplus r_i^1 \oplus r_i^2 \oplus \cdots \oplus r_i^{i-1} = (c_i * \tilde{c}_i) \bigoplus_{j=1}^{i-1} r_i^j, \\ r_i^1 = (c_i \oplus \tilde{c}_i) * (c_{i-1} * \tilde{c}_{i-1}), \quad r_i^j = r_i^{j-1} * r_{i-1}^{j-1}, \\ 2 \leq j \leq i-1, i = 2, \ldots, L-1, \qquad (42) \end{gathered}$$

$s_0 = (0, \ldots, 0)$ and $s_1 = c_1 * \tilde{c}_1$. Then, the constellation $\Gamma_{C^\star}$ is a lattice if and only if $\mathcal{S} \subseteq \mathcal{C}$.

Proof. $(\Rightarrow)$ Assume $\Gamma_{C^\star}$ to be lattice. This implies that if $x, y \in \Gamma_{C^\star}$ then $x + y \in \Gamma_{C^\star}$. From the notation and result from Lemma 1, more specifically Equations (35), (36), (32) and (33), it means that

$$(c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) \in \mathcal{C}. \qquad (43)$$

We can write this $L-$tuple as

$$\begin{aligned} & \underbrace{(c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L))}_{\in \mathcal{C}} = \\ & \underbrace{(c_1 \oplus \tilde{c}_1, c_2 \oplus \tilde{c}_2, \ldots, c_L \oplus \tilde{c}_L)}_{\in \mathcal{C}, \text{ by linearity of } \mathcal{C}} \oplus (0, s_1, \ldots, s_{L-1}) \Rightarrow (0, s_1, \ldots, s_{L-1}) \in \mathcal{C}, \qquad (44) \end{aligned}$$

which is the same as saying that for all $x, y \in \Gamma_{C^\star}$, $\mathcal{S} \subseteq \mathcal{C}$.

($\Leftarrow$) The converse is immediate, because given $x, y \in \Gamma_{C^\star}$ as in Equations (35) and (36), with the fact that $\mathcal{C}$ is linear and $\mathcal{S} \subseteq \mathcal{C}$, it is valid that

$$\begin{aligned} & (c_1 \oplus \tilde{c}_1, c_2 \oplus \tilde{c}_2, \ldots, c_L \oplus \tilde{c}_L) \oplus (0, s_1, \ldots, s_{L-1}) \in \mathcal{C} \\ \Rightarrow \quad & (c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) \in \mathcal{C} \end{aligned} \tag{45}$$

and $x + y \in \Gamma_{C^\star}$. We still need to prove that there exist the inverse element $-x \in \Gamma_{C^\star}$. It is true that for $x \in \Gamma_{C^\star}$, $x + x \in \Gamma_{C^\star}$ and also $(x + x) + (x + x) \in \Gamma_{C^\star}$. If we do this sum recursively, i.e., $\underbrace{x + x + x + \cdots + x}_{2^L \text{ times}} = 2^L j$, for a suitably $j \in \mathbb{Z}^n$. So, if we consider $y = \underbrace{x + x + \cdots + x}_{2^L - 1 \text{ times}} + 2^L(-j) \in \Gamma_{C^\star}$, because it a sum of elements in $\Gamma_{C^\star}$ for a convenient $-j \in \mathbb{Z}^n$ and it follows that $x + y = 0 \in \mathbb{R}^n$ and $y = -x$. $\square$

Example 9. *Consider the linear binary code given by* $\mathcal{C} = \{(0,0,0,0,0,0), (1,0,1,1,0,1), (0,0,1,0,1,1), (1,0,0,1,1,0), (0,0,0,0,1,0), (0,0,1,0,0,1), (1,0,0,1,0,0), (1,0,1,1,1,1)\} \subseteq \mathbb{F}_2^6$ *with* $L = 3, n = 2$. *In this specific case, it is possible to describe the set* $\mathcal{S} = \{(0,0,0,0,0,0), (0,0,1,0,1,1), (0,0,0,0,1,0), (0,0,1,0,0,1)\} \subseteq \mathcal{C}$. *Therefore, according to Theorem 4,* $\Gamma_{C^\star}$ *is a lattice.*

Remark 3. *Note that with the assumption that* $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$, *i.e.,* $\Gamma_C = \Gamma_{C^\star}$, *it follows that* $\mathcal{S} \subseteq \mathcal{C}$ *is equivalent to* $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ *and the chain is closed under Schur product [13]. Indeed,*

i) $\mathcal{S} \subseteq \mathcal{C} \Rightarrow \mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ *and the chain is closed under Schur product: we know that* $\mathcal{S} \subseteq \mathcal{C}$ *for any pair* $c, \tilde{c}$ *of codewords, so we take in particular* $\tilde{c} = c$ *and it follows that* $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$. *The fact that* $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$ *allows us to guarantee that the element* $(0, c_1 * \tilde{c}_1, c_2 * \tilde{c}_2, \ldots, c_{L-1} * \tilde{c}_{L-1}) \in \mathcal{S} \subseteq \mathcal{C}$ *and then the above chain will be closed under Schur product.*

ii) $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ *and the chain is closed under Schur product* $\Rightarrow \mathcal{S} \subseteq \mathcal{C}$: *consider an element* $(0, s_1, s_2, \ldots, s_{L-1}) \in \mathcal{S}$, *we want to prove that this element is also in* $\mathcal{C}$ *and to do that it is enough to prove that* $s_1 \in \mathcal{C}_2, s_2 \in \mathcal{C}_3 \ldots\ s_{L-1} \in \mathcal{C}_L$. *Indeed, due to the chain be* *closed under Schur product,*

$$\begin{aligned} s_1 &= c_1 * \tilde{c}_1 \in \mathcal{C}_2 && (46)\\ s_2 &= \underbrace{((c_1 * \tilde{c}_1) * (c_2 \oplus \tilde{c}_2))}_{\in \mathcal{C}_3} \oplus \underbrace{(c_2 * \tilde{c}_2)}_{\in \mathcal{C}_3} \in \mathcal{C}_3 && (47)\\ s_3 &= \underbrace{((c_3 \oplus \tilde{c}_3) * (c_2 * \tilde{c}_2)) * (c_2 \oplus \tilde{c}_2 * (c_1 * \tilde{c}_1))}_{\in \mathcal{C}_4} \\ &\oplus \ \underbrace{((c_3 \oplus \tilde{c}_3) * (c_2 * \tilde{c}_2))}_{\in \mathcal{C}_4} \oplus \underbrace{(c_3 * \tilde{c}_3)}_{\in \mathcal{C}_4} \in \mathcal{C}_4 && (48)\\ &\vdots \end{aligned}$$

and proceeding recursively, we can prove that $s_i \in \mathcal{C}_{i+1}, i = 1, \ldots, L-1$.

The previous remark lead the us to the following result:

Corollary 2. *(Latticeness of associated Construction C) Let* $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$. *If* $\Gamma_{C^\star}$ *is a lattice then also the associated Construction C is also lattice.*

Proof. If $\Gamma_{C^\star}$ is a lattice, then according to Theorem 4, $\mathcal{S} \subseteq \mathcal{C}$. In the associated Construction C, we make $\mathcal{C} = \mathcal{C}_1 \times \mathcal{C}_2 \times \cdots \times \mathcal{C}_L$, where $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L$ are the projection codes. Hence, according to the Remark 3, $\mathcal{S} \subseteq \mathcal{C}$ is equivalent to $\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_L$ and the chain being closed under Schur product, which is sufficient to guarantee that Γ_C is a lattice. □

Observe that condition given by Theorem 4 is well-established, however, it is not easy to check for lattices in higher dimensions. For this reason, we introduce the following consequent result which is weaker, but easier to verify in general.

Corollary 3. *(Special lattice condition for* $\Gamma_{C^\star}$*) Let* $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ *be a linear binary code with projection codes* $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L$ *such that* $\mathcal{C}_1 \subseteq \mathcal{S}_2(0, \ldots, 0) \subseteq \mathcal{C}_2 \subseteq \cdots \subseteq \mathcal{C}_{L-1} \subseteq \mathcal{S}_L(0, \ldots, 0) \subseteq \mathcal{C}_L \subseteq \mathbb{F}_2^n$. *Then the constellation given by* $\Gamma_{C^\star}$ *represents a lattice if and only if* $\mathcal{S}_i(0, \ldots, 0)$ *closes* $\mathcal{C}_{i-1}$ *under Schur product for all levels* $i = 2, \ldots, L$.

Proof. $(\Leftarrow)$ For any $x, y \in \Gamma_{C^\star}$, written as in Equations (35) and (36), we have $x + y$ as given in Lemma 1 (Equations (32) and (33)) and we need to verify if $x + y \in \Gamma_{C^\star}$.

Clearly $x + y \in \mathcal{C}_1 + 2\mathcal{C}_2 + \cdots + 2^{L-1}\mathcal{C}_L + 2^L\mathbb{Z}^n$. It remains to demonstrate that $(c_1 \oplus \tilde{c}_1, s_1 \oplus c_2 \oplus \tilde{c}_2, \ldots, s_{L-1} \oplus c_L \oplus \tilde{c}_L) \in \mathcal{C}$.

Indeed, using the fact that the chains $\mathcal{C}_{i-1} \subseteq \mathcal{S}_i(0,\ldots,0)$ for all $i = 2,\ldots,L$ are closed under the Schur product, it is an element of $\mathcal{C}$ because it is a sum of elements in $\mathcal{C}$, i.e.,

$$\begin{aligned}
&(c_1 \oplus \tilde{c}_1, s_1 \oplus c_2 \oplus \tilde{c}_2, \ldots, s_{L-1} \oplus c_L \oplus \tilde{c}_L) = \\
&\underbrace{(c_1 \oplus \tilde{c}_1, c_2 \oplus \tilde{c}_2, \ldots, c_L \oplus \tilde{c}_L)}_{\in \mathcal{C}} \oplus \underbrace{(0, s_1, \ldots, 0)}_{\in \mathcal{C}} \oplus \cdots \oplus \\
&\oplus \underbrace{(0, \ldots, 0, s_{L-1})}_{\in \mathcal{C}} \Rightarrow (0, s_1, \ldots, s_{L-1}) \in \mathcal{C} \qquad (49)
\end{aligned}$$

and from Theorem 4, $\Gamma_{C^\star}$ is a lattice. Observe that any $nL-$tuple $(0,\ldots,s_{i-1},\ldots,0)$ is in $\mathcal{C}$ because by hypothesis, the chain $\mathcal{S}_i(0,\ldots,0)$ closes $\mathcal{C}_{i-1}$ under Schur product, hence $S_i(0,\ldots,0)$ contains $(c_{i-1} * \tilde{c}_{i-1}), r_{i-1}^1, \ldots., r_{i-1}^{i-2}$ which is sufficient to guarantee that $s_{i-1} \in \mathcal{S}_i(0,\ldots,0)$ so $(0,\ldots,s_{i-1},\ldots,0) \in \mathcal{C}$, for all $i = 2,\ldots,L-1$. Using analogue arguments to Theorem 4, given $x \in \Gamma_{C^\star}$ it is true that $-x \in \Gamma_{C^\star}$.

($\Rightarrow$) For the converse, we know that given $x, y \in \Gamma_{C^\star}$ then $x + y \in \Gamma_{C^\star}$. From the notation and result from Lemma 1, more specifically Equations (35), (36), (32) and (33), it means that

$$(c_1 \oplus \tilde{c}_1, s_1 \oplus (c_2 \oplus \tilde{c}_2), \ldots, s_{L-1} \oplus (c_L \oplus \tilde{c}_L)) \in \mathcal{C} \qquad (50)$$

and from the result of Theorem 4 follows that

$$(0, s_1, \ldots, s_{L-1}) \in \mathcal{C}, \qquad (51)$$

where s_i, $i = 1,\ldots,L-1$ are defined as in Equations (47)–(49).

Due to the nesting $\mathcal{C}_1 \subseteq \mathcal{S}_2(0,\ldots,0) \subseteq \cdots \subseteq \mathcal{C}_{L-1} \subseteq \mathcal{S}_L(0,\ldots,0) \subseteq \mathcal{C}_L$, we can guarantee that there exist codewords with particular Schur products $c_i * \tilde{c}_i = 0$, for $i = 1,\ldots,L-2$. Thus, $s_{L-1} = (c_{L-1} * \tilde{c}_{L-1})$ and from Equation (51), $(0,0,\ldots,c_{L-1} * \tilde{c}_{L-1}) \in \mathcal{C}$, i.e., $S_L(0,\ldots,0)$ must close $\mathcal{C}_{L-1}$ under Schur product. Proceeding similarly, we demonstrate that $S_i(0,\ldots,0)$ must close $\mathcal{C}_{i-1}$, for all $i = 2,\ldots,L$ and it completes our proof. $\square$

While $\mathcal{S}_i(0,\ldots,0) \subseteq \mathcal{C}_i$ by construction, note that the assumption that $\mathcal{C}_i \subseteq \mathcal{S}_{i+1}(0,\ldots,0)$, for $i = 2,\ldots,L$ in Corollary 3 is not always satisfied by a general Construction $C^\star$, sometimes even if this Construction $C^\star$ is a lattice; see Example 9. In this cases we need the more general condition stated by Theorem 4.

The construction of the Leech lattice described in Example 7, for example, satisfies the condition proposed by Corollary 3, which are easier to verify.

VII. Minimum Euclidean distance of Construction $C^\star$

A. Minimum distance

An important remark is that unlike Construction C, Construction $C^\star$ is not equi-minimum distance, i.e., in general if the minimum distance d is achieved by two points $x, y \in \Gamma_{C^\star}$, i.e., $||x-y|| = d$ there may be some other $x' \in \Gamma_{C^\star}$ such that there is no $y' \in \Gamma_{C^\star}$ that makes $||x'-y'|| = d$.

Example 10. *Consider an $L = 3$ and $n = 1$ Construction $C^\star$ with main binary code $\mathcal{C} = \{(0,0,0),(1,0,1),(0,1,1),(1,1,0)\} \subset \mathbb{F}_2^3$. Thus, elements in $\Gamma_{C^\star}$ are*

$$\Gamma_{C^\star} = \{0+8z, 5+8z, 6+8z, 3+8z\}, z \in \mathbb{Z}. \tag{52}$$

The minimum Euclidean distance of $\Gamma_{C^\star}$ is $||6-5|| = 1$, but if we fix $x' = 0 \in \Gamma_{C^\star}$ there is no element $y' \in \Gamma_{C^\star}$ such that $||y'|| = 1$.

If $\Gamma_{C^\star}$ is equi-minimum distance, $d^2_{min}(\Gamma_{C^\star}) = d^2_{min}(\Gamma_{C^\star}, 0)$ (distance from any constellation point to zero), we know that to each $c \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}, c \neq 0$ we associate a unique element $x(c) \in \Gamma_{C^\star} \subseteq \mathbb{R}^n$ in the hypercube $[-2^{L-1}, 2^{L-1}]^n$, which gives the minimum distance of $\Gamma_{C^\star}(c)$ (constellation points generated by $c \in \mathcal{C}$.)

An explicit expression for the nearest constellation point in $\Gamma_{C^\star}(c)$ to zero regarding points in $\Gamma_{C^\star}$ generated by a codeword $c \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}$, $c \neq 0$ can also be written as

$$d^2_{min}(\Gamma_{C^\star}(c), 0) = m_1 + 2^2 m_2 + 3^2 m_3 + \cdots + (2^{L-1}-1)^2 m_{2^{L-1}-1} + (2^{L-1})^2 m_{2^{L-1}}, \tag{53}$$

where $m_i, i = 1, \ldots, 2^{L-1}$ are obtained as follows. For $c = (c_{11}, \ldots, c_{1n}, c_{21}, \ldots, c_{2n}, \ldots, c_{L1}, \ldots, c_{Ln})$ we consider the $L-$tuples $c_1 = (c_{11}, \ldots, c_{L1})$, $c_2 = (c_{12}, \ldots, c_{L2}), \ldots,$ $c_L = (c_{1n}, \ldots, c_{Ln})$ and $m_j, j = 1, \ldots, 2^{L-1}$ as

$$\begin{aligned} m_j \;\; = \;\; & \text{number of } L-tuples\ c_i,\ i = 1, \ldots, n, \text{ such that } c_i \text{ is the binary representation} \\ & \text{of j or the binary representation of } 2^{L-1} - j. \end{aligned} \tag{54}$$

To be more specific,

$$\begin{aligned} m_1 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (1,0,0,\ldots,0) \text{ or } c_i = \tilde{v}_i = (1,1,\ldots,1) \\ m_2 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (0,1,0,\ldots,0) \text{ or } c_i = \tilde{v}_i = (0,1,\ldots,1) \\ m_3 &= \text{the number of } c_i's \text{ such that } c_i = v_i = (1,1,0,\ldots,0) \text{ or } c_i = \tilde{v}_i = (1,0,1,\ldots,1) \end{aligned} \tag{55}$$

$$\begin{aligned}
&\vdots \qquad \vdots \\
m_{2^{L-1}-1} &= \text{the number of } c_i' s \text{ such that } c_i = v_i = (1,0,\ldots,1,0) \text{ or } c_i = \tilde{v}_i = (1,1,\ldots,0,1) \\
m_{2^{L-1}} &= \text{the number of } c_i' s \text{ such that } c_i = (0,0,0,\ldots,0,1).
\end{aligned} \tag{56}$$

Note that $\tilde{v}_i$ have the same coordinates of v_i up to the first nonzero coordinate and after that all coordinates are different. Moreover, $\sum_{i=1}^{2^L-1} m_i = n$.

Remark 4. *From the expression above, we can see that given a codeword $c \in \mathcal{C}$ of weight $\omega(c) = k$,*

$$d^2_{min}(\Gamma_{C^\star}(c), 0) \geq \frac{k}{L}, \tag{57}$$

since the minimum distance will be achieved when the projection codewords of c have the largest number of coincident coordinates as possible. Therefore, if the minimum distance d of the code $\mathcal{C}$ is such that $d_H(\mathcal{C}) \geq L2^{2L}$, we can assert that $d^2_{min}(\Gamma_{C^\star}, 0) = 2^{2L}$.

Example 11. *For $L = 2$ and $w \geq 32$, ($n \geq 16$), we have that $d^2_{min}(\Gamma_{C^\star}, 0) = 2^4$.*

A more concise expression for the minimum distance to zero in $\Gamma_{C^\star}$ can also be derived from (54), by observing that for $c = (c_1, c_2, \ldots, c_n) \in \mathcal{C}$, $c \neq 0$:

$$d^2_{min}(\Gamma_{C^\star}(c), 0) = ||2^{L-1}c_L - 2^{L-2}c_{L-1} - \cdots - 2c_2 - c_1||^2. \tag{58}$$

From what we get

$$d_{min}(\Gamma_{C^\star}, 0) = \min_{c=(c_1,c_2,\ldots,c_n)\in\mathcal{C}, c\neq 0} \{||2^{L-1}c_L - \sum_{i=1}^{L-1} 2^{i-1}c_i||^2, 2^{2L}\}. \tag{59}$$

If $\Gamma_{C^\star}$ is geometrically uniform, the above expression provides a closed formula for the minimum distance of $\Gamma_{C^\star}$, otherwise it is an upper bound for this distance. Equation (59) also presents a closed formula for the minimum distance of a lattice $\Gamma_{C^\star}$, i.e., when the conditions of Theorem 4 are satisfied.

From (59), it could be expected that given a code $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$ with minimum weight $d_H(\mathcal{C}) = d$ and minimum weight of projection codes $d_1, \ldots, d_L$, respectively, where $\sum_{i=1}^{L} d_i = d$, it will have a larger minimum distance as d_i increases with i.

For example, for $L = 2$ and weights of projection codes given by $d_H(\mathcal{C}_1)$ and $d_H(\mathcal{C}_2)$, respectively, if $d_H(\mathcal{C}_2) > d_H(\mathcal{C}_1)$, by considering $||2c_2 - c_1||^2 =< 2c_2 - c_1, 2c_2 - c_1 >$, we can derive from (59) that

$$d^2_{min}(\Gamma_{C^\star}) \geq \min\{4d_H(\mathcal{C}_2) - 3d_H(\mathcal{C}_1), 16\}. \tag{60}$$

Regarding to general upper and lower bounds, since $\Gamma_{C^\star}$ is a subset of Γ_C, $d^2_{min}(\Gamma_{C^\star}) \geq d^2_{min}(\Gamma_C)$, where Γ_C is the associated Construction C (Definition 9). An upper bound for $d^2_{min}(\Gamma_{C^\star})$ is $d^2_{min}(\Gamma_{C^\star}, 0)$, which satisfies

$$d^2_{min}(\Gamma_{C^\star}) \leq d^2_{min}(\Gamma_{C^\star}, 0) \leq 2^{2(i-1)} d_H(\mathcal{S}_i(0, \ldots, 0)), \tag{61}$$

for $i = 1, \ldots, L$. If we denote $d^2_{min}(\overline{\mathcal{S}}) = \min\limits_{d_H(\mathcal{S}_i(0,\ldots,0))\neq 0} \{d_H(\mathcal{S}_1(0, \ldots, 0)), 2^2 d_H(\mathcal{S}_2(0, \ldots, 0)), \ldots, 2^{2(L-1)} d_H(\mathcal{S}_L(0, \ldots, 0)), 2^{2L}\}$. Then, we have in general that

$$d^2_{min}(\Gamma_C) \leq d^2_{min}(\Gamma_{C^\star}) \leq d^2_{min}(\overline{\mathcal{S}}). \tag{62}$$

When $\Gamma_{C^\star} = \Gamma_C$ the sets $\mathcal{C}_i$ and $\mathcal{S}_i(0, \ldots, 0)$ for $i = 1, \ldots, L$ coincide and these bounds will give exactly the squared minimum distance.

Example 12. 1) *In Example 10, if we consider the associated Construction C, we have* $d^2_{min}(\Gamma_C) = \min\{1, 4, 16, 64\} = 1$ *and* $d^2_{min}(\overline{\mathcal{S}}) = \min\{64\} = 64$ *as* $\mathcal{S}_i(0, \ldots, 0)$ *are null sets for all* $i = 1, 2, 3$*. Hence,* $1 \leq d^2_{min}(\Gamma_{C^\star}) \leq 64$ *and* $d^2_{min}(\Gamma_{C^\star}) = 1$.

2) *For the Leech lattice presented in Example 7, we have that* $d^2_{min}(\Gamma_C) = \min\{24, 32, 32, 64\} = 24$ *and* $d^2_{min}(\overline{\mathcal{S}}) = \min\{32, 32, 64\} = 32$ *as* $\mathcal{S}_1(0, \ldots, 0)$ *is a null set. Thus,* $24 \leq d^2_{min}(\Gamma_{C^\star}) \leq 32$ *and the known minimum distance of the scaled Leech lattice, according to [6, pp. 133] is* 32.

3) *In Example 9,* $d^2_{min}(\Gamma_C) = \min\{1, 4, 16\} = 1$ *and* $d^2_{min}(\overline{\mathcal{S}}) = \min\{16\} = 16$ *as* $\mathcal{S}_1(0, \ldots, 0)$ *and* $\mathcal{S}_2(0, \ldots, 0)$ *are null sets. Hence,* $1 \leq d^2_{min}(\Gamma_{C^\star}) \leq 16$ *and the squared minimum distance in this case is* 5.

To derive a condition that states when Construction $C^\star$ have a better packing density than associated Construction C, we observe that both constellations $\Gamma_{C^\star}$ and its associated Γ_C contains the lattice $2^L\mathbb{Z}^n$, i.e., $2^L\mathbb{Z}^n \subseteq \Gamma_{C^\star} \subseteq \Gamma_C$. If the number of points of $\Gamma_{C^\star}$ and Γ_C inside the hypercube $[0, 2^L]^n$ are respectively $|\mathcal{C}|$ and $|\mathcal{C}_1| \ldots |\mathcal{C}_L|$, where $\mathcal{C}_i, i = 1, \ldots, L$ are the projection codes, we can assert

$$\Delta(\Gamma_{C^\star}) = \frac{|\mathcal{C}| \ vol\left(B\left(0, \frac{d_1}{2}\right)\right)}{2^{nL}} \quad \text{and} \quad \Delta(\Gamma_C) = \frac{|\mathcal{C}_1| \ldots |\mathcal{C}_L| \ vol\left(B\left(0, \frac{d_2}{2}\right)\right)}{2^{nL}}, \tag{63}$$

where $d_1 = d_{min}(\Gamma_{C^\star})$ and $d_2 = d_{min}(\Gamma_C)$. Hence, we can write the following remark:

Remark 5. 1) $\Delta(\Gamma_{C^\star}) \geq \Delta(\Gamma_C)$ *if and only if* $\left(\frac{d_1}{d_2}\right)^n \geq \frac{|\mathcal{C}_1|\ldots|\mathcal{C}_L|}{|\mathcal{C}|}$,

2) $\chi(\Gamma_{C^\star}) \geq \chi(\Gamma_C)$ *if and only if* $\frac{d_1}{d_2} \geq \left(\frac{|\mathcal{C}_1|\ldots|\mathcal{C}_L|}{|\mathcal{C}|}\right)^{1/n}$.

Example 13. *Let* $\mathcal{C} \subseteq \mathbb{F}_2^{2n}$*, i.e., we are considering a Construction* $C^\star$ *with* $L = 2$ *(therefore, geometrically uniform). If the minimum distance of the projection codes are* $d_H(\mathcal{C}_1) = 1$ *and* $d_H(\mathcal{C}_2) = 4$*, then, according to the formula in* (60)*,* $d^2_{min}(\Gamma_{C^\star}) \geq \min\{13, 16\} = 13$ *and* $d^2_{min}(\Gamma_C) = 1$*. Observe that, from the previous discussion,* $Delta(\Gamma_{C^\star}) \geq \Delta(\Gamma_C)$ *if*

$$(13)^{n/2} \geq \frac{|\mathcal{C}_1|\ldots|\mathcal{C}_L|}{|\mathcal{C}|}. \tag{64}$$

Example 14. *Consider the constellation* $\Gamma_{C^\star}$ *with* $L = 2, n = 4$*, generated by the main code* $\mathcal{C} = \{(0,0,0,0,0,0,0,0),(1,1,1,1,1,1,0,0),(0,0,0,0,1,1,1,1),(1,1,1,1,0,0,1,1)\}$*. Observe that* $d^2_{min}(\Gamma_{C^\star}) = d^2_{min}(\Gamma_C) = 4$ *and* $|\Gamma_C|/|\Gamma_{C^\star}| = 2$ *and Construction C presents a better packing density in this case.*

However, if we consider another code $\overline{\mathcal{C}}$ *(which is a permutation of* $\mathcal{C}$*) as* $\overline{\mathcal{C}} = \{(0,0,0,0,0,0,0,0),(1,1,0,0,1,1,1,1),(1,1,1,1,0,0,0,0),(0,0,1,1,1,1,1,1)\}$*, it is easy to see that* $d^2_{min}(\Gamma_{C^\star}) = 4$*,* $d^2_{min}(\Gamma_C) = 2$ *and again* $|\Gamma_C|/|\Gamma_{C^\star}| = 2$*. Here,* $\left(\frac{2}{\sqrt{2}}\right)^4 > 2$ *and* $\Gamma_{C^\star}$ *has a better packing density.*

Table VII-A summarizes density properties of previous examples according to the discussion presented in this subsection.

TABLE I

PROPERTIES OF CONSTRUCTION $C^\star$ AND ITS ASSOCIATED CONSTRUCTION C

Example	Dimension	$d^2_{min}(\Gamma_{C^\star})$	$d^2_{min}(\Gamma_C)$	$\Delta(\Gamma_{C^\star})$	$\Delta(\Gamma_C)$	$\chi(\Gamma_{C^\star})$	$\chi(\Gamma_C)$
5^*	2	1	1	$\pi/16$	$\pi/8$	0.4431	0.6266
6	2	4	1	$\pi/4$	$\pi/8$	0.8862	0.4431
7	24	32	24	0.001929	0.00012	0.7707	0.6236
9	2	5	1	0.8781	0.7853	0.9209	0.8861
10^*	1	1	1	0.5	1	0.5	1

B. Random interleaving

From the analysis in Subsection VII-A, it is clear that to the estimation of the minimum distance of Construction $C^\star$ is in general not an easy process. Since in order to compare Construction $C^\star$ with Construction C in terms of packing density or packing efficiency, the minimum distance is essential, we will work with *random interleaving* to approximate its average. This is also meaningful for communication applications, where the average error probability (in the presence of white Gaussian noise) is of interest.

The first analysis is regarding a deterministic interleaver. Let $c \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}$, $z \in \mathbb{Z}^n$ and $x(c,z)$ be the point in $\Gamma_{C^\star}$ given by the natural labeling. Note that each coordinate $x_j, j = 1, \ldots, n$ of $x(c,z)$ is generated by a vector of L bits and an integer z_j.

Given two codewords $c, \tilde{c} \in \mathcal{C}, c \neq \tilde{c}$ and $z, \tilde{z} \in \mathbb{Z}^n$, let n_m be the number of coordinates where the vectors $x(c,z)$ and $x(\tilde{c},\tilde{z})$ agree in the $m-1$ lower levels and disagree in the $m-$th level, $m = 1, \ldots, L$ and let n_0 be the number of coordinates where all levels are zero. Clearly, $n_0 + n_1 + n_2 + \cdots + n_L = n$, $n_1 + n_2 + \cdots + n_L \leq d_H(c,\tilde{c})$ and $n_1 + n_2 + \cdots + n_L = d_H(c,\tilde{c})$ if and only if $x(c,z)$ and $x(\tilde{c},\tilde{z})$ differ in each coordinate in at most one bit.

Proposition 1. *(Bound on the squared minimum distance) The squared minimum distance* $||x(c,z)$ $-x(\tilde{c},\tilde{z})||^2$ *between two points in Construction* $C^\star$ *is greater than or equal to*

$$n_1 + 4n_2 + \cdots + 4^{L-1}n_L. \tag{65}$$

For the special case when $L = 2$ and each coordinate of the integer vector z_2 is $z_1 - 1$ or $z_1 + 1$, according to which one gives the lowest distance (see also Equation **??**):

$$||x(c,z) - x(\tilde{c},\tilde{z})||^2 = n_1 + 4n_2. \tag{66}$$

If the interleaver π is random, then the numbers $n_1, \ldots, n_L$ above are random variables. Their expected value over all interleaver permutations is given by $E(n_m) = P_m \cdot n$, where

$$P_m = \frac{\begin{pmatrix} N-m \\ d-1 \end{pmatrix}}{\begin{pmatrix} N \\ d \end{pmatrix}} \approx P_1(1-P_1)^{m-1} \quad \text{for} \quad N \to \infty, \tag{67}$$

and $d = d_H(c,\tilde{c})$.

In particular, $P_1 = d/N$, $N = nL$. It follows from Equations (65) and (67) that the expected Euclidean distance between $x(c, z)$ and $x(\tilde{c}, \tilde{z})$, for $c \neq \tilde{c}$ is lower bounder by

$$E\{||x(\pi(c), z) - x(\pi(\tilde{c}), \tilde{z})||^2\} \geq n(P_1 + 4P_2 + \cdots + 2^{2L} P_L), \tag{68}$$

where $E(\cdot)$ denotes expectation with respect to all permutations π.

Considering the approximation in (67) for the probabilities when the dimension n goes to infinity, we have for $n \to \infty$:

$$E\left\{||x(\pi(c), z) - x(\pi(\tilde{c}), \tilde{z})||^2\right\} \geq d_c \sum_{l=1}^{L} \left[4\left(1 - \frac{d_c}{n}\right)\right]^{l-1}, \tag{69}$$

where $d_c = d_H(c, \tilde{c})/L$.

If we consider a Construction $C^\star$ with a random interleaver, then the average minimum squared distance between two distinct points in $\Gamma_{C^\star}$ is

$$\overline{d_E^2(\Gamma_{C^\star})} = E\left(\min_{y \neq \tilde{y} \in \Gamma_{C^\star}} ||y - \tilde{y}||^2\right), \tag{70}$$

for $y = x(\pi(c), z)$ and $\tilde{y} = (\pi(\tilde{c}), \tilde{z})$. That is, we take the closest two points for each permutation and then take an average. This quantity is what we wish we could estimate, however its estimation is hard. Instead, let us define the *minimum average* squared distance between two different points in $\Gamma_{C^\star}$ as

$$d_E^2(\overline{\Gamma_{C^\star}}) = \min_{y \neq \tilde{y} \in \Gamma_{C^\star}} E(||y - \tilde{y}||^2), \tag{71}$$

for $y = x(\pi(c), z)$ and $\tilde{y} = (\pi(\tilde{c}), \tilde{z})$. That is, we switch the order of expectation and minimum: take the two points which are closest on the average. Since Equation (68) lower bounds the expected squared distance for any two distinct codewords c and $\tilde{c}$, it follows that the minimum average squared distance of $\Gamma_{C^\star}$ is lower bounded by

$$d_E^2(\overline{\Gamma_{C^\star}}) \geq \min\left\{d_c \sum_{l=1}^{L} \left[4\left(1 - \frac{d_c}{n}\right)\right]^{l-1}, 2^{2L}\right\}, \tag{72}$$

where $d_c = d_H(\mathcal{C})/L$, and $d_H(\mathcal{C})$ is the minimum Hamming distance of the main code.

Clearly, the average minimum is smaller than the minimum average, i.e., $\overline{d_E^2(\Gamma_{C^\star})} \leq d_E^2(\overline{\Gamma_{C^\star}})$. In fact, since concentration occurs for most pairs but not for all pairs, the average minimum distance will be dictated by *atypical* pairs, whose distance is strictly below the average. Hence the estimate in Equation (71) is in general strictly larger than the desired quantity $\overline{d_E^2(\Gamma_{C^\star})}$. Nevertheless, in the next section we shall use the simple bound in Equation (71) to assess the packing efficiency of Construction $C^\star$.

VIII. Comparison of a hybrid Construction $C^\star/C$ and Construction C for Gilbert-Varshamov bound achieving codes

In this section, we aim to compare a hybrid Construction $C^\star/C$ to Construction C in terms of packing efficiency. To do that, we will use Gilbert-Varshamov Bound (GVB) achieving codes, i.e., codes whose size is related to their minimum Hamming distance d_H via

$$|C| \geq \frac{2^n}{|B(d-1,n)|}, \tag{73}$$

where $B(r,n)$ is an $n-$dimensional zero-centered Hamming ball of radius r, which is the set of all n length binary vectors with Hamming weight smaller than or equal to r. For a large n, $|B(r,n)| \doteq 2^{nH(\overline{q})}$, with $\overline{q} = r/n$ and where $H(\overline{q}) = -q\log_2 q - (1-q)\log_2(1-q)$ is the binary entropy function for $q \in [0,1]$.

Suppose we start with a Construction $C^\star$ with $L^\star$ levels, so that its distance satisfies

$$d^2_{min}(\Gamma_{C^\star}) = \min\left\{\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2L^\star}\right\}, \tag{74}$$

$c, \tilde{c} \in \mathcal{C} \subseteq \mathbb{F}_2^{nL}$. If the cubic term $2^{2L^\star}$ is the minimum, we add one level of Construction C above the $L^\star$ levels of Construction $C^\star$, with a code $\mathcal{C}_{L^\star+1}$ whose minimum Hamming distance is $d_{L^\star+1}$. The new construction is thus given by

$$\Gamma_{C^\star/C} = \{c_1 + 2c_2 + \cdots + 2^{L^\star-1}c_{L^\star} + 2^{L^\star}c_{L^\star+1} + 2^{L^\star+1}z\}, \tag{75}$$

$(c_1,\ldots,c_{L^\star}) \in \mathcal{C}, c_{L^\star+1} \in \mathcal{C}_{L^\star+1}, z \in \mathbb{Z}^n$. Its minimum distance satisfies

$$d^2_{min}(\Gamma_{C^\star/C}) = \min\left\{\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2L^\star}d_H(\mathcal{C}_{L^\star+1}), 2^{2(L^\star+1)}\right\}. \tag{76}$$

We choose the minimum Hamming distance $d_{L^\star+1}$ of the code $\mathcal{C}_{L^\star+1}$ large enough so that the second term will be the minimum. Again we check whether the cubic term $2^{2(L^\star+1)}$ minimizes. If it still does, then we add another level of Construction C and so on. We continue this process of adding more levels of Construction C until the cubic term stops being the minimum and we stop. Assuming we stopped after a total of L levels, the final formula is

$$\begin{aligned} d^2_{min}(\Gamma_{C^\star/C}) \quad = \quad & \min\{\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2L^\star}d_H(\mathcal{C}_{L^\star+1}), 2^{2(L^\star+1)}d_H(\mathcal{C}_{L^\star+2}), \ldots, \\ & 2^{2(L-1)}d_H(\mathcal{C}_L)\}. \end{aligned} \tag{77}$$

$c, \tilde{c} \in \mathcal{C}$.

We choose the minimum Hamming distances of the added codes in a balanced way, i.e., $d_{i+1} = d_i/4$, for all $L^\star < i < L$, similarly to what is required for Construction C in the definition from Conway and Sloane [6, pp. 150]. Then, we have $2^{2(L^\star+j)}d_H(\mathcal{C}_{L^\star+j+1}) = 2^{2(L-1)}d_H(\mathcal{C}_L)$, for all $0 \leq j \leq L-L^\star-1$ and $d^2_{min}(\Gamma_{C^\star/C}) = \min\{\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2, 2^{2(L^\star+j)}d_H(\mathcal{C}_{L^\star+j+1})\}$, for any j. We also assume a balancing condition with respect to the distances of Construction $C^\star$ and C, i.e., $\min\limits_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2 = 2^{2(L^\star+j)}d_H(\mathcal{C}_{L^\star+j+1})$, for any j.

According to the process described above and to take advantage of the special $L^\star = 2$ Construction $C^\star$, which is geometrically uniform, we define a hybrid Construction $C^\star/C$ as:

Definition 11. *(Hybrid Construction $C^\star/C$ for $L^\star = 2$) Let $\mathcal{C}$ be a code in $\mathbb{F}_2^{2n}$ and $\mathcal{C}_3,\ldots,\mathcal{C}_L$ be binary linear codes in $\mathbb{F}_2^{nL}$. Then the Hybrid Construction $C^\star/C$ is defined by*

$$\begin{aligned} \Gamma_{C^\star/C} \;:=\; & \{c_1 + 2c_2 + 4c_3 + \cdots + 2^{L-1}c_L + 2^L z : (c_1,c_2)\in\mathcal{C} \textit{ and} \\ & c_i \in \mathcal{C}_i,\ i=3,\ldots,L,\ z\in\mathbb{Z}^n\}. \end{aligned} \tag{78}$$

Suppose that, in terms of Definition 11, $\mathcal{C}\subseteq\mathbb{F}_2^{2n}$ and $\mathcal{C}_3,\ldots,\mathcal{C}_L\subseteq\mathbb{F}_2^n$ are all VGB achieving codes and also that 2^{2L} is not the minimum squared distance of the $\Gamma_{C^\star/C}$. Assume also the balanced condition of Construction C, i.e., the Hamming distance $d_H(\mathcal{C}_i)$ of $\mathcal{C}_i$ is 4 times smaller than $d_H(\mathcal{C}_{i-1})$ for $i = 4,\ldots,L$. For large n, we may admit the approximation of $\min_{c\neq\tilde{c}} ||x(c,z), x(\tilde{c},\tilde{z})||^2$ as lower bounded by the average $d_{min}(\overline{\Gamma_{C^\star}})$ as in Equation (71). Taking $q = d_H(\mathcal{C})/2n$ and $q_3 = d_H(\mathcal{C}_3)/n$, we have:

$$d_E^2(\Gamma_{C^\star/C}) \;\approx\; \min\{d_E^2(\overline{\Gamma_{C^\star}}), 2^4 d_H(\mathcal{C}_3)\} \tag{79}$$

Due to the balancing condition considered, i.e., $d_E^2(\overline{\Gamma_{C^\star}}) = 2^4 d_H(\mathcal{C}_3)$. Thus, Equation (79) reduces to:

$$d_E^2(\Gamma_{C^\star/C}) \;\approx\; \min\{nq[1+4(1-q)], 2^4 n q_3\} \tag{80}$$

where it follows that $q_3 = q[1+4(1-q)]/16$ (or also $d_H(\mathcal{C}_3) = \frac{5}{32}d_H(\mathcal{C})$, for large n).

We can then estimate the packing efficiency of hybrid Construction $C^\star/C$ and compare it with that of Construction C. Remember that for large n, $vol(B(0,\rho)) \approx \frac{2\pi e}{n}^{n/2}\rho^n$ and we also consider GVB codes achieving the equality in Equation (73) in order to have a fair comparison, then we have:

$$\chi(\Gamma_{C^\star/C}) \approx \frac{\sqrt{q[1+4(1-q)]}(2\pi e)^{1/2}}{2\cdot 2^{LH(q)}\cdot 2^{H(q_3)}\cdot\ldots\cdot 2^{H(q_3/2^{2(L-1)})}}, \tag{81}$$

where $\chi(\Lambda) = (\Delta(\Lambda))^{1/n}$ and the balancing gives $q_3 = q[1+4(1-q)]$. For Construction C, with $\mathcal{C}_1, \ldots, \mathcal{C}_L$ codes and a balanced distance such that the Hamming distance $d_H(\mathcal{C}_i)$ is 4 times smaller than $d_H(\mathcal{C}_{i-1})$ for $i = 2, \ldots, L$, if we define $q_1 = d_H(\mathcal{C}_1)/n$, it follows that

$$\chi(\Gamma_C) = \frac{\sqrt{q_1 \pi e}}{\sqrt{2} \cdot 2^{H(q_1)} \cdot \ldots \cdot 2^{H(q_1/2^{2(L-1)})}}. \tag{82}$$

We would like to remark that this approach was already done [17].

To compare both performances, Figure 6 illustrates the packing estimated efficiency as a function of the information rate (R) of the hybrid Construction $C^\star/C$ compared with that of Construction C for GVB achieving codes.

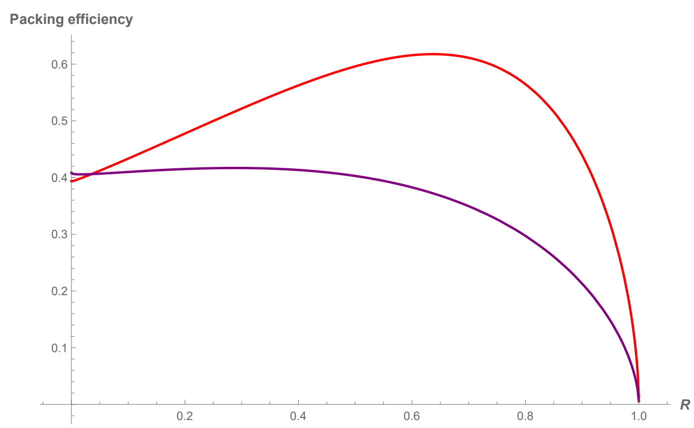

Fig. 6. Packing efficiency *versus* information rate – Hybrid $C^\star/C$ (red) and C (purple).

Remark 6. *The performance represented in Figure 6 is overestimated, because we considered the minimum average squared distance $d_E^2(\overline{\Gamma_{C^\star}})$, which is easier to obtain, instead of the average minimum squared distance $\overline{d_E^2(\Gamma_{C^\star})}$. This is clear because it is widely believed that for large n it is not feasible to have a packing efficiency greater than 0.5 (the packing efficiency guaranteed by the Minkowski bound [6, pp.247]). Thus our estimation must be loose. However, Figure 6 should therefore be viewed as a good indication for the potential superiority of Costruction $C^\star$.*

IX. Conclusion

Our contributions in this paper were: a detailed investigation about the geometric uniformity of Construction C, including the definition of general geometrically uniform constellations; the introduction of a new method of constructing constellations, denoted by Construction $C^\star$, which is a subset of Construction C and is based on a modern coding scheme, the bit-interleaved coded modulation (BICM); and the discussion of properties of Construction $C^\star$, where we could examine on a comparative basis a hybrid Construction $C^\star/C$ with Construction C in terms of packing efficiency.

Future work includes changing the natural labeling μ to the Gray map, the standard map used in BICM, and developing a decoding method for Construction $C^\star$, which takes advantage of the structure of the main code $\mathcal{C} \subseteq \mathbb{F}_2^{nL}$.

ACKNOWLEDGMENT

CNPq (140797/2017-3, 312926/2013-8) and FAPESP (2013/25977-7) supported the work of Maiara F. Bollauf and Sueli I. R. Costa. Ram Zamir was supported by Israel Science Foundation (676/15).

REFERENCES

[1] E. Agrell and T. Eriksson, *Optimization of Lattice for Quantization*. IEEE Transactions on Information Theory 44(5), 1814-1828, 1998.

[2] O. Amrani, Y. Beery, A. Vardy, F.-W. Sun, and H. C. A. van Tilborg, *The Leech Lattice and the Golay Code: Bounded-Distance Decoding and Mu1tilevel Constructions*. IEEE Transactions on Information Theory 40(4), 1030-1043. 1994.

[3] M. F. Bollauf and R. Zamir, *Uniformity properties of Construction C*. 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, pp. 1516-1520, 2016.

[4] M. F. Bollauf, R. Zamir and Sueli I. R. Costa, *Construction $C^\star$: an inter-level coded version of Construction C*. 2018 International Zurich Seminar on Information and Communication, Zurich, pp. 118-122, 2018.

[5] H. Cohn, A. Kumar, S. Miller, D. Radchenko, and M. Viazovska, *The sphere packing problem in dimension 24*. Ann. of Math., vol. 185, pp. 10171033, 2017.

[6] J. H. Conway and N.J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, USA: Springer-Verlag, 1998.

[7] R. de Buda, *Fast FSK signals and their demodulation*. Can. Electron. Eng. Journal, 1, pp. 2834, 1972.

[8] R. de Buda, *Coherent demodulation of frequency-shift keying with low deviation ratio*. IEEE Trans. Commun., COM-20, pp. 429435, 1972.

[9] G. D. Forney, *Coset codes-part I: introduction and geometrical classification*. IEEE Transactions on Information Theory 34(5), 1123-1151, 1988.

[10] G. D. Forney, *Coset codes-part II: binary lattices and related codes*. IEEE Transactions on Information Theory 34(5), 1152-1187, 1988.

[11] G. D. Forney, *Geometrically uniform codes*. IEEE Transactions on Information Theory 37(5), 1241-1260, 1991.

[12] G. D. Forney, M. D. Trott and S. Chung, *Sphere-Bound-Achieving Coset Codes and Multilevel Coset Codes*. IEEE Transactions on Information Theory 46(3), 820-850, 2000.

[13] W. Kositwattanarerk and F. Oggier, *Connections between Construction D and related constructions of lattices*. Designs, Codes and Cryptography, v.73, 441-455. Norwell, USA: Kluwer Academic Publishers, 2014.

[14] B. Nazer and M. Gastpar. *Compute-and-Forward: Harnessing Interference Through Structured Codes*. IEEE Transactions on Information Theory 57(10), 6463 - 6486, 2011.

[15] S. S. Pradhan and K. Ramchandran, *Distributed source coding using syndromes (discus): design and construction*. Proc. IEEE Data Compression Conference, Snowbird, UT, 1999.

[16] L. Szczecinski and A. Alvarado, *Bit-interleaved coded modulation : fundamentals, analysis, and design*. John Wiley & Sons, 2015.

[17] U. Erez and O. Ordentlich (private communications, 2018).

[18] R. Zamir, S. Shamai, and U. Erez. *Nested linear/lattice codes for structured multiterminal binning.* IEEE Transactions on Information Theory 48, 12501276, 2002.

[19] E. Zehavi, *8-PSK trellis codes for a Rayleigh channel*. IEEE Trans. Commun., 40 (3), pp. 873884, 1992.