

On lattice constructions D and D' from q -ary linear codes

Franciele do Carmo Silva, Ana Paula de Souza, Eleonesio Strey and Sueli Irene Rodrigues Costa

Abstract. Multilevel lattice codes, such as those associated with Constructions C , \bar{D} , D and D' , have relevant applications in communications. In this paper, we investigate some properties of lattices obtained via Constructions D and D' from q -ary linear codes. Connections with Construction A , generator matrices, expressions and bounds for the lattice volume and minimum distances are derived. Extensions of previous results regarding construction and decoding of binary and p -ary linear codes (p prime) are also presented.

1 Introduction

Lattices are discrete additive subgroups of \mathbb{R}^n that have attracted attention, due to several applications in coding for reliable and secure communications. Through their rich algebraic and geometric structures, they can achieve the capacity of the additive white Gaussian channel (AWGN) [20]. Regarding security, lattices have been also used in coding for wiretap channels [17] and currently compose one of the main approaches in the so-called Post-Quantum Cryptography [48].

MSC 2020: 94B05 - 94B35 - 52C99

Keywords: Lattices, Codes over rings, Constructions D and D' , Coding gain, Decoding of Construction D' .

Contact information:

F. C. Silva:

Affiliation: University of Campinas, Brazil.

Email: francielecs@ime.unicamp.br

A. P. Souza:

Affiliation: University of Campinas, Brazil.

Email: anasouza@ime.unicamp.br

E. Strey:

Affiliation: Federal University of Espírito Santo, Brazil.

Email: eleonesio.strey@ufes.br

S. I. R. Costa:

Affiliation: University of Campinas, Brazil.

Email: sueli@ime.unicamp.br

The association of lattices with codes is natural [15], however, lattice code construction with good performance and practical decoding is still a hard problem. In order to reduce the decoding complexity, a possible direction is the construction of multilevel lattices from a family of nested codes, which allows multistage decoding. Similar techniques are also applied in a more general sense, as introduced in [30], to obtain multilevel lattice codes, even when the constructions do not necessarily form a lattice, what include the so-called Constructions \bar{D} [27], C [39], C^* [7], D and D' [38, 10, 4, 15, 27]. These constructions are extensively studied, especially for the binary case, and appear in papers such as [56, 63, 7, 75] and references therein. Recent works deal with generalizations of Constructions D, D' and \bar{D} to linear codes over finite fields [23], codes over the ring \mathbb{Z}_q of integers modulo q [68, 67] and for cyclic codes over finite fields (Construction $D^{(cyc)}$) [29]. It is well-known that some remarkable lattices with higher coding gain can be described via binary code Constructions D and D' , as turbo lattices [59], the Barnes-Wall lattices [15] and LDPC lattices [57]. Several proposals and analyses of multistage decoding have been presented in [63, 57, 76, 40].

Regarding codes over finite rings, a great interest came from the discovery of good nonlinear binary codes connected via the Gray map to linear codes over \mathbb{Z}_4 [11]. This study motivated several works to consider codes over more general finite rings, such as \mathbb{Z}_{2^k} and \mathbb{Z}_{2^k} , and their respective Gray maps [71, 3, 19]. In particular, self-dual codes over \mathbb{Z}_{2^k} have attracted interest because of their connection with even unimodular lattices [8, 19]. Under these motivations, in this paper, we focus on Constructions D, D' and A from nested linear codes over \mathbb{Z}_q . Our objective is to study some general properties of these constructions, such as volume, L_P -minimum distance, with $1 \leq P \leq \infty$, and bounds for coding gain. For this, we establish some relations between Construction D' and A and present bounds for these parameters in terms of their underlying codes or their duals. We also extend a multistage decoding method with re-encoding to Construction D' from q -ary linear codes under specific conditions.

This paper is organized as follows. Concepts and preliminary results are presented in Section 2. In Section 3, it is pointed out some known properties of Constructions D and D' and by the association of Construction D' with Construction A (Corollary 3.14), expressions for a generator matrix (Corollary 3.15 and Corollary 3.20), volume (Corollary 3.16 and Remark 3.18) and minimum distance (Corollary 3.19) of this construction are derived. In Section 4, we obtain a lower and an upper bound, respectively, for the volume of the lattices obtained by Constructions D and D' (Theorem 4.1, 4.5) and discuss specific conditions such that they can be achieved (Theorem 4.4 and Corollaries 4.6 and 4.7). Also, it is characterized by the L_P -minimum distance and coding gain of lattices obtained via these constructions under certain conditions by using the minimum distance of the nested codes or their duals (Theorems 4.11, Corollaries 4.12, 4.20, 4.29). Specific minimum distance bounds for lattices from binary codes are derived (Theorem 4.25). In Section 5, a known multistage decoding method [76] with re-encoding for Construction D' over binary codes is extended to q -ary codes under specific conditions. Concluding remarks are included in Section 6.

2 Preliminaries

This section is devoted to presenting some concepts, notations and results to be used in the next sections. We may quote [15] and [73] as general references.

Our notations follow the convention for vectors in \mathbb{R}^n , as well as n -tuples in \mathbb{Z}_q^n , in bold letters and $\mathbf{0}$ denotes the null vector. The mapping $\rho : \mathbb{Z} \rightarrow \mathbb{Z}_q$ is the natural reduction ring homomorphism and $\sigma : \mathbb{Z}_q \rightarrow \mathbb{Z}$ is the standard inclusion map, extended to vectors and matrices in a component-wise way. For simplicity, we abuse the notation, using σ and ρ for \mathbb{Z}_q and \mathbb{Z}_q^n and omitting them in the numerical examples. When these maps are associated with \mathbb{Z}_{q^a} or $\mathbb{Z}_{q^a}^n$, with $a > 1$, we will refer to them as σ_{q^a} and ρ_{q^a} , respectively. The order of an element $\mathbf{h} \in \mathbb{Z}_q^n$, denoted by $O(\mathbf{h})$, is defined as the smallest natural m such that $m\mathbf{h} = \mathbf{0}$ in \mathbb{Z}_q^n (i.e., $m\sigma(\mathbf{h}) \equiv \mathbf{0} \pmod{q}$).

A q -ary linear code C of length n over \mathbb{Z}_q is a \mathbb{Z}_q -module of \mathbb{Z}_q^n , that is, an additive subgroup of \mathbb{Z}_q^n . The terminology of q -ary codes is also applied in the study of codes over finite fields \mathbb{F}_q , however, in this work we use q -ary code to refer to a code over \mathbb{Z}_q . The code generated by the n -tuples $\mathbf{b}_1, \dots, \mathbf{b}_k \in \mathbb{Z}_q^n$ is denoted by $C = \langle \mathbf{b}_1, \dots, \mathbf{b}_k \rangle$. We say that a set $\{\mathbf{b}_1, \dots, \mathbf{b}_k\}$ is a basis for C if they are linearly independent over \mathbb{Z}_q and they generate C . In contrast to codes over finite fields, when q is not a prime number there are q -ary linear codes that do not admit a basis. Despite this, every q -ary code C can be characterized by a minimal set of generators, due to its finitely generated module structure [55, 33]. For a code C , two different minimal sets of generators always have the same cardinality [55]. A generator matrix for a q -ary code C is a matrix whose rows constitute a minimal set of generators for C .

The usual inner product of two vectors \mathbf{x} and \mathbf{y} in \mathbb{R}^n is denoted by $\mathbf{x} \cdot \mathbf{y}$. For each pair of n -tuples $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ in \mathbb{Z}_q^n , we define the (Euclidean) semi-inner product between \mathbf{x} and \mathbf{y} as $\mathbf{x} \cdot \mathbf{y} := x_1y_1 + \dots + x_ny_n \in \mathbb{Z}_q$, where x_iy_i denote the usual product over the ring \mathbb{Z}_q for each $i = 1, \dots, n$. When q is not a prime number, this is not an inner product, since there exist nonzero elements whose product is zero. Given a q -ary linear code C , the set $C^\perp := \{\mathbf{x} \in \mathbb{Z}_q^n : \mathbf{x} \cdot \mathbf{y} = \mathbf{0}, \forall \mathbf{y} \in C\}$ is always a linear code over \mathbb{Z}_q , which is called the dual code of C . If C_1 and C_2 are q -ary linear codes such that $C_2 \subseteq C_1$, then $C_1^\perp \subseteq C_2^\perp$.

A lattice $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup of \mathbb{R}^n . Equivalently, $\Lambda \subset \mathbb{R}^n$ is a lattice if, and only if, there exists a set of linearly independent vectors $\mathbf{v}_1, \dots, \mathbf{v}_m \in \mathbb{R}^n$ such that Λ is given by all integer linear combinations of these vectors [13].

Under this description, we call the set $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$ a basis of Λ and the number m , the rank of Λ . When $m = n$, we say that Λ is a full-rank lattice. The matrix \mathbf{M} whose columns are the vectors $\mathbf{v}_1, \dots, \mathbf{v}_m$ is a generator matrix of Λ . Two matrices \mathbf{M}_1 and \mathbf{M}_2 are generator matrices of the same lattice Λ if, and only if, there is a unimodular matrix \mathbf{U} (i.e., a matrix with integer entries and $\det \mathbf{U} = \pm 1$) such that $\mathbf{M}_2 = \mathbf{M}_1 \mathbf{U}$. Given a generator matrix \mathbf{M} for Λ , we define the associated Gram matrix as $\mathbf{G} = \mathbf{M}^T \mathbf{M}$. The volume of Λ is defined as $\text{vol } \Lambda = \sqrt{\det \mathbf{G}}$, where \mathbf{G} is a Gram matrix for Λ . In this paper, we deal only with full-rank lattices ($m = n$) and, in this case, $\text{vol } \Lambda = |\det \mathbf{M}|$, where \mathbf{M} is a generator matrix for Λ . For a full-rank lattice Λ , the dual is defined as

$\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n : \mathbf{y} \cdot \mathbf{x} \in \mathbb{Z}, \forall \mathbf{x} \in \Lambda\}$. It can be shown that \mathbf{M} is a generator matrix for Λ if, and only if, $(\mathbf{M}^T)^{-1}$ is a generator matrix for Λ^* .

Considering a distance d in \mathbb{R}^n , we say that two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^n$ are d -equivalent with respect to a distance d if there exist a number $k \in \mathbb{R}^*$ and an isometry ϕ in \mathbb{R}^n with respect to d such that $\Lambda_2 = k\phi(\Lambda_1)$. Also, the minimum distance of Λ with respect to distance d is defined as $d_d(\Lambda) := \min \{d(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Lambda \text{ and } \mathbf{x} \neq \mathbf{y}\}$. The packing radius $r_{\text{pack},d}$ of a lattice Λ , with respect to a distance d , is half of the minimum distance of Λ relative to this same distance. We consider here the usual L_P -distances in \mathbb{R}^n and in \mathbb{Z}_q^n associated with the L_P -norm. The L_P -distance, with $1 \leq P \leq \infty$, between two elements \mathbf{x} and \mathbf{y} in \mathbb{R}^n is defined as:

$$d_P(\mathbf{x}, \mathbf{y}) := \left(\sum_{i=1}^n |x_i - y_i|^P \right)^{1/P} \quad \text{for } 1 \leq P < \infty \quad \text{and} \quad d_\infty(\mathbf{x}, \mathbf{y}) := \max \{|x_i - y_i| : i = 1, \dots, n\}.$$

Given a lattice $\Lambda \subset \mathbb{R}^n$, the minimum L_P -distance of Λ is defined as

$$d_P(\Lambda) = \min \{d_P(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in \Lambda \text{ and } \mathbf{x} \neq \mathbf{y}\}.$$

The Lee distance, introduced by [37] and [69], is the induced L_1 -distance from \mathbb{Z} in \mathbb{Z}_q and it is defined as $d_{\text{Lee}}(x, y) = \min \{\sigma(x - y), q - \sigma(x - y)\}$ and for two n -tuples $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$ is given by

$$d_{\text{Lee}}(\mathbf{x}, \mathbf{y}) := \sum_{i=1}^n d_{\text{Lee}}(x_i, y_i).$$

In addition, the correspondent induced L_P -distance from \mathbb{Z}^n in \mathbb{Z}_q^n (also called *P-Lee distance*) [34], for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^n$ is given by

$$d_P(\mathbf{x}, \mathbf{y}) := \left(\sum_{i=1}^n d_{\text{Lee}}(x_i, y_i)^P \right)^{1/P} \quad \text{for } 1 \leq P < \infty \quad \text{and} \quad d_\infty(\mathbf{x}, \mathbf{y}) := \max \{d_{\text{Lee}}(x_i, y_i) : i = 1, \dots, n\}.$$

We denote the L_P -norm of a vector $\mathbf{x} \in \mathbb{Z}^n$ as $\|\mathbf{x}\|_P = d_P(\mathbf{x}, \mathbf{0})$ and, similarly, the *P-Lee norm* of $\mathbf{y} \in \mathbb{Z}_q^n$ as $\|\mathbf{y}\|_P = d_P(\mathbf{y}, \mathbf{0})$. The minimum L_P -distance of a linear code $C \subseteq \mathbb{Z}_q^n$ is defined as $d_P(C) := \min \{d_P(\mathbf{x}, \mathbf{y}) : \mathbf{x}, \mathbf{y} \in C \text{ and } \mathbf{x} \neq \mathbf{y}\}$.

For $P = 2$ (Euclidean distance), we use r_{pack,d_2} , $\Delta(\Lambda)$ and $\delta(\Lambda)$ to denote the packing radius, density and center density, respectively. The coding gain and the center density of a full-rank lattice $\Lambda \subset \mathbb{R}^n$ are defined, respectively, as

$$\gamma(\Lambda) := \frac{d_2^2(\Lambda)}{(\text{vol } \Lambda)^{2/n}} \quad \text{and} \quad \delta(\Lambda) := \frac{r_{\text{pack},d_2}^n(\Lambda)}{\text{vol } \Lambda} = 2^{-n} \gamma(\Lambda)^{n/2}.$$

The strong association between lattices in \mathbb{Z}^n and linear codes in \mathbb{Z}_q^n comes from the fact that given a subset $S \subseteq \mathbb{Z}_q^n$, $\rho^{-1}(S)$ is a lattice if, and only if, S is a q -ary linear code [16]. This leads to Construction A definition [15, 73, 16]. Given a linear code $C \subseteq \mathbb{Z}_q^n$, the *Construction A lattice associated with C* , denoted by $\Lambda_A(C)$, is defined as $\Lambda_A(C) = \rho^{-1}(C) = \sigma(C) + q\mathbb{Z}^n$. It is shown in [73] that $\Lambda_A(C)$ is always a full-rank lattice.

3 Construction D and D': general properties

In this section, we present some general properties of Construction D and D'. For this, we first need to establish connections between Constructions D and D' and, subsequently, with Construction A. More details about these connections can be seen in [68, 67].

In the following, the results and definitions cited are adapted versions of [68] using the scaled version of Construction D presented next.

Definition 3.1 (Construction D). Let $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_a$ be a family of nested linear codes such that $C_\ell = \langle \mathbf{b}_1, \dots, \mathbf{b}_{k_\ell} \rangle$ with $\ell = 1, 2, \dots, a$ for a set of n -tuples $\{\mathbf{b}_1, \dots, \mathbf{b}_{k_1}\}$ in \mathbb{Z}_q^n , with integers $k_1 \geq k_2 \geq \dots \geq k_a \geq 0 =: k_{a+1}$. The lattice Λ_D is defined as

$$\Lambda_D = \left\{ q^a \mathbf{z} + \sum_{s=1}^a \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} q^{a-s} \sigma(\mathbf{b}_i) : \mathbf{z} \in \mathbb{Z}^n \text{ and } 0 \leq \alpha_i^{(s)} < q^s \right\}.$$

Equivalently, we can write

$$\Lambda_D = \left\{ q^a \mathbf{z} + \sum_{s=1}^a \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} q^{a-s} \sigma(\mathbf{b}_i) : \mathbf{z} \in \mathbb{Z}^n \text{ and } 0 \leq \alpha_i^{(s)} < O(\mathbf{b}_i) q^{s-1} \right\},$$

where $O(\mathbf{b}_i)$ is the order of \mathbf{b}_i over \mathbb{Z}_q for each $i = 1, \dots, k_1$.

Remark 3.2. The set Λ_D is a full-rank lattice in \mathbb{R}^n [68]. Also, when $a = 1$, the Construction D coincides with the Construction A. If q is prime, each linear code C_ℓ is a vector subspace of \mathbb{Z}_q^n and we can always choose as parameters $k_\ell = \dim C_\ell$ ($\ell = 1, \dots, a$) and n -tuples linearly independent $\mathbf{b}_1, \dots, \mathbf{b}_{k_1} \in \mathbb{Z}_q^n$ such that $C_\ell = \langle \mathbf{b}_1, \dots, \mathbf{b}_{k_\ell} \rangle$. When $q = 2$, the Definition 3.1 restricted to these parameters coincides with the original version of the Construction D presented in [4, 15] without the restriction on the minimum distance.

Remark 3.3. It is important to observe that Construction D depends not only on the nested codes as a whole but also on their generators chosen [68]. As an example, consider the chains of nested linear codes $C_2 \subseteq C_1 \subseteq \mathbb{Z}_5^3$ and $\hat{C}_2 \subseteq \hat{C}_1 \subseteq \mathbb{Z}_5^3$, where $C_2 = \langle (1, 2, 0) \rangle$, $C_1 = \langle (1, 2, 0), (0, 0, 1) \rangle$, $\hat{C}_2 = \langle (3, 1, 0) \rangle$ and $\hat{C}_1 = \langle (3, 1, 0), (0, 0, 1) \rangle$. Note that $C_1 = \hat{C}_1$ and $C_2 = \hat{C}_2$, but the associated Construction D provides different lattices as can be seen from next Theorem 3.7, once it guarantees that this construction can be seen as a Construction A where the generator matrices for the associated codes in \mathbb{Z}_{25}^3 are, respectively,

$$\mathbf{G} = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 0 & 5 \end{bmatrix} \quad \text{and} \quad \hat{\mathbf{G}} = \begin{bmatrix} 3 & 1 & 0 \\ 0 & 0 & 5 \end{bmatrix}.$$

As described in [16], generator matrices for the associated Construction A lattices are obtained by the Hermite Normal Form of matrices which have the code generators for the

two first columns added by the three columns which vectors $(25, 0, 0), (0, 25, 0), (0, 0, 25)$ are the following:

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 25 & 0 \\ 0 & 0 & 5 \end{bmatrix} \quad \text{and} \quad \hat{M} = \begin{bmatrix} 1 & 0 & 0 \\ 17 & 25 & 0 \\ 0 & 0 & 5 \end{bmatrix},$$

That is, M and \hat{M} are generators matrices of the Constructions D lattices Λ_D and $\hat{\Lambda}_D$ obtained from the chains $C_2 \subseteq C_1 \subseteq \mathbb{Z}_5^3$ and $\hat{C}_2 \subseteq \hat{C}_1 \subseteq \mathbb{Z}_5^3$ with the above chosen generators, respectively. Note that $\Lambda_D \neq \hat{\Lambda}_D$ since $U = \hat{M}^{-1}M$ is not unimodular. Moreover, as $d_2(\Lambda_D) = \sqrt{5}, d_2(\hat{\Lambda}_D) = \sqrt{10}$ and $\text{vol } \Lambda_D = 125 = \text{vol } \hat{\Lambda}_D$, we have that center packing densities of these lattices are $\delta(\Lambda_D) \approx 0.011$ and $\delta(\hat{\Lambda}_D) \approx 0.032$, so these lattices are not equivalent. In this case, they have the same volume, but in general, it is not always true. If we consider $\tilde{C}_2 = \langle (3, 1, 0), (4, 3, 0) \rangle$ and $\tilde{C}_1 = \langle (3, 1, 0), (4, 3, 0), (0, 0, 1) \rangle$ over \mathbb{Z}_5 , the chain remains the same with different choice of generators. Now $d_2(\Lambda_D) = \sqrt{5} = d_2(\tilde{\Lambda}_D)$, but $\text{vol } \tilde{\Lambda}_D = 25$.

A more natural construction from nested codes, but which does not always produce a lattice, is the Construction \bar{D} also known as Construction by Code Formula [26].

Definition 3.4 (Construction \bar{D}). Let $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_a$ be a family of nested linear codes, the set $\Gamma_{\bar{D}}$ is defined as follows

$$\Gamma_{\bar{D}} = q^a \mathbb{Z}^n + q^{a-1} \sigma(C_1) + \dots + q^{a-i} \sigma(C_i) + \dots + q^1 \sigma(C_{a-1}) + \sigma(C_a).$$

When $a = 1$, the Construction \bar{D} coincides with the Construction A for linear codes over \mathbb{Z}_q and therefore produces a lattice. The set $\Gamma_{\bar{D}} \subseteq \mathbb{Z}^n$ is not always a lattice, what leads to define $\Lambda_{\bar{D}}$ as the smallest lattice with respect to the natural inclusion. In this sense, $\Gamma_{\bar{D}} \subseteq \Lambda_{\bar{D}}$ and if $\Lambda \supseteq \Gamma_{\bar{D}}$ is a lattice, then $\Lambda_{\bar{D}} \subseteq \Lambda$. An equivalent description of $\Lambda_{\bar{D}}$ can also be found in [68, Thm 8].

The following theorem states a necessary and sufficient condition for the Construction \bar{D} to be a lattice. For this, in [68] it is proposed an operation in \mathbb{Z}_q^n called zero-one addition and denoted by $*$, which is defined for each pair of tuples $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ in \mathbb{Z}_q^n as

$$\mathbf{x} * \mathbf{y} = (x_1 * y_1, \dots, x_n * y_n),$$

where

$$x_i * y_i = \begin{cases} 0, & \text{if } 0 \leq \sigma(x_i) + \sigma(y_i) < q \\ 1, & \text{if } q \leq \sigma(x_i) + \sigma(y_i) \leq 2(q - 1) \end{cases}$$

for each $i \in \{1, \dots, n\}$. When $q = 2$ the zero-one addition coincides with the Schur product [35]. We say that a family of nested linear codes $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_a$ is closed under the zero-one addition if and only if for any $c_1, c_2 \in C_\ell$, then $c_1 * c_2 \in C_{\ell-1}$ for all $\ell = 2, \dots, a$.

Theorem 3.5 ([68, Thm 4.3]). *Given a family of nested linear codes $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_a$, the following statements are equivalent:*

1. $\Gamma_{\bar{D}}$ is a lattice.
2. $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ is closed under the zero-one addition.
3. $\Gamma_{\bar{D}} = \Lambda_D = \Lambda_{\bar{D}}$.

Remark 3.6. An immediate consequence of the previous theorem is that if $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ is closed under the zero-one addition then Construction D is the same as Construction \bar{D} and, therefore, it depends only on the codes C_1, C_2, \dots, C_a (and not on their generators).

The next theorem, proposed in [68], establishes a relation between Constructions D and A. A version of this result for Construction D from a family of linear codes over \mathbb{Z}_p , with p prime, can be also found in [23, Prop 2].

Theorem 3.7 ([68, Thm 3.5]). Let G_1 be a matrix whose rows are the vectors $\sigma(\mathbf{b}_1), \dots, \sigma(\mathbf{b}_{k_1})$ and $C \subseteq \mathbb{Z}_{q^a}^n$ the linear q^a -ary code generated by the rows of the matrix $\rho_{q^a}(\mathbf{G})$, where $\mathbf{G} = \mathbf{D}\mathbf{G}_1$, with \mathbf{D} the diagonal matrix given by

$$d_{jj} = \begin{cases} 1, & \text{for } 1 \leq j \leq k_a; \\ q, & \text{for } k_a < j \leq k_{a-1}; \\ \vdots & \\ q^{a-1}, & \text{for } k_2 < j \leq k_1; \end{cases}$$

Then $\Lambda_D = \Lambda_A(C)$, i.e, Λ_D is a q^a -ary lattice.

The next definition of Construction D' for q -ary linear codes [67, 68] is an extension of the one presented in [4, 15].

Definition 3.8 (Construction D'). Let $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \cdots \supseteq C_a$ be a family of nested linear codes. Given integers r_1, r_2, \dots, r_a satisfying $0 \leq r_1 \leq r_2 \leq \cdots \leq r_a$ and a set $\{\mathbf{h}_1, \dots, \mathbf{h}_{r_a}\}$ in \mathbb{Z}_q^n such that $C_\ell^\perp = \langle \mathbf{h}_1, \dots, \mathbf{h}_{r_\ell} \rangle$ for $\ell = 1, 2, \dots, a$ where C_ℓ^\perp is the dual code of C_ℓ , the set $\Lambda_{D'}$ consists of all vectors $\mathbf{x} \in \mathbb{Z}^n$ such that

$$\mathbf{x} \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{q^{i+1}}$$

for each pair of integers (i, j) satisfying $0 \leq i < a$ and $r_{a-i-1} < j \leq r_{a-i}$, where $r_0 := 0$.

Remark 3.9. The congruence equations in Definition 3.8 can be rewritten via a check matrix denoted by \mathbf{H} , providing an equivalent characterization to Construction D' which is presented in [57, 68, 76]. Indeed, let \mathbf{H}_a be the matrix whose rows are the vectors $\sigma(\mathbf{h}_1), \dots, \sigma(\mathbf{h}_{r_a})$ and C the q^a -ary linear code generated by the rows of $\rho_{q^a}(\mathbf{H})$, where $\mathbf{H} = \mathbf{D}\mathbf{H}_a$, with \mathbf{D} the diagonal matrix defined as in Theorem 3.7, with $k_i = r_{a-i+1}$ for each $i = 1, \dots, a$. Then, $\Lambda_{D'} = \{\mathbf{x} \in \mathbb{Z}^n : \mathbf{H}\mathbf{x} \equiv \mathbf{0} \pmod{q^a}\}$. Throughout this text, we call a matrix \mathbf{H} a check matrix (also known as an a -level matrix) associated to $\Lambda_{D'}$ as in

[57, 63]. We point out that there exists another definition of a check matrix associated with low-density lattice codes, which is presented in [64] and used in [76].

In general, Construction D' depends on the choice of code generators, as can be seen in the example below.

Example 3.10. Consider $\mathbb{Z}_6^2 \supseteq C_1 = \hat{C}_1 \supseteq C_2 = \hat{C}_2$ a family of nested linear codes such that $C_1^\perp = \langle (4, 2) \rangle \subseteq C_2^\perp = \langle (4, 2), (0, 1) \rangle$ and $\hat{C}_1^\perp = \langle (2, 4) \rangle \subseteq \hat{C}_2^\perp = \langle (2, 4), (0, 1) \rangle$. As in Remark 3.9, we have that

$$H = \begin{bmatrix} 4 & 2 \\ 0 & 6 \end{bmatrix} \quad \text{and} \quad \hat{H} = \begin{bmatrix} 2 & 4 \\ 0 & 6 \end{bmatrix}$$

are check matrices of $\Lambda_{D'}$ and $\hat{\Lambda}_{D'}$, respectively. Equivalently, we have

$$\Lambda_{D'} = \{(x, y) \in \mathbb{Z}^2 : 4x + 2y \equiv 0 \pmod{36} \text{ and } 6y \equiv 0 \pmod{36}\} \text{ and}$$

$$\hat{\Lambda}_{D'} = \{(x, y) \in \mathbb{Z}^2 : 2x + 4y \equiv 0 \pmod{36} \text{ and } 6y \equiv 0 \pmod{36}\}.$$

Solving each system of equations, we get generator matrices for $\Lambda_{D'}$ and $\hat{\Lambda}_{D'}$, respectively, given by

$$M = \begin{bmatrix} 9 & -3 \\ 0 & 6 \end{bmatrix} \quad \text{and} \quad \hat{M} = \begin{bmatrix} 18 & -12 \\ 0 & 6 \end{bmatrix}.$$

Since $\text{vol } \Lambda_{D'} = |\det M| = 54 \neq 108 = |\det \hat{M}| = \text{vol } \hat{\Lambda}_{D'}$, these lattices are different (and also non equivalents) and then in this case the Construction D' depends on the choice of the generators.

The Construction D' is connected with the Construction D using codes which are dual of the original ones [68].

Definition 3.11. Let $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_a$ be a family of nested linear codes, parameters r_1, r_2, \dots, r_a satisfying $0 \leq r_1 \leq r_2 \leq \dots \leq r_a$ and n -tuples $\mathbf{h}_1, \dots, \mathbf{h}_{r_a}$ in \mathbb{Z}_q^n such that $C_\ell^\perp = \langle \mathbf{h}_1, \dots, \mathbf{h}_{r_\ell} \rangle$ for $\ell = 1, 2, \dots, a$. We define Λ_{D^\perp} as the lattice obtained via Construction D from a family of nested linear codes $C_1^\perp \subseteq C_2^\perp \subseteq \dots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$.

Theorem 3.12 ([67, Thm 1]). *Let $\mathbb{Z}_q^n \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_a$ be a family of nested linear codes. Then, $\Lambda_{D'} = q^a \Lambda_{D^\perp}^*$.*

Remark 3.13. If we consider Λ_{D^\perp} the lattice obtained via Construction D as in Definition 3.11, we have an analogous result of Theorem 3.5 [67, Cor 1]. In other words, if the chain of dual codes is closed under the zero-one addition, then Construction D' does not depend on the choice of the code generators. One can observe that lattices obtained in Example 3.10 are distinct and the chain of dual codes is not closed under the zero-one addition since $(4, 2) * (4, 2) = (1, 0) \notin C_2^\perp$.

For the next result, we connect Construction D' with Construction A and, from this connection, we describe how to obtain a generator matrix for lattice $\Lambda_{D'}$ in the general case, calculate its volume, and show an expression for its minimum distance. From Theorem 3.12, we have that M is a generator matrix of $\Lambda_{D'}$ if and only if $q^a(M^{-1})^T$ is a generator matrix for $\Lambda_{D'}$. By applying Theorem 3.7, we get the following results.

Corollary 3.14. *Let $\Lambda_{D'}$ be the lattice obtained via Construction D' from Definition 3.8. Then, $\Lambda_{D'} = q^a \Lambda_A^*(C)$, where $C \subseteq \mathbb{Z}_{q^a}^n$ is the linear code generated by the rows of matrix $\rho_{q^a}(\mathbf{H})$, with \mathbf{H} as in Remark 3.9.*

Corollary 3.15 (Generator matrix for $\Lambda_{D'}$). *A generator matrix for $\Lambda_{D'}$ is given by*

$$M = q^a (\mathbf{B}^{-1})^T,$$

where \mathbf{B} is the Hermite Normal Form (HNF) of $\begin{bmatrix} \mathbf{H}^T & q^a \mathbf{e}_1 & \dots & q^a \mathbf{e}_n \end{bmatrix}$ and $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is the canonical basis of \mathbb{R}^n .

Proof. From Corollary 3.14, we have that $\Lambda_{D'} = q^a \Lambda_A^*(C)$, where $C \subseteq \mathbb{Z}_{q^a}^n$ is the linear code obtained for the rows of the matrix $\rho_{q^a}(\mathbf{H})$. Since C is a linear code in $\mathbb{Z}_{q^a}^n$, from [16, Prop. 3.3], it follows that $\Lambda_A(C)$ has a generator matrix (in column form) given by the Hermite Normal Form of

$$\begin{bmatrix} \mathbf{H}^T & q^a \mathbf{e}_1 & \dots & q^a \mathbf{e}_n \end{bmatrix}.$$

Denote \mathbf{B} the Hermite Normal Form from the previous matrix. Then, a generator matrix for $\Lambda_A^*(C)$ is $(\mathbf{B}^{-1})^T$ [16]. Finally, since $\Lambda_{D'} = q^a \Lambda_A^*(C)$, we conclude that $q^a (\mathbf{B}^{-1})^T$ is a generator matrix for $\Lambda_{D'}$. \square

Corollary 3.16 (Volume of $\Lambda_{D'}$). *The volume of $\Lambda_{D'}$ is given by*

$$\text{vol } \Lambda_{D'} = |\det M| = |C|,$$

where C is the q^a -ary linear code of Corollary 3.14 and $|C|$ is the cardinality of C . In particular, an upper bound for the volume of $\Lambda_{D'}$ is $\text{vol } \Lambda_{D'} \leq q^{an}$. Furthermore, if the rows of $\rho_{q^a}(\mathbf{H})$ are linearly independent in $\mathbb{Z}_{q^a}^n$, then we have equality.

Proof. For the description of $\Lambda_{D'}$ in Corollary 3.14 and as $\Lambda_{D'}$ is a full-rank lattice in \mathbb{R}^n , we have

$$\text{vol } \Lambda_{D'} = q^{an} \text{vol } \Lambda_A^*(C) = \frac{q^{an}}{\text{vol } \Lambda_A(C)} = \frac{q^{an}}{q^{an}/|C|} = |C|.$$

To finish the proof, it is enough to observe that $\rho_{q^a}(\mathbf{H})$ is a matrix $r_a \times n$ and C is the q^a -ary linear code generated by the rows of this matrix (Remark 3.9), which can be linearly independent or not. \square

Given a linear code $C \subseteq \mathbb{Z}_q^n$, we can see that $\Lambda_A(C^\perp) = q\Lambda_A^*(C)$ [41, 33]. In fact, we have

$$\begin{aligned} x \in \rho^{-1}(C^\perp) &\Leftrightarrow \rho(x) \cdot \mathbf{y} = 0, \forall \mathbf{y} \in C \Leftrightarrow \rho(x) \cdot \rho(\mathbf{h}) = 0, \forall \mathbf{h} \in \rho^{-1}(C) \\ &\Leftrightarrow x \cdot \mathbf{h} = qk, \text{ for some } k \in \mathbb{Z} \Leftrightarrow x \in q\Lambda_A^*(C). \end{aligned}$$

The next theorem is straightforward from Corollary 3.14 replacing $q^a\Lambda_A^*(C)$ by $\Lambda_A(C^\perp)$, and describes $\Lambda_{D'}$ as a Construction A.

Theorem 3.17. *Under the notation of Definition 3.8, we can express the lattice $\Lambda_{D'}$ as*

$$\Lambda_{D'} = \sigma_{q^a}(C^\perp) + q^a\mathbb{Z}^n = \Lambda_A(C^\perp),$$

where $C^\perp = \Lambda_{D'} \cap [0, q^a)^n$ is the dual code q^a -ary with check matrix $\rho_{q^a}(\mathbf{H})$, where \mathbf{H} is as in Remark 3.9.

Remark 3.18. It follows directly from the above theorem and from [16, Prop. 3.2] that $\text{vol } \Lambda_{D'} = q^{an}/|C^\perp|$. It should be noticed that this result is also presented in [63, Eq. 9] for Construction D' from a chain of binary codes.

We can calculate the L_P -distances and volume of the lattice $\Lambda_{D'}$ by using its association with Construction A and results of [16].

Corollary 3.19 (Minimum distance of $\Lambda_{D'}$). *Consider the distance L_P , with $1 \leq P \leq \infty$. Then, the minimum distance of $\Lambda_{D'}$ is*

$$d_P(\Lambda_{D'}) = \min \{d_P(C^\perp), q^a\}.$$

Motivated by the work of [76], we investigate an alternative way to obtain a generator matrix for the lattice $\Lambda_{D'}$. We finish this section with a generator matrix for this lattice without using the Hermite Normal Form, under specific conditions. This result is a direct consequence of Theorem 3.17 and extends, for q -ary linear codes and a larger number of lattices, the Proposition 1, proposed and demonstrated in [76] to binary linear codes, with appropriate notation adjustments.

Corollary 3.20 (Generator matrix for $\Lambda_{D'}$). *Let $C_a \subseteq C_{a-1} \subseteq \dots \subseteq C_1 \subseteq \mathbb{Z}_q^n$ be a family of nested linear codes. Given $r_1, \dots, r_a \in \mathbb{N}$ satisfying $r_0 := 0 \leq r_1 \leq r_2 \leq \dots \leq r_a = n$ and $\{\mathbf{h}_1, \dots, \mathbf{h}_n\} \subseteq \mathbb{Z}_q^n$ such that $C_\ell^\perp = \langle \mathbf{h}_1, \dots, \mathbf{h}_{r_\ell} \rangle$ for $1 \leq \ell \leq a$, where C_ℓ^\perp is the dual of C_ℓ . Consider the lattice obtained via Construction D' from that chain using the above parameters. Let $\mathbf{H} = \mathbf{D}\mathbf{H}_a$ as in the Corollary 3.14. Suppose that $\sigma(\mathbf{h}_1), \dots, \sigma(\mathbf{h}_n)$ are linearly independent. Then, $q^a\mathbf{H}^{-1}$ is a matrix of integer entries if and only if $q^a\mathbf{H}^{-1}$ is a generator matrix of the lattice $\Lambda_{D'}$.*

Proof. (\Rightarrow) Since $r_a = n$ and $\sigma(\mathbf{h}_1), \dots, \sigma(\mathbf{h}_n)$ are linearly independent, we have that \mathbf{D} and \mathbf{H}_a are invertible matrices of order n . Then, $\mathbf{H} = \mathbf{D}\mathbf{H}_a$ is also an invertible matrix of

order n . So,

$$\begin{aligned} x \in \Lambda_{D'} &\Leftrightarrow x \in \mathbb{Z}^n \text{ and } \mathbf{H}x \equiv \mathbf{0} \pmod{q^a} \\ &\Leftrightarrow x \in \mathbb{Z}^n \text{ and } x = q^a \mathbf{H}^{-1} z \text{ for some } z \in \mathbb{Z}^n \\ &\Leftrightarrow x \in \left\{ (q^a \mathbf{H}^{-1}) z : z \in \mathbb{Z}^n \right\}, \end{aligned}$$

since all entries of the matrix $q^a \mathbf{H}^{-1}$ are integers. Therefore, $q^a \mathbf{H}^{-1}$ is a generator matrix for $\Lambda_{D'}$.

(\Leftarrow) The reciprocal is immediate, since $\Lambda_{D'}$ is an integer lattice. \square

Remark 3.21. The condition that the matrix $q^a \mathbf{H}^{-1}$ has integer entries is not always satisfied. Consider $\mathbb{Z}_3^2 \supseteq C_1 \supseteq C_2$ such that $C_1^\perp = \langle (1, 0) \rangle$ and $C_2^\perp = \langle (1, 0), (0, 2) \rangle$. In this example, we have

$$\mathbf{D} = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \quad \text{and} \quad \mathbf{H}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix},$$

but

$$3^2 (\mathbf{D}\mathbf{H}_2)^{-1} = 9 \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix}^{-1} = \begin{bmatrix} 9 & 0 \\ 0 & 3/2 \end{bmatrix}$$

does not have integer entries and, therefore, cannot generate the lattice $\Lambda_{D'}$.

Example 3.22. Let $\mathbb{Z}_6^2 \supseteq C_1 \supseteq C_2$ be a family of nested linear codes such that $C_1 = \langle (1, 2) \rangle$ and $C_2 = \langle (2, 4) \rangle$. Note that $C_1^\perp = \langle (4, 1) \rangle$ and $C_2^\perp = \langle (4, 1), (3, 0) \rangle$. Applying Construction D' , we get

$$\Lambda_{D'} = \left\{ (x, y) \in \mathbb{Z}^2 : 4x + y \equiv 0 \pmod{36} \text{ and } 3x \equiv 0 \pmod{6} \right\}.$$

Since

$$\begin{aligned} \mathbf{D} &= \begin{bmatrix} 1 & 0 \\ 0 & 6 \end{bmatrix} \quad \text{and} \quad \mathbf{H}_2 = \begin{bmatrix} 4 & 1 \\ 3 & 0 \end{bmatrix}, \\ \mathbf{B} := 6^2 (\mathbf{D}\mathbf{H}_2)^{-1} &= 36 \begin{bmatrix} 4 & 1 \\ 18 & 0 \end{bmatrix}^{-1} = 36 \begin{bmatrix} 0 & 1/18 \\ 1 & -2/9 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 36 & -8 \end{bmatrix}, \end{aligned}$$

has integer entries, Corollary 3.20 guarantees that \mathbf{B} is a generator matrix of $\Lambda_{D'}$.

Remark 3.23. Consider the notation of Corollary 3.20, with $r_a = n$ and $\mathbf{h}_1, \dots, \mathbf{h}_n$ linearly independent over \mathbb{Z}_q . Suppose that $\rho_{q^a}(\mathbf{H}_a)$ is a unimodular matrix over \mathbb{Z}_q . Then $q^a \mathbf{H}^{-1}$ is a generator matrix for the lattice $\Lambda_{D'}$ and

$$\text{vol } \Lambda_{D'} = |\det \mathbf{G}| = q^{an} |\det \mathbf{H}^{-1}| = q^{an} |\det \mathbf{H}_a^{-1}| \cdot |\det \mathbf{D}^{-1}| = q^{an} |\det \mathbf{D}^{-1}| = \prod_{i=0}^{a-1} (q^{an-i})^{r_{i+1}-r_i}.$$

We highlight that when $q = 2$ this result corresponds exactly to Proposition 1 of [76]. In [76], the set of vectors $\{\mathbf{h}_1, \dots, \mathbf{h}_{r_a}\}$ is completed in such a way that \mathbf{H}_a is a unimodular matrix.

4 Volume and Minimum Distance of Construction D and D'

In Section 3, we relate Constructions D and D' with Construction A in such a way that the volume and distance of these lattices can be described through this association. Other descriptions of these lattice parameters under special conditions will be presented in this section.

4.1 Volume

The next theorem provides an upper bound for the cardinality of a linear code over \mathbb{Z}_q whose generator matrix can be written as in Theorem 3.7.

Theorem 4.1. *Let $\Lambda_D = \Lambda_A(C)$ be the lattice obtained from Construction D as in Definition 3.1, where C is the q^a -ary code generated by the rows of the matrix $\rho_{q^a}(\mathbf{G})$ as in Theorem 3.7. Then, the cardinality of C satisfies*

$$|C| = |\Lambda_D \cap [0, q^a]^n| \leq \prod_{s=1}^a \left(\prod_{i=k_{s+1}+1}^{k_s} \mathcal{O}(\mathbf{b}_i) q^{s-1} \right) = \frac{q^{\sum_{\ell=1}^a k_\ell}}{\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_i)}} = q^{\sum_{\ell=2}^a k_\ell} \prod_{i=1}^{k_1} \mathcal{O}(\mathbf{b}_i),$$

and, hence, the volume of Construction D satisfies

$$\text{vol } \Lambda_D \geq q^{an - \sum_{\ell=1}^a k_\ell} \left(\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_i)} \right).$$

Furthermore, if $\mathbf{b}_1, \dots, \mathbf{b}_{k_1}$ are linearly independent over \mathbb{Z}_q , then

$$|C| = |\Lambda_D \cap [0, q^a]^n| = q^{\sum_{\ell=1}^a k_\ell} \quad \text{and} \quad \text{vol } \Lambda_D = q^{an - \sum_{\ell=1}^a k_\ell}.$$

Proof. It is enough to prove the first upper bound since the second is a direct consequence of [16, Prop 3.2] and Theorem 3.7. By Definition 3.1,

$$\Lambda_D \cap [0, q^a]^n = \left\{ \sum_{s=1}^a \sum_{i=k_{s+1}+1}^{k_s} \alpha_i^{(s)} q^{a-s} \sigma(\mathbf{b}_i) \pmod{q^a} : 0 \leq \alpha_i^{(s)} < \mathcal{O}(\mathbf{b}_i) q^{s-1} \right\}.$$

In other words, the vectors of Λ_D inside the box $[0, q^a]^n$ are completely determined by the choices of $\alpha_i^{(s)}$, where $k_{s+1} + 1 \leq i \leq k_s$ and $1 \leq s \leq a$. Also, each $\alpha_i^{(s)}$ can be chosen in $\mathcal{O}(\mathbf{b}_i) q^{s-1}$ different ways. Since the choices of $\alpha_i^{(s)}$ are independent, the Fundamental Counting Principle states that

$$|C| = |\Lambda_D \cap [0, q^a]^n| \leq \prod_{s=1}^a \left(\prod_{i=k_{s+1}+1}^{k_s} \mathcal{O}(\mathbf{b}_i) q^{s-1} \right).$$

On the other hand, some calculations provide

$$\begin{aligned} \prod_{s=1}^a \left(\prod_{i=k_{s+1}+1}^{k_s} \mathcal{O}(\mathbf{b}_i) q^{s-1} \right) &= \prod_{s=1}^a (q^{s-1})^{k_s - k_{s+1}} \cdot \prod_{i=1}^{k_1} \mathcal{O}(\mathbf{b}_i) = \frac{\prod_{s=1}^a (q^s)^{k_s - k_{s+1}} \cdot \prod_{i=1}^{k_1} \mathcal{O}(\mathbf{b}_i)}{\prod_{s=1}^a q^{k_s - k_{s+1}}} \\ &= \frac{\prod_{s=1}^a (q^s)^{k_s - k_{s+1}} \cdot \prod_{i=1}^{k_1} \mathcal{O}(\mathbf{b}_i)}{q^{k_1}} = \frac{\prod_{s=1}^a (q^s)^{k_s - k_{s+1}}}{\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_i)}} = \frac{q^{\sum_{\ell=1}^a k_\ell}}{\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_i)}} = q^{\sum_{\ell=2}^a k_\ell} \prod_{i=1}^{k_1} \mathcal{O}(\mathbf{b}_i), \end{aligned}$$

by using that

$$\begin{aligned} \prod_{s=1}^a (q^s)^{k_s - k_{s+1}} &= q^{k_1 - k_2} (q^2)^{k_2 - k_3} (q^3)^{k_3 - k_4} (q^4)^{k_4 - k_5} \dots (q^a)^{k_a - k_{a+1}} \\ &= q^{k_1 + k_2 + k_3 + k_4 + \dots + k_a} = q^{\sum_{\ell=1}^a k_\ell}. \end{aligned}$$

For the case where $\mathbf{b}_1, \dots, \mathbf{b}_{k_1}$ are linearly independent over \mathbb{Z}_q , we have $\mathcal{O}(\mathbf{b}_i) = q$ for every $i = 1, \dots, k_1$. From this hypothesis, we also have that different choices of $\alpha_i^{(s)}$ yields n -tuples that are necessarily distinct inside the box $\Lambda_D \cap [0, q^a]^n$. This proves the expression obtained for $|C|$. For the volume of Λ_D , it is enough to apply Theorem 3.7 and [16, Prop 3.2] \square

The particular case of Theorem 4.1, where the generators are linearly independent over \mathbb{Z}_q , is stated in [68, Thm 3.4] for q -ary codes and in [4, 15], for binary codes (Theorem 1 and Theorem 13, respectively).

Remark 4.2. Under the notation used, if $C_1 = \langle \mathbf{b}_1, \dots, \mathbf{b}_{k_1} \rangle$ and $\hat{C}_1 = \langle \hat{\mathbf{b}}_1, \dots, \hat{\mathbf{b}}_{k_1} \rangle$ are both generated by k_1 linearly independent n -tuples over \mathbb{Z}_q , then both associated Construction D lattices will have the same volume. The following example illustrates this fact in a case where the lattices are not equivalent.

Example 4.3. Consider $C_2 \subseteq C_1 \subseteq \mathbb{Z}_6^2$ and $\hat{C}_2 \subseteq \hat{C}_1 \subseteq \mathbb{Z}_6^2$, where $C_2 = \langle (1, 5) \rangle$, $C_1 = \langle (1, 5), (4, 1) \rangle = \hat{C}_1$ and $\hat{C}_2 = \langle (4, 1) \rangle$. Let us denote Λ_D and $\hat{\Lambda}_D$, respectively, as the lattices obtained from these chains. From Theorem 3.7, we have $\Lambda_D = \Lambda_A(C)$ and $\hat{\Lambda}_D = \Lambda_A(\hat{C})$, where C and \hat{C} are the 6²-ary linear codes generated, respectively, by the rows of the matrices

$$G = \begin{bmatrix} 1 & 5 \\ 24 & 6 \end{bmatrix} \quad \text{and} \quad \hat{G} = \begin{bmatrix} 4 & 1 \\ 6 & 30 \end{bmatrix}.$$

Thus, Λ_D and $\hat{\Lambda}_D$ are generated, respectively, by

$$M = \begin{bmatrix} 1 & 0 \\ 5 & 6 \end{bmatrix} \quad \text{and} \quad \hat{M} = \begin{bmatrix} 2 & 0 \\ 2 & 3 \end{bmatrix}.$$

Therefore, $\text{vol } \Lambda_D = \text{vol } \hat{\Lambda}_D = 6$, as expected by Theorem 4.1. However, it is easy to see that these lattices are non equivalent since they have the same volume but different minimum (Euclidean) distances.

In the upcoming discussion, we will present a sufficient condition to achieve equality in Theorem 4.1 even for tuples that are not linearly independent. This extends Corollary 3.8 of [68].

Theorem 4.4. *Let $\mathbf{b}_1, \dots, \mathbf{b}_{k_1} \in \mathbb{Z}_q^n$ be nonzero n -tuples such that:*

1. $C_\ell = \langle \mathbf{b}_1, \dots, \mathbf{b}_{k_\ell} \rangle$, for each $\ell = 1, 2, \dots, a$.
2. Some row permutation of the matrix \mathbf{M} whose rows are $\mathbf{b}_1, \dots, \mathbf{b}_{k_1}$ forms an “upper triangular” (respectively, “lower triangular”) matrix in the row echelon form.
3. The first nonzero component (respectively, the last component) of each vector $\sigma(\mathbf{b}_i)$, with $i = 1, \dots, k_1$, divides q as well as all the other components of this vector.

Let Λ_D be the lattice obtained from the chain $C_a \subseteq \dots \subseteq C_1 \subseteq \mathbb{Z}_q^n$ via Construction D under this choice of parameters. Then, if $k_1 = n$, it holds

$$|\mathbf{C}| = |\Lambda_D \cap [0, q^n]^n| = \frac{q^{\sum_{\ell=1}^a k_\ell}}{\prod_{i=1}^n \frac{q}{\mathcal{O}(\mathbf{b}_i)}}.$$

Proof. Let us assume without loss of generality that \mathbf{M} is an upper triangular matrix. By the proof of [68, Thm 3.6], denoting α_j as the first nonzero component of $\sigma(\mathbf{b}_j)$, we know that

$$\text{vol } \Lambda_D = q^{n-k_1} \left(\prod_{j=1}^{k_1} \alpha_j \right) \prod_{s=1}^a (q^{a-s})^{k_s - k_{s+1}} = q^{(a-1)k_1} \left(\prod_{j=1}^{k_1} \alpha_j \right) q^{n - \sum_{\ell=1}^a k_\ell}.$$

Moreover, we have $\mathcal{O}(\mathbf{b}_j) = q/\alpha_j$ for all $j = 1, 2, \dots, k_1$. In fact, the third condition assures the existence of integers m_1, \dots, m_i such that $\sigma(\mathbf{b}_j) = (0, \dots, 0, \alpha_j, m_1\alpha_j, \dots, m_i\alpha_j)$ and, therefore,

$$\frac{q}{\alpha_j} \sigma(\mathbf{b}_j) = \frac{q}{\alpha_j} (0, \dots, 0, \alpha_j, m_1\alpha_j, \dots, m_i\alpha_j) = (0, \dots, 0, q, m_1q, \dots, m_iq) \in q\mathbb{Z}^n.$$

Thus, it follows that $(q/\alpha_j)\mathbf{b}_j = \mathbf{0}$ in \mathbb{Z}_q^n , from where $\mathcal{O}(\mathbf{b}_j) \leq q/\alpha_j$. Since the other inequality is trivial, we conclude that $\mathcal{O}(\mathbf{b}_j) = q/\alpha_j$ for all $j = 1, \dots, k_1$. Finally, considering $\Lambda_D = \Lambda_A(\mathbf{C})$ as in Theorem 3.7, we obtain ([16, Prop 3.2])

$$|\mathbf{C}| = |\Lambda_D \cap [0, q^n]^n| = \frac{q^{an}}{q^{(a-1)k_1} \left(\prod_{j=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_j)} \right) \left(q^{n - \sum_{\ell=1}^a k_\ell} \right)} = \frac{q^{\sum_{\ell=1}^a k_\ell}}{\prod_{j=1}^n \frac{q}{\mathcal{O}(\mathbf{b}_j)}},$$

where the second equality occurs since $k_1 = n$. □

Through connections between Constructions D and D' (Theorem 3.12), the previous results on Construction D are adapted next to Construction D'. We note that Corollary 4.6 is also presented in [4, 15, 57] for the binary case and in [10, Thm 2], which deals with an extension of Construction D, called Construction E, over p -ary codes (p prime). Furthermore, an equivalent expression to the one presented in Corollary 4.7 can be also found in [66, Thm 3.2.8].

Theorem 4.5. Consider $C_1^\perp \subseteq \dots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$ a family of linear codes. Let $\Lambda_{D^\perp} = \Lambda_A(C)$ be as in Definition 3.11, where C is the q^a -ary code generated by the rows of the matrix $\rho_{q^a}(\mathbf{G})$ as in Theorem 4.4 for this chain of dual codes. Let $\Lambda_{D'}$ be the associated lattice obtained via Construction D'. Then, the cardinality of C and volume of $\Lambda_{D'}$ satisfy

$$\text{vol } \Lambda_{D'} = |C| = |\Lambda_{D^\perp} \cap [0, q^a)^n| \leq \prod_{s=1}^a \left(\prod_{i=r_{a-s}+1}^{r_{a-s+1}} \mathcal{O}(\mathbf{h}_i) q^{s-1} \right) = \frac{q^{\sum_{\ell=1}^a r_\ell}}{\prod_{i=1}^{r_a} \frac{q}{\mathcal{O}(\mathbf{h}_i)}}.$$

In particular, if $q = p$ is prime, this upper bound is equivalent to $p^{\sum_{\ell=1}^a r_\ell}$.

Proof. Theorem 3.12 guarantees that $\Lambda_{D'} = q^a \Lambda_{D^\perp}^* = q^a \Lambda_A^*(C)$, where C is the q^a -ary linear code generated by the rows of the matrix $\rho_{q^a}(\mathbf{H})$, as in Remark 3.9. So, by Corollary 3.16, we have $\text{vol } \Lambda_{D'} = |C|$ and the result follows since the upper bound is analogous to the one presented in Theorem 4.1 under appropriate adjustments of notation. \square

Corollary 4.6. Following the notation above, if $\mathbf{h}_1, \dots, \mathbf{h}_{r_a}$ are linearly independent over \mathbb{Z}_q , then

$$\text{vol } \Lambda_{D'} = |C| = |\Lambda_{D^\perp} \cap [0, q^a)^n| = q^{\sum_{\ell=1}^a r_\ell}.$$

Corollary 4.7. Under the conditions of Theorem 4.4 applied to the dual chain [67, Thm 2] and if $r_a = n$, we have

$$\text{vol } \Lambda_{D'} = |C| = |\Lambda_{D^\perp} \cap [0, q^a)^n| = \frac{q^{\sum_{\ell=1}^a r_\ell}}{\prod_{i=1}^n \frac{q}{\mathcal{O}(\mathbf{h}_i)}}.$$

Remark 4.8. Although the upper bounds presented in this section involve the order of each code generator, we must emphasize that just these orders are not enough to determine the volume of the lattice. For instance, the generators taken in Example 3.10 have the same order in \mathbb{Z}_6^2 and provide lattices with different volumes.

4.2 Minimum Distance

In this subsection, we explore, under specific conditions, the minimum L_p -distance of lattices from Constructions D and D' by using the minimum distance of the nested

codes or their duals. The results presented here extend to lattices constructed from codes over \mathbb{Z}_q and to L_P -distance results from [57], which deals with the squared Euclidean minimum distance of lattices from binary codes, and from [66], regarding L_1 -distance of lattices obtained from q -ary codes.

Besides the Euclidean distance ($P = 2$), other L_P -distances have been considered either theoretically, such as the search for perfect and quasi-perfect codes under P -Lee distance [12, 74, 51, 72], or for applications in Cryptography and communications. Several works in lattice-based cryptography, for instance, analyze the complexity of certain computational problems related to lattices in the L_P -norms, such as the closed and the shortest vector problems (CVP and SVP) [47] and the bounded decoding distance (BDD) [5]. Under a cryptography perspective and aiming at possible applications to error-detection in lattice-based communications, in [14] it has been proposed the study of a computational problem called local testability for membership in lattices, for L_P -distances. It should be noted that, in order to obtain nearly matching bounds on the complexity, the authors of [14] focus on families of lattices constructed by Code Formula from a chain of binary Reed-Muller codes closed under the Schur product.

Particularly, the use of L_1 and L_∞ -distances plays a role in communications. As mentioned in [21], the Lee-distance had been considered for BCH codes over fields used in constrained and partial-response channels in [54], for generalized Reed-Muller codes over \mathbb{Z}_{2^r} , with $r \in \mathbb{N}$, applied to orthogonal frequency-division multiplexing in [60], for general linear codes over \mathbb{Z}_p , with p prime, in coding for multidimensional burst-error-correction [22] and also for error-correction in the rank modulation scheme for flash memories [32]. Regarding the L_∞ -distance, in [61] it is shown that sphere decoding under these distance provides a much smaller computational complexity with a marginal performance loss for independent and identically distributed (i.i.d) Rayleigh fading multiple-input multiple-output (MIMO) channels.

We establish a formula for the minimum L_P -distance of Construction \overline{D} , from which we can derive a result for Construction D. This formula will be presented in what follows after the statement of some auxiliary results.

Lemma 4.9. *Let $C \subseteq \mathbb{Z}_q^n$ be a nonzero linear code. Then, for any $1 \leq P \leq \infty$, we can assert that there exists $\mathbf{x}, \mathbf{y} \in C$ such that*

$$\|\sigma(\mathbf{x}) - \sigma(\mathbf{y})\|_P = d_P(C).$$

Proof. The proof is straightforward from the fact that the L_P -norm in \mathbb{Z}_q^n is induced by the L_P -norm in \mathbb{Z}^n for any $1 \leq P \leq \infty$ [34, Prop 2]. \square

Lemma 4.10. *Let $\mathbf{z} = (z_1, z_2, \dots, z_n)$ and $\mathbf{r} = (r_1, r_2, \dots, r_n)$ be vectors of \mathbb{Z}^n such that $0 \leq r_i < q$ for all $i \in \{1, \dots, n\}$. Then $\|q\mathbf{z} + \mathbf{r}\|_P \geq \|\boldsymbol{\mu}\|_P$, where $\boldsymbol{\mu} := (\mu_1, \dots, \mu_n)$ and $\mu_i := \min\{q - r_i, r_i\}$ for all $i \in \{1, \dots, n\}$.*

Proof. Since the largest negative integer of the form $qz_i + r_i$ is $-q + r_i$ and the smallest

positive integer is r_i , it follows that $|qz_i + r_i| \geq \min\{|-q + r_i|, |r_i|\} = \min\{r_i, q - r_i\}$. Then

$$\|qz + r\|_P = \left(\sum_{i=1}^n |qz_i + r_i|^P \right)^{1/P} \geq \left(\sum_{i=1}^n \min\{r_i, q - r_i\}^P \right)^{1/P} = \|\mu\|_P.$$

□

The next result provides a formula for L_P -distances of Construction \overline{D} . When $P = 1$, the Theorem 4.11 was proved in [67, Thm 3] and when $P = 2$, for a chain of binary codes, in [57, Thm 3].

Theorem 4.11. *Let $\{0\} \subsetneq C_a \subseteq C_{a-1} \subseteq \dots \subseteq C_1 \subseteq \mathbb{Z}_q^n$ be a family of nested linear codes. Consider the L_P -distance, with $1 \leq P \leq \infty$, and denote the minimum L_P -distance of C_ℓ by $d_P(C_\ell)$. Then, the minimum L_P -distance of $\Gamma_{\overline{D}}$ in \mathbb{R}^n satisfies*

$$d_P(\Gamma_{\overline{D}}) = \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}.$$

Proof. We use arguments such as the ones in [68, Thm 3]. For each $1 \leq \ell \leq a$, by Lemma 4.9 that there exist $x_\ell, \mathbf{y}_\ell \in C_\ell$ such that $\|\sigma(x_\ell) - \sigma(\mathbf{y}_\ell)\|_P = d_P(C_\ell)$. Fix $1 \leq \ell \leq a$. Since $q^{a-\ell} \sigma(C_\ell) \subseteq \Gamma_{\overline{D}}$, it follows that $q^{a-\ell} \sigma(x_\ell), q^{a-\ell} \sigma(\mathbf{y}_\ell) \in \Gamma_{\overline{D}}$. One the one hand, we have

$$\|q^{a-\ell} \sigma(x_\ell) - q^{a-\ell} \sigma(\mathbf{y}_\ell)\|_P = q^{a-\ell} \|\sigma(x_\ell) - \sigma(\mathbf{y}_\ell)\|_P = q^{a-\ell} d_P(C_\ell).$$

On the other hand, $q^a \mathbb{Z}^n \subseteq \Gamma_{\overline{D}}$ so that $d_P(\Gamma_{\overline{D}}) \leq q^a$, what proves that

$$d_P(\Gamma_{\overline{D}}) \leq \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}.$$

For the other inequality, let $\mathbf{x}, \mathbf{y} \in \Gamma_{\overline{D}}$ be distinct elements, with $\mathbf{x} = q^s \mathbf{v}$ and $\mathbf{y} = q^k \mathbf{w}$, where $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^n$ and $\mathbf{v}, \mathbf{w} \not\equiv \mathbf{0} \pmod{q}$. Assume $s \geq k$ without loss of generality.

(i) If $k \geq a$, we have $d_P^P(\mathbf{x}, \mathbf{y}) = d_P^P(q^s \mathbf{v}, q^k \mathbf{w}) = q^{kP} d_P^P(q^{s-k} \mathbf{v}, \mathbf{w}) \geq q^{aP}$ since $\mathbf{0} \neq q^{s-k} \mathbf{v} - \mathbf{w} \in \mathbb{Z}^n$.

(ii) If $0 \leq k \leq a - 1$, then there exist $\mathbf{c}_1 \in C_1, \dots, \mathbf{c}_{a-k} \in C_{a-k}$ and $\mathbf{z} \in \mathbb{Z}^n$ such that

$$\mathbf{y} = q^a \mathbf{z} + q^{a-1} \sigma(\mathbf{c}_1) + \dots + q^k \sigma(\mathbf{c}_{a-k}),$$

which implies

$$\mathbf{w} = q^{a-k} \mathbf{z} + q^{a-1-k} \sigma(\mathbf{c}_1) + \dots + q^0 \sigma(\mathbf{c}_{a-k}).$$

Note that $\mathbf{w} \pmod{q} = q^0 \sigma(\mathbf{c}_{a-k}) \in \sigma(C_{a-k})$. Denote $\overline{\mathbf{w}} := \rho(\mathbf{w})$ and $\overline{\mathbf{v}} := \rho(\mathbf{v})$, where $\rho : \mathbb{Z}^n \rightarrow \mathbb{Z}_q^n$ is the reduction map modulo q . Since $\mathbf{w} \pmod{q} = q^0 \sigma(\mathbf{c}_{a-k})$, we have $\overline{\mathbf{w}} = \mathbf{c}_{a-k} \in C_{a-k}$ and, thus, $q^{s-k} \overline{\mathbf{v}} - \overline{\mathbf{w}} \in C_{a-k}$ by using that $s \geq k$. Moreover, due the fact that $\mathbf{w} \not\equiv \mathbf{0} \pmod{q}$ and $\mathbf{w} \neq \mathbf{v}$, this is a nonzero vector, which guarantees

$$d_P(\mathbf{x}, \mathbf{y}) = d_P(q^s \mathbf{v}, q^k \mathbf{w}) = q^k d_P(q^{s-k} \mathbf{v}, \mathbf{w}) = q^k d_P(q^{s-k} \mathbf{v} - \mathbf{w}, \mathbf{0}) \geq q^k d_P(C_{a-k}),$$

where the last inequality follows from

$$|q^{s-k} v_i - w_i| \geq \min \{ \sigma(q^{s-k} \overline{v}_i - \overline{w}_i), q - \sigma(q^{s-k} \overline{v}_i - \overline{w}_i) \}, \text{ for each } i \in \{1, \dots, n\}.$$

Finally, we conclude that $d_P(\mathbf{x}, \mathbf{y}) \geq \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}$, completing the proof. \square

Corollary 4.12. *Under the hypothesis of Theorem 4.11, if $\Lambda_{\overline{D}}$ is the smallest lattice that contains $\Gamma_{\overline{D}}$, then*

$$d_P(\Lambda_{\overline{D}}) = \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}.$$

Moreover, it holds that $d_P(\Lambda_D) \geq \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}$, with equality if the chain is closed under the zero-one addition. In particular, if $d_P(C_\ell) \geq q^\ell$ for each $1 \leq \ell \leq a$, then $d_P(\Lambda_D) = q^a$.

Proof. Since $\Gamma_{\overline{D}} \subseteq \Lambda_{\overline{D}}$ and by Theorem 4.11, we already have

$$d(\Lambda_{\overline{D}}) \leq d_P(\Gamma_{\overline{D}}) = \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}.$$

Thus, it is sufficient to prove that $d_P(\Lambda_{\overline{D}}) \geq \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}$. Following a similar approach to the proof of Theorem 4.11, let $\mathbf{x}, \mathbf{y} \in \Lambda_{\overline{D}}$ be distinct elements. By the characterization of the elements of $\Lambda_{\overline{D}}$ [68, Thm 3.14], there exist $\mathbf{z}, \mathbf{w} \in \mathbb{Z}^n$ and $\alpha_j^{(i)}, \beta_j^{(i)} \in \{0, 1, \dots, q-1\}$ such that

$$\mathbf{x} = q^a \mathbf{z} + \sum_{i=1}^a q^{a-i} \sum_{c_j \in C_i} \alpha_j^{(i)} \sigma(c_j) \quad \text{and} \quad \mathbf{y} = q^a \mathbf{w} + \sum_{i=1}^a q^{a-i} \sum_{c_j \in C_i} \beta_j^{(i)} \sigma(c_j).$$

So $\rho(\mathbf{x}), \rho(\mathbf{y}) \in C_a$, since

$$\mathbf{x} \equiv \sum_{c_j \in C_a} \alpha_j^{(a)} \sigma(c_j) \pmod{q} \quad \text{and} \quad \mathbf{y} \equiv \sum_{c_j \in C_a} \beta_j^{(a)} \sigma(c_j) \pmod{q}.$$

Therefore,

$$\begin{aligned} \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\} &\leq d_P(C_a) \leq d_P(\rho(\mathbf{x}), \rho(\mathbf{y})) \\ &= \left[\sum_{i=1}^n (\min \{ \sigma(\rho(x_i) - \rho(y_i)), q - \sigma(\rho(x_i) - \rho(y_i)) \})^P \right]^{1/P} \\ &\leq \left(\sum_{i=1}^n |x_i - y_i|^P \right)^{1/P} = d_P(\mathbf{x}, \mathbf{y}), \end{aligned}$$

where the last inequality follows from

$$\min \{ \sigma(\rho(x_i) - \rho(y_i)), q - \sigma(\rho(x_i) - \rho(y_i)) \} \leq |x_i - y_i| \text{ for all } i \in \{1, \dots, n\}$$

as in Theorem 4.11. The arguments are analogous for the L_∞ -distance. This shows that $\min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\} \leq d_P(\Lambda_{\overline{D}})$. The inequality $d_P(\Lambda_D) \geq \min_{1 \leq j \leq a} \{q^a, q^{a-j} d_P(C_j)\}$ follows directly from the fact $\Lambda_D \subseteq \Lambda_{\overline{D}}$ [68, Thm 3.14] and the particular case from Theorem 3.5. \square

The first part of Corollary 4.12, when $P = 1$, corresponds to Conjecture 1 proposed in [67].

Remark 4.13. We can see that in the proof of Theorem 4.11 the condition of the codes being nested (required for Construction \bar{D}) was not used. We could then have considered the more general Construction C for linear codes, which is not approached here, and get an analogous expression. This generalized the result of [15] and [7] regarding the Euclidean minimum distance of Construction C to L_P -distances.

Example 4.14. Considering the family of codes given in Example 4.3, observe that both chains are closed under the zero-one addition, since $C_1 = \hat{C}_1 = \mathbb{Z}_6^2$. Thus, in this case, by Theorem 4.11 the L_P -distance of the codes C_2 and \hat{C}_2 determine completely the L_P -distance of Λ_D and $\hat{\Lambda}_D$, respectively. Specifically, for $P = 2$ (Euclidean minimum distance), we obtain $d_2(\Lambda_D) = \min \{36, 6, 1\} = 1$ and $d_2(\hat{\Lambda}_D) = \min \{36, 6, \sqrt{5}\} = \sqrt{5}$.

Example 4.15. Consider the chain of nested codes $C_2 \subseteq C_1 \subseteq \mathbb{Z}_3^3$, where $C_2 = \langle (1, 1, 1) \rangle$ and $C_1 = \langle (1, 1, 1), (0, 0, 1) \rangle$. Let Λ_D be the lattice obtained from Construction D under the generators above. From Theorem 3.7, $\Lambda_D = \Lambda_A(C)$, where C is the 9-ary code generated by the rows of the matrix

$$G = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 3 \end{bmatrix}$$

Thus, by using Hermite Normal Form [16], we get a generator matrix for Λ_D given by

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 9 & 0 \\ 1 & 0 & 3 \end{bmatrix}.$$

It is straightforward to see that for $P = 2, 1$ and ∞ , the Euclidean, Lee and maximum distance of Λ_D are $d_2(\Lambda_D) = \sqrt{3}$, $d_1(\Lambda_D) = 1$ and $d_\infty(\Lambda_D) = 1$, respectively. On the other hand, the minimum distances of the codes C_1 and C_2 in these distances are $d_2(C_1) = 1$, $d_2(C_2) = \sqrt{3}$, $d_1(C_1) = 1 = d_1(C_2)$ and $d_\infty(C_1) = 1 = d_\infty(C_2)$. So, for $P = 1, 2, \infty$, we can verify that $d_P(\Lambda_D) = \min \{9, 3d_P(C_1), d_P(C_2)\}$. Finally, the chain is closed under the zero-one addition since $(1, 1, 1) * (1, 1, 1) = (0, 0, 0) \in C_2$ and $(2, 2, 2) * (2, 2, 2) = (1, 1, 1) \in C_2$. This illustrates Corollary 4.12 for the L_P -distances, with $P = 1, 2, \infty$.

In order to provide some bounds for L_P -distances of Construction D' for a certain chain of q -ary linear codes, we present an auxiliary result. This is one of the so-called Transference's Theorems, which relate some properties of a lattice Λ and its dual lattice Λ^* . The following version is a consequence of the First and Second Minkowski's Theorems [62, 45] and can be also viewed as a particular case of Banaszczyk's Theorem for successive minima [2, Thm 2.2].

Theorem 4.16 ([2, 62]). *Let $\Lambda \subset \mathbb{R}^n$ be a full-rank lattice. Then, the minimum Euclidean distances of Λ and Λ^* satisfy $d_2(\Lambda) \cdot d_2(\Lambda^*) \leq n$. Another inequality also satisfied is $d_2(\Lambda) \cdot d_2(\Lambda^*) \leq$*

γ_n , where γ_n is the Hermite's constant in dimension n , that is, $\gamma_n = 4\delta_n^{2/n}$, and δ_n is the maximum center density for lattices in dimension n .

Remark 4.17. It is worth noticing that $\gamma_n \leq n/4 + 1$ for all n , as shown in [45], what means that the bound with Hermite's constant is more restrictive than with n . Unfortunately, the exact value of γ_n is only known for dimensions $1 \leq n \leq 8$ and $n = 24$.

Some well-known inequalities involving the L_P -distances in \mathbb{R}^n allow us to directly derive a consequence from the theorem above.

Corollary 4.18. For a full-rank lattice $\Lambda \subset \mathbb{R}^n$, we have

$$d_P(\Lambda) \cdot d_P(\Lambda^*) \leq \gamma_n \leq \frac{n}{4} + 1 \quad \text{for } 2 < P \leq \infty; \tag{1}$$

$$d_P(\Lambda) \cdot d_P(\Lambda^*) \leq \left(n^{\frac{1}{P}-\frac{1}{2}}\right)^2 \gamma_n \leq \left(n^{\frac{1}{P}-\frac{1}{2}}\right)^2 \left(\frac{n}{4} + 1\right) \quad \text{for } 1 \leq P < 2. \tag{2}$$

Proof. Recall that from the Holder's inequality for L_P -norm [36], if $2 < P < \infty$, then $\|\mathbf{x}\|_P \leq \|\mathbf{x}\|_2 \leq n^{\frac{1}{2}-\frac{1}{P}}\|\mathbf{x}\|_P$, and for $P = \infty$, we have $\|\mathbf{x}\|_\infty \leq \|\mathbf{x}\|_2$. Thus, (1) follows from Theorem 4.16. For $P < 2$, we have $\|\mathbf{x}\|_P \leq n^{\frac{1}{P}-\frac{1}{2}}\|\mathbf{x}\|_2$ and, then (2) holds from Theorem 4.16. \square

Remark 4.19. Banaszczyk's Theorem [2] states that $d_2(\Lambda) \cdot d_2(\Lambda^*) \leq n$ and this result is considered tight up to a constant. Under this approach, in [42] it is presented another bound

$$d_2(\Lambda) \cdot d_2(\Lambda^*) \leq \frac{n}{2\pi} + \frac{3\sqrt{n}}{\pi}.$$

There is a result shown by [43, Thm 9.5] which asserts the existence of a sequence of self-dual lattices that satisfy $d_2(\Lambda) = \Theta(\sqrt{n})$, i.e., bounded below and above by a constant multiple of \sqrt{n} . For such lattices, we have $d_2(\Lambda) \cdot d_2(\Lambda^*) = \Omega(n)$, where $\Omega(n)$ denote a quantity bounded below by a constant multiple of n .

The Corollary 4.18 states an upper bound for the L_P -distance of the dual lattice Λ^* related to the L_P -distance of Λ . Nevertheless, since they are obtained by simply applying inequalities relating to Euclidean minimum distance, they certainly can be improved. In this sense, in [42] it is also proposed an upper bound for the L_1 -distance [42, Thm 3.9], namely

$$d_1(\Lambda) \cdot d_1(\Lambda^*) \leq 0.154264n^2 \left(1 + 2\pi \sqrt{\frac{3}{n}}\right)^2.$$

To establish a result similar to Corollary 4.12 for L_P -distances of Construction D' lattice, we use Corollary 4.18 applied to the chain of dual codes jointly to Theorem 3.12.

Corollary 4.20. Let $C_a \subseteq \dots \subseteq C_1 \subseteq \mathbb{Z}_q^n$ be a family of nested linear codes. Consider $\Lambda_{D'}$ the lattice obtained from Construction D' and a fixed L_P -distance, with $1 \leq P \leq \infty$. Denote by

$d_P(C_\ell^\perp)$ the minimum L_P -distance of C_ℓ^\perp for each $1 \leq \ell \leq a$. Thus,

$$d_P(\Lambda_{D'}) \geq \min_{1 \leq j \leq a} \{1, q^{-j} d_P(C_{a-j+1}^\perp)\},$$

and the equality holds if the chain of dual codes is closed under the zero-one addition. In particular, the L_P -distances of $\Lambda_{D'}$ satisfy

$$\begin{aligned} d_P(\Lambda_{D'}) &\leq \frac{\gamma_n}{\min_{1 \leq j \leq a} \{1, q^{-j} d_P(C_{a-j+1}^\perp)\}} \leq \frac{\frac{n}{4} + 1}{\min_{1 \leq j \leq a} \{1, q^{-j} d_P(C_{a-j+1}^\perp)\}} && \text{for } 2 \leq P \leq \infty \\ d_P(\Lambda_{D'}) &\leq \left(n^{\frac{1}{p} - \frac{1}{2}}\right)^2 \cdot \frac{\gamma_n}{\min_{1 \leq j \leq a} \{1, q^{-j} d_P(C_{a-j+1}^\perp)\}} \leq \frac{\frac{n}{4} + 1}{\min_{1 \leq j \leq a} \{1, q^{-j} d_P(C_{a-j+1}^\perp)\}} && \text{for } 1 < P < 2, \end{aligned}$$

where γ_n is the Hermite's constant in dimension n .

Proof. These bounds are a simple consequence of Corollary 4.12 and Theorem 4.16, since $\Lambda_{D'} = q^a \Lambda_{D'^\perp}$, as proved in Theorem 3.12. The second part follows directly from Corollary 4.18. \square

Corollary 4.21. Under the hypothesis of Corollary 4.20, for $2 \leq P \leq \infty$, if $d_P(C_\ell^\perp) \geq q^\ell$ for each $1 \leq \ell \leq a$, it follows that $d_P(\Lambda_{D'}) = q^{1-a}$ and $d_P(\Lambda_{D'}) \leq \min\{\gamma_n, n\} \cdot q^{a-1}$.

Remark 4.22. Note that the required condition of the corollary above is assumed for binary codes and $P = 2$ in [15, 4].

The next example shows that the conditions of the chain of nested dual codes in Construction D' being closed under the zero-one addition cannot be omitted in Corollary 4.20 in order to attain the equality.

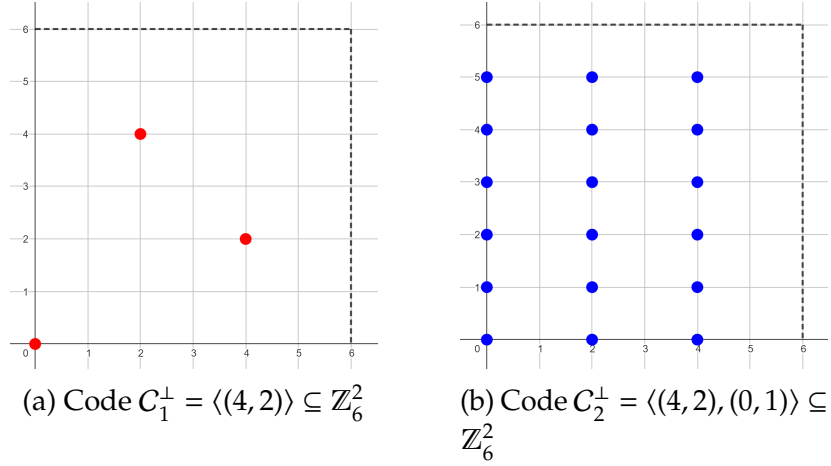
Example 4.23. Let $C_2 \subseteq C_1 \subseteq \mathbb{Z}_6^2$ be the family of nested linear codes, where $C_1^\perp = \langle (4, 2) \rangle$ and $C_2^\perp = \langle (4, 2), (0, 1) \rangle$ (as in Example 3.10). We know that $\Lambda_{D'}$ and $36\Lambda_{D'}^*$ are generated, respectively, by

$$M_1 = \begin{bmatrix} 9 & -3 \\ 0 & 6 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} 4 & 0 \\ 2 & 6 \end{bmatrix}.$$

Let $C \subseteq \mathbb{Z}_{36}^2$ be the linear code such that $36\Lambda_{D'}^* = \Lambda_A(C)$. Thus, the Euclidean minimum distance of $\Lambda_{D'}$ follows by the Euclidean minimum distance for C , namely $d_2(\Lambda_{D'}) = \min\{2\sqrt{5}/36, 36/36\} = \sqrt{5}/18$. On the other hand, we have

$$\min\{1, 6^{-1}d_2(C_2^\perp), 6^{-2}d_2(C_1^\perp)\} = \min\{1, 1/6, 6^{-2}(2\sqrt{2})\} = \sqrt{2}/18 < \sqrt{5}/18.$$

Note that the chain $C_2 \subseteq C_1 \subseteq \mathbb{Z}_6^2$ is not closed under the zero-one addition.


 Figure 1: Dual codes used for Construction D' .

For binary codes, it is also possible to obtain a lower bound for the minimum L_P -distance without restrictions under the chain. These bounds are related to the minimum distance of the original codes and not of their dual codes. We present next some of them, which extend to L_P -distances results previously known for Euclidean distance from binary codes [57, Thm 3.1] and the ones known for L_1 -distance from q -ary linear codes [67, Thm 4].

Lemma 4.24. *Let $\{0\} \subsetneq C_a \subseteq \dots \subseteq C_1 \subsetneq \mathbb{Z}_2^n$ be a family of nested binary linear codes, $0 \leq r_1 \leq \dots \leq r_a$ and $\mathbf{h}_1, \dots, \mathbf{h}_{r_a} \in \mathbb{Z}_2^n$ such that $C_\ell^\perp = \langle \mathbf{h}_1, \dots, \mathbf{h}_{r_a} \rangle$ for each $\ell = 1, \dots, n$. If $\mathbf{x} \in \mathbb{Z}^n$ has at least one odd coordinate and $\mathbf{x} \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{2}$ for $1 \leq j \leq r_k$, then $\|\mathbf{x}\|_P \geq d_P(C_k)$.*

Proof. Let $\mathbf{x} = \mathbf{c} + 2\mathbf{z}$, where $\mathbf{z} \in \mathbb{Z}^n$ and $\mathbf{c} = (c_1, \dots, c_n)$, with $c_i = 0$ or 1 . According to the hypothesis, $\mathbf{c} \neq \mathbf{0}$ and $\mathbf{c} \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{2}$ for $1 \leq j \leq r_k$. Thus, $\rho(\mathbf{c}) \in C_k$ and, consequently, $\|\mathbf{c}\|_P \geq d_P(C_k)$. On the other hand, by taking $\boldsymbol{\mu} = \mathbf{c}$, since $\min\{2 - c_i, c_i\} = c_i$ for all $i = 1, \dots, n$, it follows that $\|\mathbf{x}\|_P \geq \|\mathbf{c}\|_P \geq d_P(C_k)$ by Lemma 4.10. \square

Theorem 4.25. *Let $\{0\} \subsetneq C_a \subseteq \dots \subseteq C_1 \subsetneq \mathbb{Z}_2^n$ be a family of nested binary linear codes, $0 \leq r_1 \leq \dots \leq r_a$ and $\mathbf{h}_1, \dots, \mathbf{h}_{r_a} \in \mathbb{Z}_2^n$ such that $C_\ell^\perp = \langle \mathbf{h}_1, \dots, \mathbf{h}_{r_a} \rangle$ for each $\ell = 1, \dots, n$. Denote by $\Lambda_{D'}$ the lattice obtained via Construction D' using the parameters above and $d_P(C)$ the L_P -distance of C_ℓ for each $\ell = 1, \dots, a$. Then,*

$$\min_{1 \leq j \leq a} \{2^a, 2^{a-j} d_P(C_j)\} \leq d_P(\Lambda_{D'}) \leq 2^a.$$

Proof. Let $\mathbf{x} \in \Lambda_{D'} \setminus \{0\}$. Since \mathbf{x} is a nonzero vector, we can choose an integer $k \geq 0$ such that $2^{-k}\mathbf{x} \in \mathbb{Z}^n$, but $2^{-k-1}\mathbf{x} \notin \mathbb{Z}^n$. If $k < a$, then $2^{-k}\mathbf{x} \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{2}$ for $1 \leq j \leq r_{a-k}$. In

fact, we have

$$\begin{aligned} x \in \Lambda_{D'} &\Leftrightarrow x \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{2^{i+1}} \text{ for all } 0 \leq i \leq a-1 \text{ and } r_{a-i-1} < j \leq r_{a-i} \\ &\Rightarrow x \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{2^{k+1}} \text{ for all } k \leq i \leq a-1 \text{ and } r_{a-i-1} < j \leq r_{a-i} \\ &\Leftrightarrow 2^{-k}x \cdot \sigma(\mathbf{h}_j) \equiv 0 \pmod{2} \text{ for } 1 \leq j \leq r_{a-k}. \end{aligned}$$

Thus, by Lemma 4.24, $\|x\|_P \geq 2^k d_P(C_{a-k})$. In the other case (that is, if $k \geq a$), we have $x = 2^a z$ for some $z \in \mathbb{Z}^n$ and consequently

$$\|x\|_P = \|2^a z\|_P = 2^a \|z\|_P \geq 2^a.$$

Therefore

$$\min_{1 \leq j \leq a} \{2^j, 2^{a-j} d_P(C_j)\} \leq d_P(\Lambda_{D'}).$$

To obtain the upper bound for $d_P(\Lambda_{D'})$, it is sufficient to use that $2^a \mathbb{Z}^n \subseteq \Lambda_{D'}$. \square

The next examples illustrate that both bounds in Theorem 4.25 can be attained.

Example 4.26. Let us consider the family of linear codes given by $C_2 \subseteq C_1 \subseteq \mathbb{Z}_2^4$, where $C_2^\perp = \langle (0, 0, 0, 1), (1, 1, 1, 1) \rangle$ and $C_1^\perp = \langle (1, 1, 1, 1) \rangle$. We use Theorem 4.25 to estimate the Euclidean minimum distance of $\Lambda_{D'}$. Since the Euclidean minimum distance of the codes C_1 and C_2 are $d_2(C_1) = \sqrt{2} = d_2(C_2)$, it follows that $\min\{4, 2d_2(C_1), d_2(C_2)\} = \sqrt{2}$, which implies $\sqrt{2} \leq d_2(\Lambda_{D'}) \leq 4$ by Theorem 4.25. One can show that, in this case, the lower bound is attained. Indeed, by Theorem 3.17 we know that $\Lambda_{D'} = \Lambda_A(C^\perp)$, where C^\perp is the 4-ary linear code whose check matrix is

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

Thus, from Corollary 3.15, we get a generator matrix for $\Lambda_{D'}$ given by

$$M = \begin{bmatrix} 4 & -1 & -1 & -2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix},$$

from where the Euclidean minimum distance of $\Lambda_{D'}$ is $\sqrt{2}$.

Example 4.27. Consider the family of linear codes $C_2 \subseteq C_1 \subseteq \mathbb{Z}_2^4$, where $C_1^\perp = \langle (-1, 0, 1, 0), (0, -1, 0, 1) \rangle$ and $C_2^\perp = \langle (-1, 0, 1, 0), (0, -1, 0, 1), (1, 0, 0, 0), (0, 0, 0, 1) \rangle$. By Theorem 3.17 we have that $\Lambda_{D'} = \Lambda_A(C^\perp)$, where C^\perp is the 4-ary linear code with check matrix

$$H = \begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix}.$$

So, from Corollary 3.15, a generator matrix for $\Lambda_{D'}$ is given by

$$M = \begin{bmatrix} 4 & 0 & -2 & 0 \\ 0 & 4 & 0 & -2 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{bmatrix},$$

from where the Lee minimum distance of $\Lambda_{D'}$ is 4 which is the upper bound of Theorem 4.25.

Remark 4.28. The main difficulty of extending the previous result to L_p -distances for a chain of q -ary linear codes is the Lemma 4.24, which cannot be true under these conditions, unless $P = 1$ or $q = 2$. To the best of our knowledge, it appears that there is no similar result for the general case.

4.3 Coding Gain

As a consequence of the expressions obtained for the minimum Euclidean distance and the volume of the lattices from Constructions D and D' , we derive next bounds for the coding gain under specific conditions. For the binary case of Construction D' and a choice of linearly independent generators, Corollary 4.29-(iii) is related to what is presented in [57, Cor 3.1] with appropriate notation adjustments. The next result follows immediately from the bounds obtained for volume (Theorem 4.1 and Theorem 4.5, respectively) and Euclidean minimum distance (Corollary 4.12 and Corollary 4.20, respectively) of Λ_D and $\Lambda_{D'}$.

Corollary 4.29. *Let Λ_D (respectively, $\Lambda_{D'}$) be the lattice obtained via Construction D (respectively, Construction D') following the usual notation and choice of parameters. For a chain $\{\mathbf{0}\} \neq C_a \subseteq \dots \subseteq C_1 \subseteq \mathbb{Z}_q^n$ (respectively, a associated dual chain $\{\mathbf{0}\} \neq C_1^\perp \subseteq \dots \subseteq C_a^\perp \subseteq \mathbb{Z}_q^n$), we have the following results:*

(i) *Under the conditions of Theorem 4.4 and if $k_1 = n$, we have*

$$\gamma(\Lambda_D) \geq \frac{\min_{1 \leq j \leq a} \{q^{2a}, q^{2(a-j)} d_P^2(C_j)\}}{\left((q^2)^{a - \sum_{\ell=1}^a \frac{k_\ell}{n}} \left(\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_i)} \right)^{2/n} \right)}.$$

(ii) *If the chain is closed under zero-one addition, then*

$$\gamma(\Lambda_D) \leq \frac{\min_{1 \leq j \leq a} \{q^{2a}, q^{2(a-j)} d_P(C_j)\}}{\left((q^2)^{a - \sum_{\ell=1}^a \frac{k_\ell}{n}} \left(\prod_{i=1}^{k_1} \frac{q}{\mathcal{O}(\mathbf{b}_i)} \right)^{2/n} \right)}.$$

In particular, if the conditions of (i) and (ii) are satisfied the equality holds.

(iii) Under the conditions of Theorem 4.4 for the dual chain and if $r_a = n$, we have

$$\gamma(\Lambda_{D'}) \leq \frac{\gamma_n q^{2a} \cdot \left(\prod_{i=1}^{r_a} \frac{q}{\mathcal{O}(\mathbf{h}_i)} \right)^{2/n}}{(q^2)^{\sum_{i=1}^a \frac{r_i}{n}} \min_{1 \leq j \leq a} \{q^{2a}, q^{2(a-j)} d_P(C_j^\perp)\}} \leq \frac{\left(\frac{n}{4} + 1\right) q^{2a} \cdot \left(\prod_{i=1}^{r_a} \frac{q}{\mathcal{O}(\mathbf{h}_i)} \right)^{2/n}}{(q^2)^{\sum_{i=1}^a \frac{r_i}{n}} \min_{1 \leq j \leq a} \{q^{2a}, q^{2(a-j)} d_P(C_j^\perp)\}}.$$

Remark 4.30. The coding gain and the center density of a lattice Λ are related by $\delta(\Lambda) = 2^{-n} \gamma(\Lambda)^{n/2}$, from what similar bounds for the center density with respect to the Euclidean distance are given.

We emphasize that, under the conditions of Corollary 4.29-(i) for Construction D , it is possible to obtain good lattices in low dimensions with respect to packing density. This is the case, for instance, of the constructions of lattices via Construction D from a family of linear codes over \mathbb{Z}_4 equivalent to E_8 , BW_{16} and Λ_{24} , as presented in [66, 68].

Regarding the upper bound given in Corollary 4.29-(ii), it is interesting to note that some chains of generalized linear Reed-Muller over \mathbb{Z}_q , where q is a prime power [6], are closed under the zero-one addition. In order to verify this, let us denote the r -th generalized Reed-Muller code of length 2^m , $RM_{\mathbb{Z}_q}(r, m)$, where $0 \leq r \leq m(p-1)$ and $q = p^s$, with p prime. Using the concept of generalized Boolean functions, $RM_q(m, r)$ is defined as the linear code over \mathbb{Z}_q generated by the set of all monomials of order at most r in m variables. Equivalently, $RM_q(m, r)$ is obtained from all the \mathbb{Z}_q -linear combinations of the rows of the generator matrix for the classical binary Reed-Muller codes [46]. The next result presents a chain of generalized Reed-Muller codes that is closed under the zero-one addition, as well as in the binary case [15, 35].

Theorem 4.31. Under the above notation, the following chain is closed under the zero-one addition

$$RM_{\mathbb{Z}_q}(m, 2^0) \subseteq RM_{\mathbb{Z}_q}(m, 2) \subseteq RM_{\mathbb{Z}_q}(m, 2^2) \subseteq \cdots \subseteq RM_{\mathbb{Z}_q}(m, 2^{\log_2 2^m}) = \mathbb{Z}_q^{2^m}.$$

Proof. In fact, note that the sum of two monomials with a degree at most than r results in a monomial of degree at most $2r$, and the zero-one addition can not increase the order of a monomial. Since in this case r is a power of 2, follows that the previous chain is closed under the zero-one addition. \square

We point out that the class of generalized Reed-Muller codes have good properties for decoding purposes, as shown in [46, 60]. Certain special families of quaternary linear Reed-Muller codes have been attracted attention due to their relation with the associated binary linear Reed-Muller codes obtained from Gray map [9, 50, 49]. Also, it is known that a family of binary Reed-Muller codes allows constructing Barnes-Wall lattices from Construction D [26].

5 Coding and Decoding of Construction D' for certain q -ary codes

Several methods for encoding and multistage decoding for binary Constructions D and D' have been proposed recently, with approaches using re-encoding [40, 76, 70, 75], by computing cosets [63] and by applying a min-sum algorithm at each level of decoding, as proposed in [57, 56, 58]. In this paper, we focus on multistage decoding with re-encoding following the approach proposed by [76]. We extend some results to a class of lattices obtained by Construction D' from nested q -ary linear codes. The original method performs re-encoding via the check matrix in the sense of [76, 64], that is, as an inverse of a generator matrix for the lattice. In what follows, the notation of [75] is applied to our approach.

5.1 Encoding Method B

In [76], two equivalent encoding methods are given, called Encoding Method A and Encoding Method B. The first requires that the check matrix is in the ALT form and can be efficient when the matrix is sparse [75]. The second one requires that the generators are linearly independent over \mathbb{Z}_2 and the check matrix is square. We focus here on Encoding Method B.

Following the established notation and adopting an approach completely analogous to [76], let $\Lambda_{D'}$ be the lattice obtained via Construction D' from a chain of q -ary linear codes $C_a \subseteq \dots \subseteq C_1 \subseteq \mathbb{Z}_q^n =: C_0$ similarly to Definition 3.8, that is,

$$\Lambda_{D'} = \{x \in \mathbb{Z}^n : Hx \equiv \mathbf{0} \pmod{q^a}\},$$

and assume that the linearly independent generators h_1, \dots, h_{r_a} over \mathbb{Z}_q are completed with h_{r_a+1}, \dots, h_n in such a way that H_a is invertible over \mathbb{Z}_q . Only in this section, for simplicity, we consider that r_0 denotes the number of generators for C_0 obtained from the code generators of the underlying codes. Let $x \in \Lambda_{D'}$ be a lattice vector, denote $Hx = q^a \mathbf{b}$, where $\mathbf{b} \in \mathbb{Z}^n$, and write

$$\begin{aligned} b_j &= & z_j & \text{for } 1 \leq j \leq r_1; \\ b_j &= & u_{1j} + qz_j & \text{for } r_1 < j \leq r_2; \\ b_j &= & u_{2j} + qu_{1j} + q^2z_j & \text{for } r_2 < j \leq r_3; \\ &\vdots & & \vdots \vdots \\ b_j &= & u_{(a-2)j} + qu_{(a-3)j} + \dots + q^{a-3}u_{1j} + q^{a-2}z_j & \text{for } r_{a-2} < j \leq r_{a-1}; \\ b_j &= & u_{(a-1)j} + qu_{(a-2)j} + q^2u_{(a-3)j} + \dots + q^{a-2}u_{1j} + q^{a-1}z_j & \text{for } r_{a-1} < j \leq r_a; \\ b_j &= & u_{aj} + qu_{(a-1)j} + q^2u_{(a-2)j} + q^3u_{(a-3)j} + \dots + q^{a-1}u_{1j} + q^az_j & \text{for } r_a < j \leq n, \end{aligned} \tag{3}$$

where $\mathbf{u}_i = (u_{i1}, \dots, u_{i(n-r_i)})^T \in \mathbb{Z}^{(n-r_i)}$, $u_{ij} \in \sigma^*(\mathbb{Z}_q)$ for each $i = 0, \dots, a-1$ and $j = 1, \dots, n$, and $\mathbf{z} \in \mathbb{Z}^n$. Here, $\sigma^*(\mathbb{Z}_q)$ denote a choice of centralized representatives class, i.e.,

$$\begin{aligned} \sigma^*(\mathbb{Z}_q) &:= \left\{ -\frac{q-1}{2}, -\frac{q-3}{2}, \dots, 0, \dots, \frac{q-3}{2}, \frac{q-1}{2} \right\} \text{ if } q \text{ is odd;} \\ \sigma^*(\mathbb{Z}_q) &:= \left\{ -\frac{q}{2}, -\frac{q-2}{2}, \dots, 0, \dots, \frac{q-4}{2}, \frac{q-2}{2} \right\} \text{ if } q \text{ is even.} \end{aligned}$$

Similarly to [76], we consider $\tilde{\mathbf{u}}'_i$ as obtained from $\mathbf{u}_i = (u_{i(r_i+1)}, \dots, u_{in})^T$ with adjunction of zero coordinates. To preserve the adopted notation, the null coordinates will be added at the beginning, as follows

$$\tilde{\mathbf{u}}'_i := \underbrace{(0, \dots, 0)}_{r_i}, u_{i(r_i+1)}, \dots, u_{in})^T \in \mathbb{Z}_q^n.$$

Lemma 5.1. *Let $\mathbf{b} = (b_1, \dots, b_n)^T \in \mathbb{Z}^n$ as in (3). Considering the vectors $\tilde{\mathbf{u}}'_i$ as before, we have*

$$\mathbf{b} = D(q^{-a}\tilde{\mathbf{u}}'_0 + q^{-(a-1)}\tilde{\mathbf{u}}'_1 + q^{-(a-2)}\tilde{\mathbf{u}}'_2 + \dots + q^{-1}\tilde{\mathbf{u}}'_{a-1} + \mathbf{z}),$$

where D is the diagonal matrix presented in Remark 3.9.

Proof. Denote

$$\mathbf{c} := D(q^{-a}\tilde{\mathbf{u}}'_0 + q^{-(a-1)}\tilde{\mathbf{u}}'_1 + q^{-(a-2)}\tilde{\mathbf{u}}'_2 + \dots + q^{-1}\tilde{\mathbf{u}}'_{a-1} + \mathbf{z}) =: D\tilde{\mathbf{c}}.$$

We can write $\tilde{\mathbf{c}} = q^{-a}(0, \dots, 0, u_{0(r_0+1)}, \dots, u_{1(n-r_0)})^T + \dots + q^{-1}(0, \dots, 0, u_{(a-1)(r_{a-1})}, \dots, u_{(a-1)n})^T + (z_1, \dots, z_n)^T$. Now, multiplying each term by the matrix D , we get $D\tilde{\mathbf{c}} = \mathbf{b}$, as described in (3). \square

In a natural extension of the binary case, observe that a vector $\mathbf{x} \in \Lambda_{D'}$ can be written as

$$\mathbf{x} = \mathbf{x}_0 + q\mathbf{x}_1 + \dots + q^a\mathbf{x}_a = \sum_{i=0}^a q^i\mathbf{x}_i, \quad (4)$$

where the components $\mathbf{x}_i \in \mathbb{Z}^n$ depend on $\tilde{\mathbf{u}}'_i$ for $i = 0, \dots, a-1$. Thus, if we denote $H\mathbf{x} = q^a\mathbf{b} =: \tilde{\mathbf{b}}$, it follows

$$\tilde{\mathbf{b}} = D(\tilde{\mathbf{u}}'_0 + q\tilde{\mathbf{u}}'_1 + \dots + q^{a-1}\tilde{\mathbf{u}}'_{a-1} + q^a\mathbf{z}).$$

Under these conditions, since $\tilde{\mathbf{b}} \in q^a\mathbb{Z}^n$ is known, we can calculate the components of \mathbf{x} by using the relations below

$$\begin{aligned} H_a\mathbf{x}_i &= \tilde{\mathbf{u}}'_i \quad \text{for each } i = 0, \dots, a-1, \\ H_a\mathbf{x}_a &= \mathbf{z}. \end{aligned}$$

5.2 Decoding of Construction D'

A natural extension of the decoding approach developed in [76] for Construction D' of a family of q-ary linear codes, under the previous conditions, is described next. We state a generalization to Proposition 2 of [76] for q-ary linear codes, when H_a is invertible over \mathbb{Z}_q and the proof is analogous to the binary case, with the appropriate notation adjustments.

Proposition 5.2. *For Construction D', the lattice component \mathbf{x}_i is congruent modulo q to a codeword $\tilde{\mathbf{x}}_i \in C_i$, for each $i = 0, \dots, a-1$.*

Proof. Denote $\tilde{x}_i := x_i \bmod q$ for each $i = 0, \dots, a - 1$. By the definition of the lattice components, we know that x_i satisfies $\mathbf{H}_a x_i = \tilde{\mathbf{u}}'_i$, where the first r_i components of $\tilde{\mathbf{u}}'_i$ are zero. Thus, it results that $\mathbf{H}_{a,i} \tilde{x}_i \equiv 0 \pmod q$, where $\rho(\mathbf{H}_{a,i})$ is the check matrix of C_i (i.e., corresponds to the first r_i rows of the matrix \mathbf{H}_a). Equivalently, we can write $\sigma(\mathbf{h}_j) \cdot x_i \equiv 0 \pmod q$, i.e., $\mathbf{h}_j \cdot \tilde{x}_i = 0$ in \mathbb{Z}_q^n , for $1 \leq j \leq r_i$. Therefore, by using the definition of C_i by its check matrix, we conclude $\tilde{x}_i \in C_i$. \square

Under these conditions, the decoding algorithm of Construction D' for a chain of q -ary linear codes is essentially the algorithm proposed by [76]. Since the Construction D' was defined for q -ary codes from an arbitrary set of tuples in \mathbb{Z}_q^n , one point that we should be careful about is requiring that $\mathbf{h}_1, \dots, \mathbf{h}_a$ are linearly independent over \mathbb{Z}_q . This hypothesis is crucial for certain stages of the algorithm (specifically, lines 4 and 9) and guarantees that the entries of \mathbf{H}_a are not zero divisors of \mathbb{Z}_q , which in practice would weak the distance spectrum of the codes and inhibit the completion convergence of the decoders [65].

In what follows, a message is a lattice point $x \in \Lambda_{D'}$ and the channel output is $\mathbf{y} = x + \mathbf{w}$, where \mathbf{w} is the noise. Also, $\bar{\mathbf{u}}$ denotes the vector with all coordinates equal to $\lfloor q/2 \rfloor$ (integer part) and $\bmod_q(\mathbf{y}_i + \bar{\mathbf{u}})$ denotes the vector obtained by reducing modulo q . The decoder Dec_i calculates a codeword $\hat{\mathbf{x}}_i$ closest to \mathbf{y}'_i in the q -ary linear code C_i , which is an estimate of \tilde{x}_i .

In a theoretical view, the next theorem provides a necessary condition for the decoders Dec_i to find the closest n -tuple over \mathbb{Z}_q to a received vector \mathbf{y}'_i over an additive white Gaussian noise (AWGN). Similar results are proposed for decoding binary turbo Construction D' lattices [59] and decoding the Leech lattice [25].

Theorem 5.3. *Given an n -uple \mathbf{y}'_i , if there exists a point $\tilde{x}_i \in C_i$ such that $\|\mathbf{y}'_i - \tilde{x}_i\|_2 \leq d_2(\Lambda_A(C_i))/2$, then at each step in the line 8 the algorithm decoders \mathbf{y}'_i to \tilde{x}_i , i.e., $\hat{\mathbf{x}}_i = \tilde{x}_i$. In particular, if the noise \mathbf{w} satisfies*

$$\left\| \bmod_q^* \left(\frac{\mathbf{w}}{q^i} \right) \right\|_2 \leq \frac{1}{2},$$

where \bmod^* denotes the "triangular function", that is, $\bmod_q^*(\mathbf{w}) := |\bmod_q(\mathbf{w} + \bar{\mathbf{u}}) - \bar{\mathbf{u}}|$, then the algorithm decoders \mathbf{y}'_i to \tilde{x}_i .

Proof. Based on the geometric uniformity of lattices, it suffices to consider $x = \mathbf{0}$ and, hence, under the notation of decomposition (4), $x_i = \mathbf{0}$ for each $i = 0, 1, \dots, a$. Let us say that there is an error at step k if $\hat{\mathbf{x}}_k \neq \mathbf{0}$.

Assume that there have been no errors at former steps $0 \leq k < i$. Since $\hat{\mathbf{x}}_k = \mathbf{0}$ for $k = 0, \dots, i - 1$, in the i -th step we have $\mathbf{y}_i = \mathbf{w}/q^i$ and, then,

$$\mathbf{y}'_i = \left| \bmod_q \left(\frac{\mathbf{y}_{i-1}}{q} + \bar{\mathbf{u}} \right) - \bar{\mathbf{u}} \right| = \left| \bmod_q^* \left(\frac{\mathbf{w}}{q^i} + \bar{\mathbf{u}} \right) - \bar{\mathbf{u}} \right| = \bmod_q^* \left(\frac{\mathbf{w}}{q^i} \right).$$

Under the hypothesis $\left\| \text{mod}_q^* \left(\frac{\mathbf{w}}{q^i} \right) \right\|_2 \leq \frac{d_2(C_i)}{2}$, the vector \mathbf{y}'_i is in the sphere packing of $\Lambda_A(C_i)$ and hence no errors occur. It is sufficient to note that $d_2(C_0) \leq \dots \leq d_2(C_a)$ to complete the proof. \square

Algorithm 1: Decoding Construction D' Lattices

Input: finite ring \mathbb{Z}_q , received message with noisy \mathbf{y} , full-rank matrix H_a .

Output: estimated lattice point $\hat{\mathbf{x}} \in \Lambda_{D'}$.

```

1  $\mathbf{y}_0 \leftarrow \mathbf{y}$ ;
2  $\mathbf{y}'_0 \leftarrow \lfloor \text{mod}_q(\mathbf{y}_0 + \bar{\mathbf{u}}) - \bar{\mathbf{u}} \rfloor$ ;
3  $\hat{\mathbf{x}}_0 \leftarrow \text{Dec}_0(\mathbf{y}'_0)$ ;
4  $\hat{\mathbf{u}}'_1 \leftarrow H_a \hat{\mathbf{x}}_0 \text{ mod } q$ , then solve  $H_a \hat{\mathbf{x}}_0 = \sigma(\hat{\mathbf{u}}'_1)$ ;
5 for  $1, 2, \dots, a-1$  do
6    $\mathbf{y}_i \leftarrow (\mathbf{y}_{i-1} - \hat{\mathbf{x}}_{i-1})/q$ ;
7    $\mathbf{y}'_i \leftarrow \lfloor \text{mod}_q(\mathbf{y}_i + \bar{\mathbf{u}}) - \bar{\mathbf{u}} \rfloor$ ;
8    $\hat{\mathbf{x}}_i \leftarrow \text{Dec}_i(\mathbf{y}'_i)$ ;
9    $\hat{\mathbf{u}}'_{i+1} \leftarrow H_a \hat{\mathbf{x}}_i \text{ mod } q$ , then solve  $H_a \hat{\mathbf{x}}_i = \sigma(\hat{\mathbf{u}}'_i)$ 
10 end
11  $\mathbf{y}_a \leftarrow (\mathbf{y}_{a-1} - \hat{\mathbf{x}}_{a-1})/q$ ;
12  $\hat{\mathbf{x}}_a \leftarrow \lfloor \mathbf{y}_a \rfloor$ ;
13  $\hat{\mathbf{x}} \leftarrow \hat{\mathbf{x}}_0 + q\hat{\mathbf{x}}_1 + \dots + q^{a-1}\hat{\mathbf{x}}_{a-1} + q^a\hat{\mathbf{x}}_a$ .
```

Multilevel lattice constructions based on codes have the promise of attain a manageable decoding complexity. On the other hand, it is worth emphasizing that the decoding algorithms for a code C_i in each interaction must be an efficient one. In a practical view, some nearest-neighbor lattice decoding schemes may not be feasible to implement even for p -ary linear codes, where p is prime [63]. Motivated by the construction of lattices with good performance over AWGN channels and a manageable decoding complexity, several works focus on certain families of nested codes for Construction D and D' over a field. Among these, there are designs and decoding processes for lattices based on p -ary linear low-density parity-check (LDPC) codes, which can be decoded by belief propagation (BP) or min-sum algorithms [57], generalized low density (GLD) codes, by BP decoding [18] and turbo codes, by using soft-input soft-output (SISO) and soft-input hard-output (SIHO) decoding algorithms [59].

Although those classes of codes allow generalizations to codes over \mathbb{Z}_q , the ring size, as in \mathbb{Z}_p , with p prime, can affect the decoding complexity. Especially for algorithms based on belief decoding, this leads most works to consider codes over rings that admit a fast Fourier transform, which can provide a reasonable decoding complexity [28]. These classes include nested codes over \mathbb{Z}_{2k} and \mathbb{Z}_{p^r} , with p prime, with good decoding properties, such as LDPC codes [1, 24], turbo codes [52], low-rank parity-check codes (LRPC) [53], BCH, Reed-Solomon [31], generalized Reed-Muller codes [46] over \mathbb{Z}_{2k} , and

Reed-Solomon codes over \mathbb{Z}_{p^r} [44]. It is expected that for families of codes belonging to these classes, Dec_i chosen as the proper mentioned decoder to be applied at each level i in the Decoding Construction D' lattice algorithm above could provide efficient decoding.

6 Conclusion

The volume and L_p -distances of Construction D and D' are investigated here considering generator matrices for these constructions. An upper bound for the volume by using a generator and a check matrix, respectively, is presented. We also provide an expression for L_p -distances of Construction \bar{D} in terms of the minimum distance of underlying codes and derive some bounds for L_p -distances of Construction D and D' , under certain conditions. In addition, it is established bounds for the coding gain and a sufficient condition for achieving it. A multistage decoding method with re-encoding applied to Construction D' from q -ary linear codes under specific conditions is adapted from [76]. Further work in the directions presented here includes the discussion of efficient decoding for Construction D' for q -ary lattices considered in a more general context and possible dependency of the decoding complexity and coding gain on certain lattice parameters, such as the choice of generators.

Acknowledgements

The authors wish to thank the Editors of this Special Issue and the referees for their important comments which have mindfully improved the original manuscript. They also thank Juliana G. F. Souza for very fruitful discussions. This work is partially supported by Brazilian foundations Coordination for the Improvement of Higher Education Personnel (CAPES - Financial Code 001), CNPq (32441/2021-2), FAPESP (2020/09838-0).

References

- [1] M. A. Armand and K. Ng. Decoding LDPC codes over integer residue rings. *IEEE transactions on information theory*, 52(10):4680–4686, 2006.
- [2] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296:625–635, 1993.
- [3] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura. Type II codes, even unimodular lattices, and invariant rings. *IEEE Transactions on Information Theory*, 45(4):1194–1205, 1999.
- [4] E. Barnes and N. Sloane. New lattice packings of spheres. *Canadian Journal of Mathematics*, 35(1):117–130, 1983.
- [5] H. Bennett and C. Peikert. Hardness of Bounded Distance Decoding on Lattices in ℓ_p -norms. In *35th Computational Complexity Conference (CCC 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), 2020.

- [6] M. Bhaintwal and S. K. Wasan. Generalized Reed–Muller codes over \mathbb{Z}_q . *Designs, Codes and Cryptography*, 54(2):149–166, 2010.
- [7] M. F. Bollauf, R. Zamir, and S. I. Costa. Multilevel constructions: coding, packing and geometric uniformity. *IEEE Transactions on Information Theory*, 65(12):7669–7681, 2019.
- [8] A. Bonnecaze, P. Solé, and A. R. Calderbank. Quaternary quadratic residue codes and unimodular lattices. *IEEE Transactions on information theory*, 41(2):366–377, 1995.
- [9] J. Borges, C. Fernández, and K. T. Phelps. Quaternary Reed-Muller codes. *IEEE transactions on information theory*, 51(7):2686–2691, 2005.
- [10] A. Bos, J. Conway, and N. Sloane. Further lattice packings in high dimensions. *Mathematika*, 29(2):171–180, 1982.
- [11] A. Calderbank, A. Hammons Jr, P. V. Kumar, N. Sloane, and P. Solé. The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inf. Theory*, 40(2):301–319, 1994.
- [12] A. Campello, G. C. Jorge, J. E. Strapasson, and S. I. Costa. Perfect codes in the ℓ_p -metric. *European Journal of Combinatorics*, 53:72–85, 2016.
- [13] J. W. S. Cassels. *An introduction to the geometry of numbers*. Springer Science & Business Media, 2012.
- [14] K. Chandrasekaran, M. Cheraghchi, V. Gandikota, and E. Grigorescu. Local testing of lattices. *SIAM Journal on Discrete Mathematics*, 32(2):1265–1295, 2018.
- [15] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*. New York, NY, USA: Springer-Verlag, 1998.
- [16] S. I. Costa, F. Oggier, A. Campello, J.-C. Belfiore, and E. Viterbo. *Lattices applied to coding for reliable and secure communications*. Springer, 2017.
- [17] M. T. Damir, A. Karrila, L. Amoros, O. W. Gnilke, D. Karpuk, and C. Hollanti. Well-rounded lattices: Towards optimal coset codes for gaussian and fading wiretap channels. *IEEE Transactions on Information Theory*, 67(6):3645–3663, 2021.
- [18] N. di Pietro, J. J. Boutros, G. Zémor, and L. Brunel. Integer low-density lattices based on Construction A. In *2012 IEEE Information Theory Workshop*, pages 422–426, 2012.
- [19] S. T. Dougherty and C. Fernández-Córdoba. Codes over \mathbb{Z}_{2^k} , Gray map and self-dual codes. *Adv. Math. Commun*, 5(4):571–588, 2011.
- [20] U. Erez and R. Zamir. Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding. *IEEE Transactions on Information Theory*, 50(10):2293–2314, 2004.
- [21] T. Etzion, A. Vardy, and E. Yaakobi. Coding for the Lee and Manhattan metrics with weighing matrices. *IEEE transactions on information theory*, 59(10):6712–6723, 2013.
- [22] T. Etzion and E. Yaakobi. Error-correction of multidimensional bursts. *IEEE Transactions on Information Theory*, 55(3):961–976, 2009.

- [23] C. Feng, D. Silva, and F. R. Kschischang. Lattice network coding over finite rings. In *2011 12th Canadian Workshop on Information Theory*, pages 78–81. IEEE, 2011.
- [24] M. Ferrari, S. Bellini, and A. Tomasoni. Low-Complexity \mathbb{Z}_4 LDPC Code Design under a Gaussian Approximation. *IEEE Wireless Communications Letters*, 1(6):589–592, 2012.
- [25] G. Forney. A bounded-distance decoding algorithm for the Leech lattice, with generalizations. *IEEE Transactions on Information Theory*, 35(4):906–909, 1989.
- [26] G. D. Forney. Coset codes. I. Introduction and geometrical classification. *IEEE Transactions on Information Theory*, 34(5):1123–1151, 1988.
- [27] G. D. Forney, M. D. Trott, and S.-Y. Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *IEEE Transactions on Information Theory*, 46(3):820–850, 2000.
- [28] A. Goupil, M. Colas, G. Gelle, and D. Declercq. On belief propagation decoding of LDPC codes over groups. In *4th International Symposium on Turbo Codes & Related Topics; 6th International ITG-Conference on Source and Channel Coding*, pages 1–4. VDE, 2006.
- [29] S. Hu and G. Nebe. Strongly perfect lattices sandwiched between Barnes–Wall lattices. *Journal of the London Mathematical Society*, 101(3):1068–1089, 2020.
- [30] H. Imai and S. Hirakawa. A new multilevel coding method using error-correcting codes. *IEEE Transactions on Information Theory*, 23(3):371–377, 1977.
- [31] J. C. Interlando, R. Palazzo, and M. Elia. On the decoding of Reed-Solomon and BCH codes over integer residue rings. *IEEE Transactions on Information Theory*, 43(3):1013–1021, 1997.
- [32] A. Jiang, M. Schwartz, and J. Bruck. Correcting charge-constrained errors in the rank-modulation scheme. *IEEE Transactions on Information Theory*, 56(5):2112–2120, 2010.
- [33] G. C. Jorge. *q-ary and Algebraic Lattices (in Portuguese)*. PhD thesis, Institute of Mathematics, University of Campinas, Brazil, 2012.
- [34] G. C. Jorge, A. Campello, and S. I. Costa. *q-ary lattices in the ℓ_p norm and a generalization of the Lee metric*. In *Proceedings of the International Workshop on Coding and Cryptography, Bergen*, 2013.
- [35] W. Kositwattanarek and F. Oggier. Connections between construction D and related constructions of lattices. *Designs, codes and cryptography*, 73(2):441–455, 2014.
- [36] E. Kreyszig. *Introductory functional analysis with applications*, volume 17. John Wiley & Sons, 1991.
- [37] C. Lee. Some properties of nonbinary error-correcting codes. *IRE Transactions on Information Theory*, 4(2):77–82, 1958.
- [38] J. Leech. Some sphere packings in higher space. *Canadian Journal of Mathematics*, 16:657–682, 1964.
- [39] J. Leech and N. Sloane. Sphere packings and error-correcting codes. *Canadian Journal of Mathematics*, 23(4):718–745, 1971.

- [40] T. Matsumine, B. M. Kurkoski, and H. Ochiai. Construction D lattice decoding and its application to BCH code lattices. In *2018 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2018.
- [41] D. Micciancio and O. Regev. Lattice-based cryptography. *Post-quantum cryptography*, pages 147–191, 2009.
- [42] S. D. Miller and N. Stephens-Davidowitz. Kissing numbers and transference theorems from generalized tail bounds. *SIAM Journal on Discrete Mathematics*, 33(3):1313–1325, 2019.
- [43] J. W. Milnor and D. Husemoller. *Symmetric bilinear forms*, volume 5. Springer, 1973.
- [44] E. Mook and C. Peikert. Lattice (list) decoding near Minkowski’s inequality. *IEEE Transactions on Information Theory*, 68(2):863–870, 2021.
- [45] P. Q. Nguyen. Hermite’s constant and lattice algorithms. In *The LLL Algorithm: Survey and Applications*, pages 19–69. Springer, 2009.
- [46] K. G. Paterson and A. E. Jones. Efficient decoding algorithms for generalized Reed-Muller codes. *IEEE Transactions on Communications*, 48(8):1272–1285, 2000.
- [47] C. Peikert. Limits on the hardness of lattice problems in ℓ_p norms. *computational complexity*, 17:300–351, 2008.
- [48] C. Peikert et al. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016.
- [49] J. Pernas, J. Pujol, and M. Villanueva. Classification of some families of quaternary Reed-Muller codes. *IEEE transactions on information theory*, 57(9):6043–6051, 2011.
- [50] J. Pujol, J. Rifa, and F. I. Solov’eva. Construction of \mathbb{Z}_4 -Linear Reed-Muller Codes. *IEEE transactions on information theory*, 55(1):99–104, 2008.
- [51] C. Qureshi and S. I. Costa. On perfect q -ary codes in the maximum metric. In *2016 Information Theory and Applications Workshop (ITA)*, pages 1–4. IEEE, 2016.
- [52] A. C. Reid, T. A. Gulliver, and D. P. Taylor. Rate-1/2 component codes for nonbinary turbo codes. *IEEE transactions on communications*, 53(9):1417–1422, 2005.
- [53] J. Renner, S. Puchinger, A. Wachter-Zeh, C. Hollanti, and R. Freij-Hollanti. Low-rank parity-check codes over the ring of integers modulo a prime power. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 19–24. IEEE, 2020.
- [54] R. M. Roth and P. H. Siegel. Lee-metric BCH codes and their application to constrained and partial-response channels. *IEEE Transactions on Information Theory*, 40(4):1083–1096, 1994.
- [55] J. J. Rotman. *Advanced modern algebra*, volume 165. American Mathematical Soc., 2015.
- [56] M.-R. Sadeghi. Lattice and construction of high coding. In: *Woungang I, Misra S, Chandra Misra S (eds) Selected topics in information and coding theory. Series on coding theory and cryptology*, 7:41–76, 2010.

- [57] M.-R. Sadeghi, A. H. Banihashemi, and D. Panario. Low-density parity-check lattices: Construction and decoding analysis. *IEEE Transactions on Information Theory*, 52(10):4481–4495, 2006.
- [58] M.-R. Sadeghi and A. Sakzad. On the performance of 1-level LDPC lattices. *IEEE Transactions on Information Theory*, pages 1–5, 2013.
- [59] A. Sakzad, M.-R. Sadeghi, and D. Panario. Construction of turbo lattices. *IEEE Transactions on Information Theory*, pages 14–21, 2010.
- [60] K.-U. Schmidt. Complementary sets, generalized Reed–Muller codes, and power control for OFDM. *IEEE Transactions on Information Theory*, 53(2):808–814, 2007.
- [61] D. Seethaler and H. Bolcskei. Performance and complexity analysis of infinity-norm sphere-decoding. *IEEE transactions on information theory*, 56(3):1085–1105, 2010.
- [62] C. L. Siegel. *Lectures on the Geometry of Numbers*. Springer Science & Business Media, 1989.
- [63] P. R. B. d. Silva et al. Multilevel LDPC lattice codes with efficient encoding and decoding. *IEEE Transactions on Information Theory*, 65:3246–3259, 2020.
- [64] N. Sommer, M. Feder, and O. Shalvi. Shaping methods for low-density lattice codes. In *2009 IEEE Information Theory Workshop*, pages 238–242. IEEE, 2009.
- [65] D. Sridhara and T. E. Fuja. LDPC codes over rings for PSK modulation. *IEEE Transactions on Information Theory*, 51(9):3209–3220, 2005.
- [66] E. Strey. *Construction of lattices from q-ary codes (in Portuguese)*. PhD thesis, Institute of Mathematics, University of Campinas, Brazil, 2017.
- [67] E. Strey and S. I. Costa. Bounds for the ℓ_1 -distance of q-ary lattices obtained via Constructions D , D' and \bar{D} . *Computational and Applied Mathematics*, 37:2413–2427, 2018.
- [68] E. Strey and S. I. R. Costa. Lattices from codes over \mathbb{Z}_q : Generalization of Constructions D , D' and \bar{D} . *Designs, Codes and Cryptography*, 85(1):77–95, 2017.
- [69] W. Ulrich. Non-binary error correction codes. *Bell System Technical Journal*, 36(6):1341–1388, 1957.
- [70] A. Vem, Y.-C. Huang, K. R. Narayanan, and H. D. Pfister. Multilevel lattices based on spatially-coupled LDPC codes with applications. In *2014 IEEE International Symposium on Information Theory*, pages 2336–2340. IEEE, 2014.
- [71] Z. Wan. *Quaternary codes*, volume 8. World Scientific, 1997.
- [72] X. Xu and Y. Zhou. On almost perfect linear lee codes of packing radius 2. *IEEE Transactions on Information Theory*, 2023.
- [73] R. Zamir. *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory*. Cambridge University Press, 2014.

- [74] T. Zhang and G. Ge. Perfect and quasi-perfect codes under the ℓ_p -metric. *IEEE Transactions on Information Theory*, 63(7):4325–4331, 2017.
- [75] F. Zhou, A. Fitri, K. Anwar, and B. M. Kurkoski. Encoding and Decoding Construction D' Lattices for Power-Constrained Communications. In *2021 IEEE International Symposium on Information Theory (ISIT)*, pages 1005–1010. IEEE, 2021.
- [76] F. Zhou and B. M. Kurkoski. Construction D' Lattices for Power-Constrained Communications. *IEEE Transactions on Communications*, 70(4):2200–2212, 2022.

Received: April 1, 2023

Accepted for publication: August 30, 2023

Communicated by: Camilla Hollanti and Lenny Fukshansky