J. Algebra Comb. Discrete Appl.
13(2) • 199–216

Received: 11 June 2024
Accepted: 19 November 2025

Journal of Algebra Combinatorics Discrete Structures and Applications

Generalized subspace subcodes in the rank metric

Research Article

Ousmane Ndiaye, Peter Arnaud Kidoudou, Hervé Talé Kalachi*

Abstract: Rank-metric codes were studied by E. Gabidulin in 1985 after a brief introduction by Delsarte in 1978 as analogues of Reed-Solomon codes in the rank metric, but based on linearized polynomials. They have found applications in many areas, including linear network coding and space-time coding. They are also used in cryptography to reduce the size of the keys compared to Hamming metric codes at the same level of security. However, some families of rank-metric codes suffer from structural attacks due to the strong algebraic structure from which they are defined. It therefore becomes interesting to find new code families in order to address these questions in the landscape of rank-metric codes. In this paper, we provide a generalization of Subspace Subcodes in Rank metric introduced by Gabidulin and Loidreau. We also characterize this family by giving an algorithm which allows to have its generator and parity-check matrices based on the associated extended codes. We have also studied the specific case of Gabidulin codes whose underlying decoding algorithms are known. Bounds for the cardinalities of these codes, both in the general case and in the case of Gabidulin codes, are also provided.

2020 MSC: 11T71, 94B05

Keywords: Coding theory, rank-metric, Gabidulin code, Cryptography, Shortened code, Punctured code, Subfield Subcodes

1. Introduction

Rank-metric codes were studied by E. Gabidulin in 1985 [9] after a brief introduction by Delsarte in 1978 [7] who gave a description based on finite fields and its properties. By construction, Gabidulin codes

Ousmane Ndiaye (Corresponding Author); LACGAA, DMI, FST, Université Cheikh Anta Diop de Dakar, Senegal (email: ousmane3.ndiaye@ucad.edu.sn).
Peter Arnaud, Kidoudou; Faculty of Science and Technology, Université Marien Ngouabi (UMNG), Congo (email: peter.kidoudou@umng.cg).
Hervé Talé Kalachi; Department of Computer Engineering, National Advanced School of Engineering of Yaoundé, University of Yaounde 1, Cameroon, (email: herve.tale@univ-yaounde1.cm).
* *The author was supported by the UNESCO-TWAS and the German Federal Ministry of Education and Research (BMBF) under the SG-NAPI grant number 4500454079.*

are analogues of Reed-Solomon codes in the rank metric [30], since codewords are obtained by evaluation of $q-$polynomials on a support included in an extension of degree m of $\mathbb{F}_q$. Rank-metric codes have found applications in network coding [8], for example, when the transmitter and receiver are oblivious to the inner workings and topological network. Rank-metric codes has been also used in the theory of space-time codes, introduced by Lu and Kumar from Gabidulin codes [22].

Current cryptographic systems mostly rely on number-theoretic problems such as integer factorization and discrete logarithms. However, these problems are all vulnerable to quantum algorithms [31]. The theory of error correcting codes is a serious candidate that offers perspectives to face quantum computers via the Syndrome Decoding problem in the Hamming metric or in the Rank metric. They have been very used in cryptography these last decades to provide cryptographic primitives for encryption, signature, hashing or pseudo-random number generation. The main reason for using rank-metric codes in cryptography is the possibility of reducing the size of the keys compared to Hamming metric codes at the same level of security. Rank metric based cryptography began with the GPT cryptosystem and its variants [1, 12, 13, 21, 28, 29] based on Gabidulin codes [9], which are rank-metric analogues of Reed-Solomon codes. Unfortunately, as in the case of Reed-Solomon codes, the strong algebraic structure of these codes has been successfully exploited to attack the original GPT cryptosystem and its variants in a series of works initiated by Gibson and Overbeck [14, 15, 17, 20, 26, 27]. Recently, some public key cryptosystems based on rank-metric codes [23, 24] were candidates at the NIST competition for Post-Quantum Cryptography and up to the second round. But again, they were all eliminated after the second round of the competition due to security defects. Considering the fact that the very old McEliece cryptosystem that uses Subspace Subcodes of Generalized Reed-Solomon codes is still secure and currently at the fourth found of the NIST competition, it becomes theoretically interesting to study Subspace Subcodes in the rank-metric.

The notion of Subspace Subcode is used to denote a Subcode whose components of each codeword belong to the same vector subspace. This notion was first introduced in the Hamming metric for Reed-Solomon codes by Hattori, McEliece, and Solomon, G. [16]. A few years later, the same notion was introduced for rank-metric codes by Gabidulin and Loidreau with applications to cryptography [1, 11]. Recently, Berger, Gueye and Klamti [2] proposed a generalization of these Subcodes in the Hamming metric by allowing the components of each codeword of the Subcode to be in different subspaces. This previous work was followed by an article of Berger, Gueye, Klamti and Ruatta [3], proposing a cryptosystem based on quasi–cyclic Subcodes of Subspace Subcode of Reed-Solomon codes.

This paper introduces and characterizes the family of Generalized Subspace Subcodes of a rank-metric code by giving an algorithm which allows to construct their generator and parity-check matrices based on the associated extended codes. Bounds of the cardinalities of these codes both in the general case and in the case of Gabidulin codes are also provided as a generalization of the results obtained in [11]. The work ends by a focus on the specific case of Gabidulin codes whose decoding algorithms are known.

The rest of the document is organized as follows, we start in section 2 with some preliminaries to identify the generalities related to rank-metric codes. Section 3 presents some results on Generalized Subspace Subcodes in the rank-metric and a new result on the lower bound of their size. We give our main results on Generalized Subspace Subcodes of Gabidulin codes in section 4 by giving bounds of their size and an algorithm to construct directly a generator matrix. Section 5 deals with the parent Codes of Gabidulin RGSS [1] codes for decoding subcodes as alternative to using the decoding algorithm of the supercode. In section 6 we give some directions for their potential applications in cryptology and how it can reduce the key sizes. Finally, section 7 concludes the paper and gives some perspectives.

[1] *Rank Generalized Subspace Subcodes*

2. Preliminaries

2.1. Rank-metric codes

The *rank weight* $w_R(\mathbf{x})$ of a word $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ in an extension field $\mathbb{F}_{q^m}/\mathbb{F}_q$ is defined by the maximal number of its elements that are linearly independent over the base field $\mathbb{F}_q$, where m and n are positive integers and q a power of a prime number. The *rank distance* d_R between two words is defined by the rank weight of their difference, i.e. $d_R(\mathbf{x}, \mathbf{y}) = w_R(\mathbf{x} - \mathbf{y})$. It is well known that d_R has the properties of a metric on $\mathbb{F}_{q^m}^n$.

Definition 2.1. *Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ and $\{b_1, b_2, \ldots, b_m\}$ a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We can write $x_j = \sum_{i=1}^{m} x_{ij} b_i \in \mathbb{F}_{q^m}$ for each $j = 1, \cdots, n$ with $x_{ij} \in \mathbb{F}_q$. The rank weight $w_R(\mathbf{x})$ of $\mathbf{x}$ is defined as the rank of the matrix $M_{\mathbf{x}} = (x_{ij}) \in \mathbb{F}_q^{m \times n}$.*

In the sequel, a linear code of length n and dimension k (also called $[n,k]-$linear code or simply $[n,k]-$code) over $\mathbb{F}_{q^m}$ will denote a $k-$dimensional subspace of the $n-$dimensional vector space $\mathbb{F}_{q^m}^n$. A rank-metric code is then a linear code endowed with the above metric, called rank-metric. Given a rank-metric code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$, its minimum rank distance is

$$d_R(\mathcal{C}) = \min_{\mathbf{c}_1 \neq \mathbf{c}_2 \in \mathcal{C}} w_R(\mathbf{c}_1 - \mathbf{c}_2) = \min_{\mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}} w_R(\mathbf{c}).$$

If $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ is a $k-$dimensional rank-metric code with minimum rank distance $d_R(\mathcal{C})$, it is said to be a $[n, k, d = d_R(\mathcal{C})]_{q^m}-$code. The parameters of a $[n, k, d = d_R(\mathcal{C})]_{q^m}-$code are related by an equivalent of the Singleton bound for the rank distance, see [9]:

$$Card(\mathcal{C}) \leq q^{\min(m(n-d+1), n(m-d+1))}$$

where $Card$ is the cardinality of $\mathcal{C}$. Furthermore, a code satisfying the equality $Card(\mathcal{C}) = q^{\min(m(n-d+1), n(m-d+1))}$ is called a Maximum Rank Distance (MRD) code.

2.2. Punctured and shortened codes

Punctured and shortened codes of a given code are very important derivative codes to characterize certain subcodes, but also to mount structural attacks against code-based cryptosystems [6]. We are going to use them on extended codes to characterize Subspace Subcodes in the rank-metric. We recall here their definitions and some needed properties.

Definition 2.2 (Punctured code)**.** *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code, $\mathcal{I} \subseteq \{1, .., n\}$ a set of coordinate positions.*

- *Given a vector $\mathbf{y} \in \mathbb{F}_q^n$, the puntured vector $\mathbf{y}_{/\mathcal{I}}$ of $\mathbf{y}$ on $\mathcal{I}$ is defined by $\mathbf{y}_{/\mathcal{I}} := (y_i)_{i \in \{1,\ldots,n\} \setminus \mathcal{I}}$.*
- *The punctured code $\mathcal{C}_{/\mathcal{I}}$ of $\mathcal{C}$ on $\mathcal{I}$ is the code of length $n - |\mathcal{I}|$ defined by $\mathcal{C}_{/\mathcal{I}} = \{\mathbf{c}_{/\mathcal{I}} \mid \mathbf{c} \in \mathcal{C}\}$.*

In this paper, we will sometimes use the puncturing operation on matrices as follows. For a matrix $\boldsymbol{M} \in \mathbb{F}_q^{m \times n}$, the punctured matrix of $\boldsymbol{M}$ on $\mathcal{I}$ is the matrix $\boldsymbol{M}_{/\mathcal{I}} \in \mathbb{F}_q^{m \times (n - |\mathcal{I}|)}$ obtained by puncturing all the row vectors of $\boldsymbol{M}$ on $\mathcal{I}$.

Proposition 2.3. *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a $[n, k, d]-$code, $\mathcal{I} \subseteq \{1, \ldots, n\}$. Then $\mathcal{C}_{/\mathcal{I}}$ is an $[n - |\mathcal{I}|, k', d']-$code such that:*

$$k - |I| \leq k' \leq k \text{ and } d - |I| \leq d' \leq d.$$

Definition 2.4 (Shortened Code)**.** *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a linear code, $\mathcal{I} \subseteq \{1, \ldots, n\}$ a set of coordinates and $\mathcal{C}' = \{c \in \mathcal{C} \mid c_i = 0,\ \forall\ i \in \mathcal{I}\}$. The Shortened code of $\mathcal{C}$ on $\mathcal{I}$ denoted by $\mathcal{C}_{|\mathcal{I}}$ is the punctured code of $\mathcal{C}'$ on $\mathcal{I}$ i.e., $\mathcal{C}_{|\mathcal{I}} = \mathcal{C}'_{/\mathcal{I}}$.*

Proposition 2.5. *Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a $[n, k, d]-$code and $\mathcal{I} \subseteq \{1, \ldots, n\}$. Then $\mathcal{C}_{|\mathcal{I}}$ is a $[n - |\mathcal{I}|, k', d']-$code satisfying:*

$$k - |I| \leq k' \leq k \text{ and } d \leq d'.$$

Theorem 2.6. *(Link between Shortened and Punctured Codes [18], Theorem 1.5.7]) Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a $[n, k, d]-$code and $\mathcal{I} \subseteq \{1, \ldots, n\}$. We have*

1. $(\mathcal{C}^\perp)_{|\mathcal{I}} = (\mathcal{C}_{/\mathcal{I}})^\perp$
2. $(\mathcal{C}_{|\mathcal{I}})^\perp = (\mathcal{C}^\perp)_{/\mathcal{I}}$

This link allows us to have a generator matrix of a shortened code (subcode) of a code from the punctured code of its dual code.

3. Generalized subspace subcodes in the rank metric

Subspace Subcodes in the rank-metric were introduced by Gabidulin and Loidreau in [11], where decoding methods were also proposed. In this section, we give a generalization of Subspace Subcodes in the rank-metric.

Definition 3.1 ([11])**.** *Let $\mathcal{C}$ be a $[n, k, d = d_R(\mathcal{C})]_{q^m}-$code, and V a $\mathbb{F}_q-$vector subspace of $\mathbb{F}_{q^m}$ with dimension $s \leq m$. The Subspace Subcode of $\mathcal{C}$, with respect to V, is the $\mathbb{F}_q-$vector space $\mathcal{C} \cap V^n$.*

The elements of $\mathcal{C} \cap V^n$ are codewords whose components lie in the alphabet formed by the subspace V. In general, $\mathcal{C} \cap V^n$ is not $\mathbb{F}_{q^m}-$linear, but it is $\mathbb{F}_q-$linear and also linear over some intermediate extension depending on V. This code also corresponds by projection to the Subgroup Subcode [19] on the alphabet $\mathbb{F}_q^s$.
In the following, we introduce a generalization of definition 3.1 by allowing the choice of different vector subspaces for each coordinate.

Definition 3.2. *Let $\mathcal{C}$ be a $[n, k, d = d_R(\mathcal{C})]_{q^m}-$code, and $V_1, \ldots, V_n$ a series of n $\mathbb{F}_q-$vector subspaces of $\mathbb{F}_{q^m}$ with dimensions respectively s_1, s_2, …, s_n. Let denotes $\prod_{i=1}^{n} V_i$ the Cartesian product of $V_1, \ldots, V_n$. The Rank Generalized Subspace Subcode of $\mathcal{C}$ with respect to $\prod_{i=1}^{n} V_i$ is the $\mathbb{F}_q-$vector space $\mathcal{C} \cap \prod_{i=1}^{n} V_i$.*

Remark that all the V_i's are equal in definition 3.1, contrary to what we have in the above definition 3.2.
Let $B = \{b_1, b_2, \ldots, b_m\}$ be a basis of $\mathbb{F}_{q^m}$ as a $\mathbb{F}_q-$vector space. We consider the map $\phi_B : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$, mapping each element of $\mathbb{F}_{q^m}$ to its $\mathbb{F}_q-$coordinates in the basis B. That is to say, for any $x = \sum_{i=1}^{m} x_i b_i \in \mathbb{F}_{q^m}$ (with $x_i \in \mathbb{F}_q$), $\phi_B(x) = (x_1, x_2, \ldots, x_m)$. Given n $\mathbb{F}_q-$bases $B_1, \ldots, B_n$ of $\mathbb{F}_{q^m}$, this map can be extended to $\mathbb{F}_{q^m}^n$ by

$$\begin{aligned} \phi_{(B_i)_i} : \mathbb{F}_{q^m}^n &\longrightarrow \mathbb{F}_q^{mn} \\ (c_1, c_2, \ldots, c_n) &\longmapsto (\phi_{B_1}(c_1), \phi_{B_2}(c_2), \ldots, \phi_{B_n}(c_n)), \end{aligned}$$

In the case $B_1 = \cdots = B_n = B$, we will simply use ϕ_B insteed of $\phi_{(B_i)_i}$.

$\phi_{(B_i)_i}$ is called the expansion function and, applying it to all codewords of a $[n,k]-$code $\mathcal{C}$, this gives a new linear code of length nm called $q-$ary image of $\mathcal{C}$ and denoted by $\mathcal{C}^{((B_i)_i)}$ or simply $\mathcal{C}^{(B)}$ if $B_1 = \cdots = B_n = B$. More formally, we have the following definition.

Definition 3.3. *Let $\mathcal{C}$ be a linear code of length n and dimension k over $\mathbb{F}_{q^m}$. The $q-$ary image $\mathcal{C}^{((B_i)_i)}$ of $\mathcal{C}$ with respect to the n bases $B_1, \ldots, B_n$ of $\mathbb{F}_{q^m}$ is the image of $\mathcal{C}$ by the $\mathbb{F}_q-$linear map $\phi_{(B_i)_i}$:*

$$\mathcal{C}^{((B_i)_i)} = \phi_{(B_i)_i}(\mathcal{C})$$

Let $\mathcal{C}$ be an $[n,k]$ linear code over $\mathbb{F}_{q^m}$. In the following proposition, we describe how to explicitly compute a generator matrix and a parity-check matrix for the q-ary image $\mathcal{C}^{((B_i)_i)}$ of $\mathcal{C}$, where each coordinate expansion is done with respect to a possibly distinct basis B_i of $\mathbb{F}_{q^m}$.

Proposition 3.4. *Let $\mathcal{C}$ be a $[n,k]-$code over $\mathbb{F}_{q^m}$ and $B = \{b_1, b_2, \ldots, b_m\}$ be a basis of $\mathbb{F}_{q^m}$.*

1. *If $\boldsymbol{G} = \begin{pmatrix} \mathbf{g}_1 \\ \mathbf{g}_2 \\ \vdots \\ \mathbf{g}_k \end{pmatrix} \in \mathbb{F}_{q^m}^{k\times n}$ is a generator matrix of $\mathcal{C}$ then, the matrix $\hat{\boldsymbol{G}}^B_{(B_j)_j}$ defined by*

$$\hat{\boldsymbol{G}}^B_{(B_j)_j} = \begin{pmatrix} \phi_{(B_j)_j}(b_1\mathbf{g}_i) \\ \phi_{(B_j)_j}(b_2\mathbf{g}_i) \\ \vdots \\ \phi_{(B_j)_j}(b_m\mathbf{g}_i) \end{pmatrix}_{1\le i\le k} \in \mathbb{F}_q^{mk\times mn} \tag{1}$$

is a generator matrix of the $q-$ary image $\mathcal{C}^{((B_i)_i)}$ of $\mathcal{C}$ with respect to the n bases $B_1, \ldots, B_n$ of $\mathbb{F}_{q^m}$.

2. *If $\boldsymbol{H} = \begin{pmatrix} \mathbf{h}_1 \\ \mathbf{h}_2 \\ \vdots \\ \mathbf{h}_n \end{pmatrix}^T \in \mathbb{F}_{q^m}^{(n-k)\times n}$ is a parity-check [2] matrix of $\mathcal{C}$, then the matrix $\hat{\boldsymbol{H}}^B_{(B_j)_j}$ defined by*

$$\hat{\boldsymbol{H}}^B_{(B_j)_j} = \begin{pmatrix} \phi_{(B_j)_j}(b_1\mathbf{h}_i) \\ \phi_{(B_j)_j}(b_2\mathbf{h}_i) \\ \vdots \\ \phi_{(B_j)_j}(b_m\mathbf{h}_i) \end{pmatrix}^T_{1\le i\le n} \in \mathbb{F}_q^{m(n-k)\times mn} \tag{2}$$

is a parity-check matrix of the $q-$ary image $\mathcal{C}^{((B_i)_i)}$ of $\mathcal{C}$ with respect to the $n-k$ bases $B_1, \ldots, B_{n-k}$ of $\mathbb{F}_{q^m}$.

Proof. For the first point, let us consider for any line $i \in \{1, \cdots, k\}$ of $\boldsymbol{G}$, the map

$$\begin{aligned} f_{\mathbf{g}_i} : \mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_{q^m}^n \\ x &\longmapsto f_{\mathbf{g}_i}(x) = x\mathbf{g}_i, \end{aligned}$$

Since ϕ_B is an $\mathbb{F}_q-$isomorphism from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q^m$, we consider the $\mathbb{F}_q-$linear map $\theta_{\mathbf{g}_i} = \phi_{(B_j)_j} \circ f_{\mathbf{g}_i} \circ \phi_B^{-1}$ from $\mathbb{F}_q^m$ to $\mathbb{F}_q^{mn}$. Let $B^* = (b_1^*, \ldots, b_m^*)$ be a basis of $\mathbb{F}_q^m$ such that for any $i \in \{1, \cdots, m\}$, $b_i^* = \phi_B(b_i)$.

[2] *Here, the $\mathbf{h}_i$ are the column vectors of the matrix $\boldsymbol{H}$.*

As the encoding is considered as a vector-matrix product, the matrix of $\theta_{\mathbf{g}_i}$ in the basis B^* is given by a matrix $\boldsymbol{M}_{\mathbf{g}_i} \in \mathbb{F}_q^{m\times mn}$ such that:

$$\boldsymbol{M}_{\mathbf{g}_i} = \begin{pmatrix} \theta_{\mathbf{g}_i}(b_1^*) \\ \theta_{\mathbf{g}_i}(b_2^*) \\ \vdots \\ \theta_{\mathbf{g}_i}(b_m^*) \end{pmatrix} = \begin{pmatrix} \phi_{(B_j)_j} \circ f_{\mathbf{g}_i} \circ \phi_B^{-1}(b_1^*) \\ \phi_{(B_j)_j} \circ f_{\mathbf{g}_i} \circ \phi_B^{-1}(b_2^*) \\ \vdots \\ \phi_{(B_j)_j} \circ f_{\mathbf{g}_i} \circ \phi_B^{-1}(b_m^*) \end{pmatrix} = \begin{pmatrix} \phi_{(B_j)_j}(b_1\mathbf{g}_i) \\ \phi_{(B_j)_j}(b_2\mathbf{g}_i) \\ \vdots \\ \phi_{(B_j)_j}(b_m\mathbf{g}_i) \end{pmatrix}$$

To finish, we have by definition

$$\begin{aligned} \phi_{(B_j)_j}(\mathcal{C}) &= \{\phi_{(B_j)_j}(\mathbf{m}\boldsymbol{G}), \mathbf{m} \in \mathbb{F}_{q^m}^k\} \\ &= \{\phi_{(B_j)_j}(\textstyle\sum_{i=1}^k m_i\mathbf{g}_i), \mathbf{m} = (m_1, \cdots, m_k) \in \mathbb{F}_{q^m}^k\} \\ &= \{\textstyle\sum_{i=1}^k \phi_{(B_j)_j} \circ f_{\mathbf{g}_i}(m_i), \mathbf{m} = (m_1, \cdots, m_k) \in \mathbb{F}_{q^m}^k\} \\ &= \{\textstyle\sum_{i=1}^k \theta_{\mathbf{g}_i} \circ \phi_B(m_i), \mathbf{m} = (m_1, \cdots, m_k) \in \mathbb{F}_{q^m}^k\} \\ &= \{\textstyle\sum_{i=1}^k \theta_{\mathbf{g}_i}(\mathbf{m}_i'), \mathbf{m}' = (\mathbf{m}_1', \cdots, \mathbf{m}_k') \in (\mathbb{F}_q^m)^k\} \\ &= \{\textstyle\sum_{i=1}^k \mathbf{m}_i'\boldsymbol{M}_{\mathbf{g}_i}, \mathbf{m}' = (\mathbf{m}_1', \cdots, \mathbf{m}_k') \in (\mathbb{F}_q^m)^k\} \\ &= \{\mathbf{m}' \cdot \begin{pmatrix} \boldsymbol{M}_{\mathbf{g}_1} \\ \boldsymbol{M}_{\mathbf{g}_2} \\ \vdots \\ \boldsymbol{M}_{\mathbf{g}_k} \end{pmatrix}, \quad \mathbf{m}' \in \mathbb{F}_q^{km}\} \\ &= < \begin{pmatrix} \boldsymbol{M}_{\mathbf{g}_1} \\ \boldsymbol{M}_{\mathbf{g}_2} \\ \vdots \\ \boldsymbol{M}_{\mathbf{g}_k} \end{pmatrix} >_{\mathbb{F}_q} \end{aligned}$$

The proof of the second point of the proposition is similar. Indeed, by considering only the $n-k$ bases $B_1, \ldots, B_{n-k}$ of $\mathbb{F}_{q^m}$, let us apply $\phi_{(B_j)_j}$ on a syndrome $\mathbf{s}$ given by $\mathbf{s}^T = \mathbf{y} \cdot H^T$. We have

$$\begin{aligned} \phi_{(B_j)_j}(\mathbf{s}^T) &= \phi_{(B_j)_j}(\mathbf{y} \cdot H^T) \\ &= \textstyle\sum_{i=1}^n \phi_{(B_j)_j} \circ f_{\mathbf{h}_i}(y_i) \\ &= \phi_B(\mathbf{y}) \cdot \begin{pmatrix} \boldsymbol{M}_{\mathbf{h}_1} \\ \boldsymbol{M}_{\mathbf{h}_2} \\ \vdots \\ \boldsymbol{M}_{\mathbf{h}_n} \end{pmatrix} = \phi_B(\mathbf{y}) \cdot \begin{pmatrix} \phi_{(B_j)_j}(b_1\mathbf{h}_i) \\ \phi_{(B_j)_j}(b_2\mathbf{h}_i) \\ \vdots \\ \phi_{(B_j)_j}(b_m\mathbf{h}_i) \end{pmatrix}_{1\le i\le n} \end{aligned}$$

□

One can remark that this proposition is a general case of [32, Theorem 1], that can be obtained from the above proposition by taking $B_1 = B_2 = \cdots = B_n$. Furthermore, by using the notations in the above proof, one can remark that for any $i \in \{1, \cdots, k\}$, the map $f_{\mathbf{g}_i}$ can be decomposed as $f_{\mathbf{g}_i} = (f_{g_{i1}}, f_{g_{i2}}, \cdots, f_{g_{in}})$. So, the matrix $\hat{\boldsymbol{G}}^B_{(B_j)_j}$ can be written as follows :

$$\hat{\boldsymbol{G}}^B_{(B_j)_j} = (\boldsymbol{M}_{g_{ij}})_{1\le i\le k, 1\le j\le n} = \begin{pmatrix} \boldsymbol{M}_{g_{11}} & \cdots & \boldsymbol{M}_{g_{1n}} \\ \boldsymbol{M}_{g_{21}} & \cdots & \boldsymbol{M}_{g_{2n}} \\ \vdots & \ddots & \vdots \\ \boldsymbol{M}_{g_{k1}} & \cdots & \boldsymbol{M}_{g_{kn}} \end{pmatrix} \in (\mathbb{F}_q^{m\times m})^{k\times n}$$

where the matrix $\boldsymbol{M}^T_{g_{ij}} = \mathcal{M}_{B,B_j}(\theta_{g_{ij}})$ is the matrix of the linear map $\theta_{g_{ij}}$ from the basis B to the basis B_j, for $i \in \{1, \cdots, k\}$ and $j \in \{1, \cdots, n\}$. Another remark is that, for a different basis B' we get another

generator matrix $\hat{\boldsymbol{G}}^{B'}_{(B_j)_j}$ of the same code, and this is the same for $\hat{\boldsymbol{H}}^{B'}_{(B_j)_j}$. To simplify things in the following, we will sometimes write $\hat{\boldsymbol{G}}_{(B_j)_j}$ instead of $\hat{\boldsymbol{G}}^{B}_{(B_j)_j}$ and if $B_1 = B_2 = \cdots = B_n = B$, we define $\hat{\boldsymbol{G}}_B := \hat{\boldsymbol{G}}^{B}_{(B_j)_j}$.

Example 3.5. *Let $n = 7$, $m = 3$, and let α be a root of the irreducible polynomial $x^3 + x + 1$. Let's consider the $[n, 3]-$code $\mathcal{C}$ generated by the following generator matrix:*

$$\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 \\ 0 & 1 & 0 & \alpha^6 & \alpha^6 & 1 & \alpha^2 \\ 0 & 0 & 1 & \alpha^5 & \alpha^4 & 1 & \alpha^4 \end{pmatrix}$$

For $\mathcal{B} = \{1 = (100), \alpha = (010), \alpha^2 = (001)\} = B_1 = \cdots B_7$, a generator matrix of the binary image $\mathcal{C}^{(B)}$ of $\mathcal{C}$ is :

$$\hat{\boldsymbol{G}}_B = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc} 1&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&1&1&0 \\ 0&1&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&1&1 \\ 0&0&1&0&0&0&0&0&0&1&1&1&1&1&0&0&0&1&1&1&1 \\ \hline 0&0&0&1&0&0&0&0&0&1&0&1&1&0&1&1&0&0&0&0&1 \\ 0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&1&0&1&1&0 \\ 0&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&1&0&1&1 \\ \hline 0&0&0&0&0&0&1&0&0&1&1&1&0&1&1&1&0&0&0&1&1 \\ 0&0&0&0&0&0&0&1&0&1&0&1&1&1&1&0&1&0&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&1&1&0&1 \end{array}\right)$$

A parity-check matrix of $\mathcal{C}^{(B)}$ is, by using the fact that $\hat{\boldsymbol{G}}_B \cdot (\hat{\boldsymbol{H}}_B)^T = 0$, :

$$\hat{\boldsymbol{H}}_B = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc|ccc} 1&0&1&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&1&1&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&1&1&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ \hline 0&0&1&1&1&0&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0 \\ 1&0&1&0&0&1&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&1&0&1&0&0&1&1&1&0&0&0&0&0&1&0&0&0&0&0&0 \\ \hline 1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&1&0&0&0 \\ \hline 1&0&1&0&1&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0&0 \\ 1&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&1&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right)$$

To construct a subcode restricted to subspaces, the general approach begins by computing the $q-$ary image of the code via a fixed basis of $\mathbb{F}_{q^m}$. Then, for each coordinate block of size m, a suitable change of basis is applied. After this transformation, the code is punctured on selected positions to eliminate undesired coordinates, and taking the dual of the resulting code yields the desired subcode. In what follows, we present several results underlying this process.

In the sequel, given a set of positions $U \subseteq \{1, 2, \ldots, nm\}$, we denote its complement by $\bar{U} := \{1, 2, \ldots, nm\} \setminus U$. The next proposition formalizes this construction: it shows that shortening the q-ary image of a code $\mathcal{C}$ on the positions $\bar{U}$ yields the q-ary image of a subspace subcode $\mathcal{C} \cap V^n$, where $V \subset \mathbb{F}_{q^m}$ is an appropriately chosen $\mathbb{F}_q$-subspace. Since $\mathcal{C} \cap V^n \subset V^n$, each codeword can be expressed using a basis B_s of V. We will abusively denote by $(\mathcal{C} \cap V^n)^{(B_s)}$ the q-ary image obtained via coordinate-wise expansion with respect to B_s.

Proposition 3.6. *Let $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ be a linear code of length n, $B = \{b_1, b_2, \ldots, b_m\}$ an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$, and let $B_s = \{b_1, \ldots, b_s\}$ with $V = \langle B_s \rangle \subset \mathbb{F}_{q^m}$ an s-dimensional $\mathbb{F}_q$-subspace. Define the set $U = u_1 \cup \ldots \cup u_n \subseteq \{1, 2, \ldots, nm\}$, where for each $1 \leq j \leq n$, we let $u_j = \{(j-1)m + 1, \ldots, (j-1)m + s\}$. Then, the shortened code $(\mathcal{C}^{(B)})_{|\bar{U}}$ is equal to the q-ary image of the subspace subcode $\mathcal{C} \cap V^n$ with respect to the basis B_s:*

$$(\mathcal{C} \cap V^n)^{(B_s)} = (\mathcal{C}^{(B)})_{|\bar{U}}$$

Proof. Let $\mathbf{y} = (y_{1,1}, \ldots, y_{s,1}, \ldots, y_{1,j}, \ldots, y_{s,j}, \ldots, y_{1,n}, \ldots, y_{s,n}) \in (\mathcal{C}^{(B)})_{|\bar{U}}$.

Then there exists $\mathbf{c} \in \phi_B(\mathcal{C}) = \mathcal{C}^{(B)}$ such that $\mathbf{y}$ is obtained by puncturing $\mathbf{c}$ at the positions in $\bar{U}$, and $\mathbf{c}_i = 0$ for all $i \in \bar{U}$.

Since $V = \phi_B^{-1}\big(\{(x_1, \ldots, x_s, 0, \ldots, 0) \mid x_1, \ldots, x_s \in \mathbb{F}_q\}\big)$, it follows that $\phi_B^{-1}(\mathbf{c}) \in \mathcal{C} \cap V^n$, and thus $\mathbf{c} \in \phi_B(\mathcal{C} \cap V^n)$. Hence,

$$\mathbf{y} \in ((\mathcal{C} \cap V^n)^{(B)})_{/\bar{U}} = (\mathcal{C} \cap V^n)^{(B_s)}.$$

Conversely, it is immediate that $(\mathcal{C} \cap V^n)^{(B_s)} \subseteq (\mathcal{C}^{(B)})_{|\bar{U}}$, and we conclude $(\mathcal{C} \cap V^n)^{(B_s)} = (\mathcal{C}^{(B)})_{|\bar{U}}$. □

Thanks to Proposition 3.6, the construction of a subspace subcode $\mathcal{C} \cap V^n$ can, in practice, be reduced to computing the q-ary image of $\mathcal{C}$ and then shortening it at appropriately chosen positions. To do so, we may use theorem 2.6, $((\mathcal{C}^{(B)})_{|\bar{U}})^{\perp} = ((\mathcal{C}^{(B)})^{\perp})_{/\bar{U}}$ and compute the punctured code that is easier to do.

Example 3.7. *Using the same code defined in Example 3.5, we consider $s = 1$ and $V = \mathbb{F}_2 = \langle 1 \rangle_{\mathbb{F}_2}$ to mean $B_s = \{1\}$. By definition, this yields the index set*

$$U = u_1 \cup \cdots \cup u_7 = \{1, 4, 7, 10, 13, 16, 19\},$$

corresponding to the first coordinate of each block of size $m = 3$. Thanks to Theorem 2.6, the dual of the shortened code $(\mathcal{C}^{(B)})_{|\bar{U}}$ is generated by the matrix $(\hat{\boldsymbol{H}}_B)_{/\bar{U}}$ obtained from the full parity-check matrix $\hat{\boldsymbol{H}}_B$ by retaining only the columns indexed by U. That is to say

$$(\hat{\boldsymbol{H}}_B)_{/\bar{U}} = \left(\begin{array}{ccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{array}\right)$$

Thus, we obtain that $((\mathcal{C}^{(B)})_{|\bar{U}})^{\perp} = (\mathcal{C} \cap \mathbb{F}_2^7)^{\perp}$ is generated by

$$\boldsymbol{H}_{\bar{U}} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Note that one can easily compute a generator matrix $\boldsymbol{G}_{\bar{U}}$ of the subspace subcode $\mathcal{C} \cap \mathbb{F}_2^7$ from $\boldsymbol{H}_{\bar{U}}$.

We now recall a fundamental result describing how a coordinate-wise change of basis in $\mathbb{F}_{q^m}^n$ impacts the q-ary image of a code, as well as its associated generator and parity-check matrices.

Theorem 3.8. *[5, lemma 34] Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_{q^m}$, $B = \{b_1, b_2, \ldots, b_m\}$ be a basis of $\mathbb{F}_{q^m}$. Let $(\boldsymbol{Q}_j)_j \in (GL_m(\mathbb{F}_q))^n$. The following equalities hold.*

$$\mathcal{C}^{((\boldsymbol{Q}_j^{-1}B)_j)} = \mathcal{C}^{(B)} \cdot \begin{pmatrix} \boldsymbol{Q}_1 & & \\ & \ddots & \\ & & \boldsymbol{Q}_n \end{pmatrix},$$

$$\hat{\boldsymbol{G}}^B_{(\boldsymbol{Q}_j^{-1}B)_j} = \hat{\boldsymbol{G}}_B \cdot \begin{pmatrix} \boldsymbol{Q}_1 & & \\ & \ddots & \\ & & \boldsymbol{Q}_n \end{pmatrix}, \text{ and}$$

$$\hat{\boldsymbol{H}}^B_{(\boldsymbol{Q}_j^{-1}B)_j} = \hat{\boldsymbol{H}}_B \cdot \begin{pmatrix} (\boldsymbol{Q}_1^{-1})^T & & \\ & \ddots & \\ & & (\boldsymbol{Q}_n^{-1})^T \end{pmatrix}$$

In practice, Theorem 3.8 implies that changing the basis at each coordinate position corresponds to right-multiplication by a block-diagonal matrix on the q-ary image. This technique offers several important benefits. Firstly, it allows working from a global basis (e.g., the canonical basis), simplifying the expansion process via standard coordinate maps. Secondly, the change-of-basis matrices can be structured so that their first s_i columns span the subspace V_i, and the remaining columns form a complement, enabling efficient coordinate elimination through puncturing. During decoding, this layout also helps easily identify the eliminated positions, facilitating reliable error correction in the subspace subcode. These features make this approach well suited for the construction and decoding of generalized subspace subcodes.

Consequently, we deduce the following corollary.

Corollary 3.9. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_{q^m}$, $B = \{b_1, b_2, \ldots, b_m\}$ be a basis of $\mathbb{F}_{q^m}$ and $V =< d_1, \ldots, d_s >_{\mathbb{F}_q}$ a $s-$dimensional subspaces of $\mathbb{F}_{q^m}$. Given any completed basis $D = \{d_1, d_2, \ldots, d_s, \ldots, d_m\}$ from $D_s = \{d_1, d_2, \ldots, d_s\}$, and $\boldsymbol{Q}$ the change-of-basis matrix from the basis D to the basis B, we have :*

$$(\mathcal{C}^{(D)})_{|\bar{U}} = (\mathcal{C} \cap V^n)^{(B)} \cdot \begin{pmatrix} \boldsymbol{Q} & & \\ & \ddots & \\ & & \boldsymbol{Q} \end{pmatrix}_{|\bar{U}}$$

Where $U = u_1 \cup \ldots \cup u_n \subseteq \{1, 2, \ldots, nm\}$ with $u_j = \{(j-1)m + 1, \ldots, (j-1)m + s\}$ for $1 \leq j \leq n$.

Before giving the proof, we note that the change-of-basis matrices are defined with the convention that message encoding is performed via vector-matrix multiplication (i.e., messages are treated as row vectors). Consequently, the change of basis is applied row-wise. When we represent a basis $B = \{b_1, b_2, \ldots, b_m\}$ as a matrix, it simply corresponds to the change-of-basis matrix from the canonical basis $K = \{1, \alpha, \ldots, \alpha^{m-1}\}$ to the chosen basis : $B = \begin{pmatrix} \phi_K(b_1) \\ \phi_K(b_2) \\ \vdots \\ \phi_K(b_m) \end{pmatrix} \in \mathbb{F}_q^{m \times m}$

Proof. According to Proposition 3.6, we have $(\mathcal{C}^{(D)})_{|\bar{U}} = (\mathcal{C} \cap V^n)^{(D_s)} = ((\mathcal{C} \cap V^n)^{(D)})_{/\bar{U}}$. As $\boldsymbol{Q}D = B$, then $(\mathcal{C} \cap V^n)^{(D_s)} = \left((\mathcal{C} \cap V^n)^{(Q^{-1}B)}\right)_{|\bar{U}} = (\mathcal{C} \cap V^n)^{(B)} \cdot \begin{pmatrix} \boldsymbol{Q} & & \\ & \ddots & \\ & & \boldsymbol{Q} \end{pmatrix}_{|\bar{U}}$. □

We now extend the previous result to the case where each coordinate of the code is restricted to a different subspace $V_j \subseteq \mathbb{F}_{q^m}$. This leads to the following expression for the q-ary image of a generalized subspace subcode.

Corollary 3.10. *Let $\mathcal{C}$ be a linear code of length n over $\mathbb{F}_{q^m}$ and B be a $\mathbb{F}_q-$basis of $\mathbb{F}_{q^m}$. For any $j \in \{1, \cdots, m\}$, let $V_j =< d_{1,j}, \ldots, d_{s_j,j} >$ be a s_j-dimensional $\mathbb{F}_q-$subspaces of $\mathbb{F}_{q^m}$, $D_j = \{d_{1,j}, \ldots, d_{s_j,j}, \ldots, d_{m,j}\}$ be a completed basis from $D_{s_j} = \{d_{1,j}, \ldots, d_{s_j,j}\}$, and $\boldsymbol{Q}_j$ the change-of-basis matrix from the basis D_j to the basis D. By setting $W = \prod_{i=1}^{n} V_i$, we have*

$$(\mathcal{C}^{((D_j)_j)})_{|\bar{U}} = ((\mathcal{C} \cap W)^{((\boldsymbol{Q}_j^{-1}B)_j)})_{|\bar{U}} = (\mathcal{C} \cap W)^{(B)} \cdot \begin{pmatrix} \boldsymbol{Q}_1 & & \\ & \ddots & \\ & & \boldsymbol{Q}_n \end{pmatrix}_{|\bar{U}}$$

Where $U = u_1 \cup \ldots \cup u_n \subseteq \{1, 2, \ldots, nm\}$ with $u_j = \{(j-1)m + 1, \ldots, (j-1)m + s_j\}$ for $1 \leq j \leq n$.

Thanks to the duality between shortening and puncturing (Theorem 2.6), a generator matrix of the generalized subspace subcode $(\mathcal{C} \cap W)^{((\boldsymbol{Q}_j^{-1}B)_j)}$ can be obtained by computing the kernel of the punctured parity-check matrix $(\hat{\boldsymbol{H}}_{(\boldsymbol{Q}_j^{-1}B)_j})_{/\bar{U}}$.

Example 3.11. *Using the same code defined in Example 3.5, let us define $W = V_1 \times V_2 \times V_1 \times V_3 \times V_1 \times V_2 \times V_1$, with $V_1 = \langle 1, \alpha \rangle$, $V_2 = \langle 1, \alpha^2 \rangle$, and $V_3 = \langle \alpha, \alpha^2 \rangle$. We consider $D_1 = D_3 = D_5 = D_7 = \mathcal{B} = \{1, \alpha, \alpha^2\}$, $D_2 = D_6 = \{1, \alpha^2, \alpha\}$, and $D_4 = \{\alpha, \alpha^2, 1\}$. It is obvious that all the s_j have the same value, which is 2 and $U = u_1 \cup \cdots \cup u_7 = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20\}$. The different change-of-basis matrices from D_j to the bases B ($j = 1, \ldots, 7$) are :*

$$\boldsymbol{Q}_1 = \boldsymbol{Q}_3 = \boldsymbol{Q}_5 = \boldsymbol{Q}_7 = \boldsymbol{I}_3,\ \boldsymbol{Q}_2 = \boldsymbol{Q}_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \boldsymbol{Q}_4 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Let $\boldsymbol{D} = \mathrm{Diag}(\boldsymbol{Q}_1^T, \boldsymbol{Q}_2^T, \boldsymbol{Q}_3^T, \boldsymbol{Q}_4^T, \boldsymbol{Q}_5^T, \boldsymbol{Q}_6^T, \boldsymbol{Q}_7^T)_{/\bar{U}}$. Then an extended parity-check matrix of the subcode $\mathcal{C} \cap W$ is given by $H_U = \hat{\boldsymbol{H}}_B \cdot D$.

Hence, H_U is obtained by deleting columns $3, 5, 9, 10, 15, 17, 21$ from $\hat{\boldsymbol{H}}_B$, resulting in:

$$H_U = \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc} 1&0&1&0&1&1&0&0&0&0&0&0&0&0\\ 1&1&0&1&1&0&1&0&0&0&0&0&0&0\\ 0&1&1&0&1&1&0&1&0&0&0&0&0&0\\ \hline 0&0&1&0&0&1&0&0&1&0&0&0&0&0\\ 1&0&0&1&1&1&0&0&0&1&0&0&0&0\\ 0&1&1&0&1&1&0&0&0&0&0&0&0&0\\ \hline 1&0&1&0&1&0&0&0&0&0&1&0&0&0\\ 0&1&0&0&0&1&0&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0&0&0&0&1&0&0\\ \hline 1&0&0&0&0&1&0&0&0&0&0&0&1&0\\ 1&1&0&1&1&1&0&0&0&0&0&0&0&1\\ 0&1&1&1&1&1&0&0&0&0&0&0&0&0 \end{array}\right)$$

After row operations, we obtain an extended generator matrix of $\mathcal{C} \cap W$ in a systematic form with respect to the bases D_j:

$$G_U = \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc} 1&0&1&1&0&0&0&1&1&0&0&1&1&1\\ 0&1&0&1&1&1&1&1&1&1&1&1&1&1 \end{array}\right)$$

As a binary code, $\mathcal{C}$ has length $n = 14$ and dimension $k = 2$. As a block code, it has length $n = 7$ and dimension $k = 2$.

Let's now establish a lower bound on the cardinality of a generalized subspace subcode in the rank metric, expressed in terms of the dimensions of the underlying subspaces.

Proposition 3.12. *Let $\mathcal{C}$ be a $[n, k, d = d_R(\mathcal{C})]_{q^m}$-code, and let $V_1, \ldots, V_n$ be $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$ of respective dimensions $s_1, \ldots, s_n \leq m$. Define the ambient subspace $W := \prod_{i=1}^{n} V_i \subseteq \mathbb{F}_{q^m}^n$. Then the following inequality holds :*

$$q^{\sum_{i=1}^{n} s_i - m(n-k)} \leq |\mathcal{C} \cap W|.$$

Proof. Without loss of generality, assume that $s_1 \leq s_2 \leq \cdots \leq s_n$. By permuting the coordinates of $\mathcal{C}$, which preserves its code parameters and subcode dimension (up to isometry), we may assume that $V_1 \subseteq V_2 \subseteq \cdots \subseteq V_n$.

Let $\{\beta_1, \ldots, \beta_{s_n}\}$ be a common $\mathbb{F}_q$-basis such that $V_i = \langle \beta_1, \ldots, \beta_{s_i} \rangle$. Then any vector $\mathbf{c} = (c_1, \ldots, c_n) \in W$ can be written as:

$$c_i = \sum_{t=1}^{s_i} u_{t,i}\beta_t = \sum_{t=1}^{s_n} u_{t,i}\beta_t, \quad \text{where } u_{t,i} = 0 \text{ for } t > s_i.$$

Hence,

$$\mathbf{c} = (\beta_1, \ldots, \beta_{s_n}) \cdot \boldsymbol{U}, \quad \text{where } \boldsymbol{U} \in \mathbb{F}_q^{s_n \times n}.$$

Let $\boldsymbol{H} \in \mathbb{F}_{q^m}^{(n-k)\times n}$ be a parity-check matrix of $\mathcal{C}$. Then $\mathbf{c} \in \mathcal{C}$ if and only if :

$$(\beta_1, \ldots, \beta_{s_n}) \cdot \boldsymbol{U} \cdot \boldsymbol{H}^T = 0.$$

Expanding each product $\beta_i h_{j,t}$ over a fixed $\mathbb{F}_q$-basis $\{\gamma_1, \ldots, \gamma_m\}$ of $\mathbb{F}_{q^m}$, we write :

$$\beta_i h_{j,t} = \sum_{\ell=1}^{m} \delta_{i,t}^{(j,\ell)} \gamma_\ell, \quad \delta_{i,t}^{(j,\ell)} \in \mathbb{F}_q.$$

So the condition above leads to the following linear system over $\mathbb{F}_q$ in the unknowns $u_{t,i}$:

$$\sum_{i=1}^{s_n} \sum_{t=1}^{n} \delta_{i,t}^{(j,\ell)} u_{i,t} = 0 \quad \text{for all } j = 1, \ldots, n-k, \ \ell = 1, \ldots, m.$$

This gives a system of $m(n-k)$ linear equations in $\sum_{i=1}^{n} s_i$ unknowns. Hence, the space of solutions has dimension at least $\sum_{i=1}^{n} s_i - m(n-k)$, which yields $|\mathcal{C} \cap W| \geq q^{\sum_{i=1}^{n} s_i - m(n-k)}$. □

Notice that taking $s_1 = \ldots = s_n$ leads to the result obtained by E. Gabidulin and P. Loidreau in [11] as a special case.

Corollary 3.13 ([11], Proposition 1)**.** *Let $\mathcal{C}$ be a $[n, k, d = d_R(\mathcal{C})]_{q^m}$-code and let $V \subseteq \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-subspace of dimension $s \leq m$. Then,*

$$q^{ns - m(n-k)} \leq |\mathcal{C} \cap V^n|.$$

To summarize, we have established an explicit representation of generalized subspace subcodes using expansion maps, change-of-basis matrices, and shortening operations. These tools pave the way for efficient construction and analysis of subcodes with tailored structural properties.

4. Generalized subspace subcodes of Gabidulin codes

4.1. Gabidulin codes

Gabidulin codes [9] are a class of maximum rank distance (MRD) codes constructed using q-polynomials, also known as linearized polynomials, first studied by Ore in [25]. These polynomials are of the form $P(z) = \sum_i p_i z^{q^i}$, with $p_i \in \mathbb{F}_{q^m}$ and finitely many nonzero coefficients. We adopt the shorthand notation $[i] := q^i$, so that $P(z) = \sum_i p_i z^{[i]}$.

The set of q-polynomials with coefficients in $\mathbb{F}_{q^m}$, equipped with addition and composition, forms a non-commutative ring denoted by $\mathcal{P}_{q^m}$. These polynomials induce $\mathbb{F}_q$-linear endomorphisms of $\mathbb{F}_{q^m}$.

Definition 4.1. *Let $\mathbf{g} = (g_1, \ldots, g_n) \in \mathbb{F}_{q^m}^n$ be such that the g_j's are $\mathbb{F}_q$-linearly independent, and let $k < n$. The* Gabidulin code *of length n, dimension k, and support $\mathbf{g}$ is defined as:*

$$Gab_k(\mathbf{g}) = \left\{ (P(g_1), \ldots, P(g_n)) \in \mathbb{F}_{q^m}^n \;\middle|\; P \in \mathcal{P}_{q^m}, \ \deg_q(P) < k \right\}.$$

A generator matrix of $Gab_k(\mathbf{g})$ is given by the $k \times n$ matrix:

$$G = \begin{pmatrix} g_1^{[0]} & \cdots & g_n^{[0]} \\ g_1^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \ddots & \vdots \\ g_1^{[k-1]} & \cdots & g_n^{[k-1]} \end{pmatrix}.$$

Gabidulin codes meet the Singleton bound for the rank metric, and therefore satisfy $d_R = n - k + 1$. Consequently, they can correct up to $\tau_{\max} = \left\lfloor \frac{n-k}{2} \right\rfloor$ rank errors.

Note that the structure of Gabidulin codes is analogous to that of Reed-Solomon codes, with the classical monomial powers g_j^i replaced by Frobenius powers $g_j^{[i]}$, and the support being a set of linearly independent elements over $\mathbb{F}_q$.

It is also well known that a parity-check matrix of a $[n,k,d]$-Gabidulin code is given by:

$$H = \begin{pmatrix} h_1^{[0]} & \cdots & h_n^{[0]} \\ h_1^{[1]} & \cdots & h_n^{[1]} \\ \vdots & \ddots & \vdots \\ h_1^{[d-2]} & \cdots & h_n^{[d-2]} \end{pmatrix},$$

where $\mathbf{h} = (h_1, \ldots, h_n) \in Gab_k(\mathbf{g})^{\perp}$ is a codeword of full rank.

4.2. Rank generalized Subspace subcodes of Gabidulin codes

We now specialize the results established previously to the important family of Gabidulin codes. We first present a lemma relating the generalized subspace subcodes of Gabidulin codes to a well-known Gabidulin parent code, and derive explicit cardinality bounds.

Lemma 4.2. *Let $Gab_k(\mathbf{g})$ be an $[n,k,d]$-Gabidulin code over $\mathbb{F}_{q^m}$. Consider subspaces $V_1, \ldots, V_n$ of dimensions $s_1, \ldots, s_n \leq m$ and define $W = \prod_{i=1}^n V_i$. Then, each codeword of $Gab_k(\mathbf{g}) \cap W$ maps uniquely to a codeword of the Gabidulin code $\mathcal{B}_W$ having parity-check matrix*

$$T = (\beta_j^{[m-i+1]})_{1 \leq i \leq d-1,\, 1 \leq j \leq s}$$

with $s = \max_i(s_i)$ and $(\beta_1, \ldots, \beta_s)$ linearly independent.

Proof. According to Proposition 3.12, we have

$$c \in \mathcal{C} \cap W \iff \begin{cases} c = (\beta_1, \beta_2, \cdots, \beta_{s_n})\boldsymbol{U} \\ (\beta_1, \beta_2, \cdots, \beta_{s_n})\boldsymbol{U}\boldsymbol{H}^T = 0 \end{cases}$$

where $\boldsymbol{H} = \begin{pmatrix} h_1^{[0]} & \cdots & h_n^{[0]} \\ h_1^{[1]} & \cdots & h_n^{[1]} \\ \vdots & \cdots & \vdots \\ h_1^{[d-2]} & \cdots & h_n^{[d-2]} \end{pmatrix}$.

By setting $\boldsymbol{L} = \boldsymbol{U}\boldsymbol{H}^T$, we have

$$\boldsymbol{L}_{i,j} = \sum_{l=1}^{n} u_{i,l} h_l^{[j-1]} = \left(\sum_{l=1}^{n} u_{i,l} h_l \right)^{[j-1]} = \boldsymbol{L}_{i,1}^{[j-1]}.$$

Since $0 = (\beta_1, \beta_2, \cdots, \beta_{s_n})\boldsymbol{U}\boldsymbol{H}^T$, for $w_i = \boldsymbol{L}_{i,1}$ and $1 \leq j \leq d-1$ we have

$$\begin{aligned} 0 &= (\beta_1, \beta_2, \cdots, \beta_{s_n}). \begin{pmatrix} w_1^{[j-1]} \\ w_2^{[j-1]} \\ \vdots \\ w_{s_n}^{[j-1]} \end{pmatrix} \\ &= \beta_1 w_1^{[j-1]} + \beta_2 w_2^{[j-1]} + \cdots + \beta_{s_n} w_{s_n}^{[j-1]} \\ &= (\beta_1^{[m-j+1]} w_1 + \beta_2^{[m-j+1]} w_2 + \cdots + \beta_{s_n}^{[m-j+1]} w_{s_n})^{[j-1]} \end{aligned}$$

$$= \beta_1^{[m-j+1]} w_1 + \beta_2^{[m-j+1]} w_2 + \cdots + \beta_{s_n}^{[m-j+1]} w_{s_n}$$
$$= (w_1, \cdots, w_{s_n}) \begin{pmatrix} \beta_1^{[m-j+1]} \\ \beta_2^{[m-j+1]} \\ \vdots \\ \beta_{s_n}^{[m-j+1]} \end{pmatrix}$$

Which leads to

$$(w_1, \ldots, w_{s_n}) \begin{pmatrix} \beta_1^{[m]} & \beta_1^{[m-1]} & \cdots & \beta_1^{[m-d+2]} \\ \beta_2^{[m]} & \beta_2^{[m-1]} & \cdots & \beta_2^{[m-d+2]} \\ \vdots & \vdots & \cdots & \vdots \\ \beta_{s_n}^{[m]} & \beta_{s_n}^{[m-1]} & \cdots & \beta_{s_n}^{[m-d+2]} \end{pmatrix} = 0$$

Let $\mathcal{B}_W$ be the Gabidulin code having parity-check matrix $\boldsymbol{T} = (\beta_j^{[m-i+1]})_{i=1,j=1}^{d-1,s_n}$. Then, $c = (\beta_1, \beta_2, \cdots, \beta_{s_n})\boldsymbol{U} \in Gab_k(\mathbf{g}) \cap W \Longrightarrow (w_1, \cdots, w_{s_n}) \in \mathcal{B}_W$. □

The lemma above allows us to establish explicit cardinality bounds.

Theorem 4.3. *Let $Gab_k(\mathbf{g})$ be a $[n,k,d]$-Gabidulin code over $\mathbb{F}_{q^m}$, and $W = \prod_i V_i$ as above. Then,*

$$q^{\sum_i s_i - m(n-k)} \leq |Gab_k(\mathbf{g}) \cap W| \leq q^{m(\max_i(s_i)-(n-k))}.$$

Proof. According to Lemma 4.2, $c = (\beta_1, \beta_2, \cdots, \beta_{s_n})\boldsymbol{U} \in Gab_k(\mathbf{g}) \cap W \Longrightarrow (w_1, \cdots, w_{s_n}) \in \mathcal{B}_W$. So we have $|Gab_k(\mathbf{g}) \cap W| \leq |\mathcal{B}_W| = q^{m(s_n-d+1)} = q^{m(\max\limits_i(s_i)-d+1)}$. According to proposition 3.12, and since $d = n-k+1$, we get $q^{\sum\limits_{i=1}^{n} s_i - m(n-k)} \leq |Gab_k(\mathbf{g}) \cap W| \leq q^{m(\max\limits_{1\leq i\leq n}(s_i)-(n-k))}$. □

One can remark that taking $s_1 = \cdots = s_n = s$ gives the following corollary, which is also a known result from [11].

Corollary 4.4 ([11])**.** *Let $Gab_k(\mathbf{g})$ be a $[n,k,d]-$Gabidulin code of length n over $\mathbb{F}_{q^m}$ and V be a $\mathbb{F}_q-$subspaces of $\mathbb{F}_{q^m}$ with dimension $s \leq m$. If $ns - m(n-k) > 0$ then,*

$$q^{ns-m(n-k)} \leq |Gab_k(\mathbf{g})_{|V}| \leq q^{m(s-(n-k))}$$

The following result is a direct consequence of Proposition 3.4, and will be useful to compute a generator matrix of a Generalized Subspace Subcode of a Gabidulin code.

Proposition 4.5. *The $q-$ary image $Gab_k(\mathbf{g})^{((B_i)_i)}$ of a Gabidulin code $Gab_k(\mathbf{g})$ with respect to the n bases $(B_1, \ldots, B_n)$ of $\mathbb{F}_{q^m}$, is generated by the block matrix $((\boldsymbol{M}_{g_j}^{q^{i-1}}))_{1\leq i\leq k, 1\leq j\leq n} \in (\mathbb{F}_q^{m\times m})^{k\times n}$ where the matrix $\boldsymbol{M}_{g_j}^T = \mathcal{M}_{B,B_j}(\theta_{g_j})$ is the matrix of the linear map $\theta_{g_j} = \phi_{B_j} \circ f_{g_j} \circ \phi_B^{-1}$ with $f_{g_j}(x) = g_j x$ for any $x \in \mathbb{F}_{q^m}$, and B being a fixed basis.*

Using the previous results and the relation between shortening and puncturing operations, we obtain the following explicit algorithm to construct a generator matrix for the generalized subspace subcodes of Gabidulin codes.

Algorithm 1 Generator matrix of $Gab_k(\mathbf{g}) \cap W$

Input A generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$ of $Gab_k(\mathbf{g})$, a set of n bases $D_1, \ldots, D_n$ of subspaces from $\mathbb{F}_{q^m}$ with dimensions respectively $s_1, \cdots, s_n \leq m$.

Output G_U generator matrix of $(Gab_k(\mathbf{g}) \cap W)^{((D_j)_j)}$

$U = \bigcup_{j=1}^{n} u_j$ such that for $1 \leq j \leq n$, $u_j = \{(j-1)m+1, \ldots, (j-1)m+s_j\}$.
Complete the families $D_1, \ldots, D_n$ into n basis $B_1, \ldots, B_n$ of $\mathbb{F}_{q^m}$
Set $\boldsymbol{Q}_j$ be the change-of-basis matrix from the basis B to the basis B_j,
Compute a generator matrix $\hat{\boldsymbol{G}}_B$ of $Gab_k(\mathbf{g})^{(B)}$
Compute a parity check matrix $\hat{\boldsymbol{H}}_B$ from $\hat{\boldsymbol{G}}_B$
Compute $\hat{\boldsymbol{H}}^B_{(B_j)_j} = \hat{\boldsymbol{H}}_B \cdot \mathrm{Diag}((\boldsymbol{Q}_1^{-1})^T, \ldots, (\boldsymbol{Q}_n^{-1})^T)$
Compute $\boldsymbol{H}_U = (\hat{\boldsymbol{H}}^B_{(B_j)_j})_{/\bar{U}}$ as a parity-check matrix of $(Gab_k(\mathbf{g}))_{|\bar{U}}$
Compute G_U, generator matrix of $(Gab_k(\mathbf{g}) \cap W)^{((D_j)_j)}$ from $\boldsymbol{H}_U$.

Algorithm 1 thus provides a practical method to explicitly generate generalized subspace subcodes.

5. Parent codes of Gabidulin RGSS codes

In the previous section, we established a close relationship between generalized subspace subcodes of Gabidulin codes and certain "parent" Gabidulin codes. We now formalize this relationship by introducing the notion of a *parent code*, which plays a key role for decoding and structural analysis. Recall that given $s = \max(s_i) \geq d$, each codeword in $Gab_k(\mathbf{g}) \cap W$ corresponds uniquely to a codeword in the Gabidulin code $\mathcal{B}_W$, which is an MRD code with parameters $[s, s-d+1, d]$ and parity-check matrix:

$$T = (\beta_j^{[m-i+1]})_{1\leq i\leq d-1,\, 1\leq j\leq s}.$$

Definition 5.1 (Parent Code)**.** *Let $W = \prod_{i=1}^{n} V_i$ be a product of $\mathbb{F}_q$-subspaces of $\mathbb{F}_{q^m}$. The Gabidulin code $\mathcal{B}_W$ defined by the parity-check matrix*

$$T = (\beta_j^{[m-i+1]})_{1\leq i\leq d-1,\, 1\leq j\leq s}$$

is called the parent code *of the generalized subspace subcode $Gab_k(\mathbf{g}) \cap W$, denoted by $P_{Gab_k(\mathbf{g})\cap W}$.*

The following proposition formalizes the linear embedding from the generalized subspace subcode into its parent code.

Proposition 5.2. *Let $Gab_k(\mathbf{g})$ be a $[n,k,d]_{q^m}$-Gabidulin code with a parity-check matrix whose first row is $\mathbf{h} = (h_1, \ldots, h_n)$. Consider subspaces V_i with dimensions $s_i \leq m$, and let $W = \prod_i V_i$. Assume bases $\mathbf{b}_i = \{\beta_1, \ldots, \beta_{s_i}\}$ form an inclusion chain, and let $\mathbf{b} = (\beta_1, \ldots, \beta_{s_n})$. Then the $\mathbb{F}_q$-linear map*

$$f_{\mathbf{b}} : W \to \mathbb{F}_{q^m}^{s_n}, \quad c = \mathbf{b}\boldsymbol{U} \mapsto h\boldsymbol{U}^T,$$

is rank-preserving, injective, and satisfies:

$$f_{\mathbf{b}}(Gab_k(\mathbf{g}) \cap W) \subseteq P_{Gab_k(\mathbf{g})\cap W}.$$

Proof. Since the vectors in $\mathbf{h}$ are linearly independent over $\mathbb{F}_q$, $\ker(f_{\mathbf{b}}) = \{0\}$. Therefore, $f_{\mathbf{b}}$ is injective and preserves the rank :

$$w_R(\mathbf{b}\boldsymbol{U}) = rank(\boldsymbol{U}) = w_R(h\boldsymbol{U}^T).$$

By construction, it follows that $f_{\mathbf{b}}(Gab_k(\mathbf{g}) \cap W) \subseteq P_{Gab_k(\mathbf{g})\cap W}$. □

Remark 5.3. *From the previous Proposition 5.2, we can also deduce that the minimum distance of d' of $Gab_k(\mathbf{g}) \cap W$ satisfies $d' \geq d$.*

In [10], the authors used this technique to make an algorithm for the encoding and decoding of the subcode on the subspace because there was no simple method to do it. Unfortunately, this method offers the same correction capacity as that of primary code. So we prefer to use the construction described in the previous section, which allows us to have a direct construction method even if we still do not have an improvement for the correction capacity.

6. Applications to cryptography

Cryptography based on rank-metric codes is a very serious alternative to reduce key sizes in code-based cryptography, because the best attacks in rank-metric are exponential with a quadratic exponent, while the best in hamming metric are exponential with a linear exponent. The goal of this section is to show that these codes are potential candidates for rank-metric cryptography in a McEliece settings. Let us recall that the general idea in a McEliece-like cryptosystems is to first choose a linear code $\mathcal{C}$ from a family of structured codes, that will serve as the secret key. The code $\mathcal{C}$ will then undergo some transformations in order to hide its structure and will result in a public code $\mathcal{C}_{pub}$ that will be published together with a correction capacity t' depending on the used transformations and the correction capacity of the secret code $\mathcal{C}$. It is well known that, faced to such a system, the attacker must either distinguish the public code from a random code, or solve and instance of the general decoding problem with a random code. Following this idea, Gabidulin, Paramonov and Tretjakov (GPT) [13] were the first to propose the use of the family of Gabidulin codes in a system today known as GPT cryptosystem. Unfortunately, a polynomial-time attack was proposed on the GPT cryptosystem and its improvements by Overbeck [27] and several other works. The weaknesses mainly come from the fact that Gabidulin codes are invariant under the Frobenius automorphism. To avoid this type of attacks, some directions have been taken, and one of them is the use of subcodes of Gabidulin codes. The latter idea was followed by Berger, Gaborit and Ruatta [4] with a system based on subcodes of $q-$ary images $Gab_k(\mathbf{g})^{(B)}$ of Gabidulin codes for a fixed basis B. The security of the system is then relied on the subcode equivalence problem [4].

According to [4] the complexity for solving the subcode equivalence problem by enumeration of Basis B is a factor of the number of $\mathbb{F}_q-$bases in $\mathbb{F}_{q^m}$. Therefore, Generalized Subspace Subcodes can be used to improve the security or the key-sizes of the cryptosystem in [4] as using GSS codes of Gabidulin codes is equivalent to base the system on subcodes of $q-$ary images $Gab_k(\mathbf{g})^{((B_j)_j)}$ of Gabidulin codes for a family of bases $B_1, \cdots, B_n$ and, in our case, the attacker must search for n bases instead of just one for solving the subcode equivalence problem by enumeration of Basis. More formally, let's consider $\boldsymbol{Q}, \boldsymbol{Q}_1, \cdots, \boldsymbol{Q}_n \in GL(q,m)$. For a $q-$ary matrix code $\mathcal{D}$ [3] we also define $\Phi_{(\boldsymbol{Q}_j)_{j=1}^n, \boldsymbol{Q}}(\mathcal{D})$ by

$$\Phi_{(\boldsymbol{Q}_j)_{j=1}^n, \boldsymbol{Q}}(\mathcal{D}) = \{(\boldsymbol{Q}_1 M_1, \cdots, \boldsymbol{Q}_n M_n)Q \mid M = M_{\phi_B^{-1}}(\mathbf{c}),\ \mathbf{c} \in \mathcal{D}\}. \tag{3}$$

Using Generalized Subspace Subcodes of Gabidulin codes in a McEliece-like cryptosystem results to the following problem.

Problem 6.1. *(Generalized Subcode equivalence on binary Image Codes, GSIC).*
Given two $q-$ary matrix codes $\mathcal{C}$ and $\mathcal{D}$, find $\boldsymbol{Q}, \boldsymbol{Q}_1, \cdots, \boldsymbol{Q}_n \in GL(q,m)$, such that $\Phi_{(\boldsymbol{Q}_j)_{j=1}^n, \boldsymbol{Q}}(\mathcal{D})$ is a subcode of $\mathcal{C}$.

One can remark that for $\boldsymbol{Q}_1 = \boldsymbol{Q}_2 = \cdots = \boldsymbol{Q}_n$, the previous problem gives rise to the SEMC problem defined in [4, Theorem 3], and shown to be NP-complete.

[3] *Here the code $\mathcal{D}$ can be viewed as included in $\mathbb{F}_q^{mn}$, but we use the term matrix code here to make connection with [4] where the codewords of $\mathcal{D}$ are viewed as matrices from $\mathbb{F}_q^{m\times n}$, and it is also the case here*

One of the best ways to solve the SEMC as shown in [4], is to enumerate the set of all $\mathbb{F}_q$-bases in $\mathbb{F}_{q^m}$ to find $\boldsymbol{Q}_1$ whereas in our case we need to find n different bases $\boldsymbol{Q}_1, \boldsymbol{Q}_2, \ldots, \boldsymbol{Q}_n$ simultaneously and, these will give a cost estimated as

$$\frac{m^n N_{q,m,n}}{m(q^m-1)} \times (n + \frac{q-1}{q})m^3 \times k'm^2(n-k)$$

instead of

$$\frac{N_{q,m,1}}{m(q^m-1)} \times (n + \frac{q-1}{q})m^3 \times k'm^2(n-k)$$

as obtained in [4], where

$$N_{q,m,n} = (\prod_{i=0}^{m-1}(q^m - q^i))^n = N_{q,m,1} \cdot (\prod_{i=0}^{m-1}(q^m - q^i))^{n-1}.$$

We emphasize that the idea of this section was not to propose a cryptosystem, because this requires a complete overview of the different existing attacks and this goes beyond the scope of this paper. However, we wanted to at least show that generalized subspace subcodes in the rank-metric deserve to be studied for their potential applications in cryptography. We see from the above that there could be a significant gain by using RGSS of Gabidulin codes in a McEliece settings compared to the system of Berger et al. [4].

7. Conclusion

In conclusion, we have generalized the notion of Subspace Subcodes in Rank metric introduced by Gabidulin and Loidreau and also characterize this family by giving an algorithm allowing to compute generator and parity-check matrices of these codes from the generator and parity-check matrices of the associated extended codes. We have also studied the specific case of generalized subspace subcodes of Gabidulin codes and show that they are applicable to cryptography in a McEliece settings.

The proposed algorithm for generating generator and parity-check matrices based on associated extended codes not only enhances the practicality of these codes but also opens avenues for further exploration and application in cryptology.

Acknowledgment: The authors are grateful to the anonymous reviewers for their thorough evaluation of the manuscript. Their insightful remarks, detailed observations, and thoughtful suggestions have greatly contributed to strengthening the presentation and improving the overall quality of this work. Herve Tale Kalachi also acknowledges the UNESCO-TWAS and the German Federal Ministry of Education and Research (BMBF) for the financial support under the SG-NAPI grant number 4500454079.

References

[1] T. P. Berger and P. Loidreau, How to mask the structure of codes for a cryptographic use, Des. Codes Cryptogr. 35(1) (2005) 63–79.
[2] T. P. Berger, C. Thiécoumba Gueye, J. Belo Klamti, Generalized subspace subcodes with application in cryptology, IEEE Trans. Inf. Theory 65(8) (2019) 4641–4657.
[3] T. P. Berger, C. Thiécoumba Gueye, J. Belo Klamti, O. Ruatta, Designing a public key cryptosystem based on quasi-cyclic subspace subcodes of Reed–Solomon codes, in: Algebra, Codes and Cryptology, Springer (2019) 97–113.
[4] T. P. Berger, P. Gaborit, O. Ruatta, Gabidulin matrix codes and their application to small ciphertext size cryptosystems, in: Indocrypt 2017, LNCS 10698, Springer (2017) 247–266.

[5] A. Couvreur, M. Lequesne, On the security of subspace subcodes of Reed–Solomon codes for public key encryption, IEEE Trans. Inf. Theory 68(1) (2021) 632–648.
[6] A. Couvreur, A. Otmani, J.-P. Tillich, Polynomial time attack on wild McEliece over quadratic extensions, IEEE Trans. Inf. Theory 63(1) (2017) 404–427.
[7] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Comb. Theory A 25(3) (1978) 226–241.
[8] I. El Qachchach, O. Habachi, J.-P. Cances, V. Meghdadi, Efficient multi-source network coding using low rank parity check code, in: IEEE WCNC 2018, IEEE (2018) 1–6.
[9] E. M. Gabidulin, Theory of codes with maximum rank distance, Problemy Peredachi Informatsii 21(1) (1985) 3–16.
[10] E. M. Gabidulin and P. Loidreau, On subcodes of codes in rank metric, in: Proc. IEEE Int. Symp. Inf. Theory (ISIT 2005), IEEE (2005) 121–123.
[11] E. M. Gabidulin and P. Loidreau, Properties of subspace subcodes of Gabidulin codes, Adv. Math. Commun. 2(2) (2008) 147–157.
[12] E. M. Gabidulin, Attacks and counter-attacks on the GPT public key cryptosystem, Des. Codes Cryptogr. 48(2) (2008) 171–177.
[13] E. M. Gabidulin, A. V. Paramonov, O. V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, in: Workshop on the Theory and Application of Cryptographic Techniques, Springer (1991) 482–489.
[14] J. K. Gibson, Severely denting the Gabidulin version of the McEliece public key cryptosystem, Des. Codes Cryptogr. 6(1) (1995) 37–45.
[15] K. Gibson, The security of the Gabidulin public key cryptosystem, in: Eurocrypt '96, LNCS 1070, Springer (1996) 212–223.
[16] M. Hattori, R. J. McEliece, G. Solomon, Subspace subcodes of Reed–Solomon codes, IEEE Trans. Inf. Theory 44(5) (1998) 1861–1880.
[17] A.-L. Horlemann-Trautmann, K. Marshall, J. Rosenthal, Extension of Overbeck's attack for Gabidulin-based cryptosystems, Des. Codes Cryptogr. 86(2) (2018) 319–340.
[18] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge Univ. Press (2003).
[19] J. M. Jensen, Subgroup subcodes, IEEE Trans. Inf. Theory 41(3) (1995) 781–785.
[20] H. T. Kalachi, On the failure of the smart approach of the GPT cryptosystem, Cryptologia 46(2) (2022) 167–182.
[21] P. Loidreau, Designing a rank metric based McEliece cryptosystem, in: Post-Quantum Cryptography (PQC 2010), LNCS 6061, Springer (2010) 142–152.
[22] H.-F. Lu, P. V. Kumar, A unified construction of space-time codes with optimal rate-diversity trade-off, IEEE Trans. Inf. Theory 51(5) (2005) 1709–1730.
[23] C. A. Melchor, N. Aragon, M. Bardet, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, ROLLO–Rank-Ouroboros, LAKE & LOCKER, NIST Competition for Post-Quantum Cryptography (2019).
[24] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, P. Gaborit, G. Zémor, Rank quasi-cyclic (RQC), NIST Competition for Post-Quantum Cryptography (2017).
[25] O. Ore, On a special class of polynomials, Trans. Amer. Math. Soc. 35(3) (1933) 559–584.
[26] A. Otmani, H. T. Kalachi, S. Ndjeya, Improved cryptanalysis of rank metric schemes based on Gabidulin codes, Des. Codes Cryptogr. 86(9) (2018) 1983–1996.
[27] R. Overbeck, A new structural attack for GPT and variants, in: Mycrypt 2005, LNCS 3715, Springer (2005) 50–63.
[28] H. Rashwan, E. M. Gabidulin, B. Honary, A Smart approach for GPT cryptosystem based on rank codes, in: IEEE Int. Symp. Inf. Theory (ISIT 2010), IEEE (2010) 2463–2467.
[29] H. Rashwan, E. M. Gabidulin, B. Honary, Security of the GPT cryptosystem and its applications to cryptography, Secur. Commun. Networks 4(8) (2011) 937–946.
[30] I. S. Reed, G. Solomon, Polynomial codes over certain finite fields, J. Soc. Indust. Appl. Math. 8(2) (1960) 300–304.
[31] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: 35th Annu. Symp. Foundations of Computer Science (FOCS 1994), IEEE (1994) 124–134.
[32] Y. Wu, On expanded cyclic and Reed–Solomon codes, IEEE Trans. Inf. Theory 57(2) (2011) 601–620.