Cardinal Rank Metric Codes over Galois Rings

Markel Epelde[a,*], Ignacio F. Rúa[b]

[a] Universidad del País Vasco - Euskal Herriko Unibertsitatea, 48940 Leioa, Bizkaia, Spain
[b] Departamento de Matemáticas, Universidad de Oviedo, 33007 Oviedo, Asturias, Spain

Abstract

In 1985, Gabidulin introduced the rank metric in coding theory over finite fields, and used this kind of of codes in a McEliece cryptosystem, six years later. In this paper, we consider rank metric codes over Galois rings. We propose a suitable metric for codes over such rings, and show its main properties. With this metric, we define Gabidulin codes over Galois rings, propose an efficient decoding algorithm for them, and hint their cryptographic application.

Keywords: Rank metric codes, Error-correcting codes, McEliece cryptosystem
2010 MSC: 11T71, 94B05

1. Introduction

The notion of error correcting codes was presented by Shannon in [11] as an effective method to improve communication through a noisy channel. Their applications, however, go beyond this. In fact, coding theory is also used for cryptographic purposes, e.g., encrypting a codeword by encoding and decoding to retrieve it, while keeping the code secret [10].

Initially, only linear subspaces over finite fields $\mathbb{F}_q$ were considered to represent codes, while the Hamming distance between codewords, i.e., the number of components in which they differ, was considered as the metric. However, in 1970, Gabidulin proposed a new family of codes [4]. These codes were also linear subspaces over finite fields, but the rank metric was considered, instead of the Hammming distance. Unfortunately, these codes are nowadays discarded for their use in the McEliece cryptosystem [5] [7].

On the other hand, the concept of linear codes has been generalized multiple times to submodules over finite rings (see [3] or [8]). Inspired by the cryptographic applications, in this paper we will define a rank metric distance over residual integer rings and define the Galois ring analogs to the Gabidulin codes. The metric can be directly connected to the cardinal of the codes considered, and so we call it *cardinal rank metric*.

In section 2 of this paper, we give a quick preview of some notions of rank metric codes. In section 3, we introduce the notion of cardinal rank metric over residual integer rings and prove some of its properties. In section 4, we define cardinal rank metric and MCRD codes, and generalizations of Gabidulin codes are presented in the final section.

2. Preliminaries

The rank metric over finite fields is defined as follows.

Definition 1 (Rank metric)**.** Let q be a power of a prime number, and $m, n \in \mathbb{N}$. The rank weight of an element $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ is defined as

$$w_{\mathcal{R}}(\boldsymbol{x}) = \operatorname{rank} \boldsymbol{x} = \dim_{\mathbb{F}_q} \langle x_1, \ldots, x_n \rangle,$$

where $\mathbb{F}_{q^m}$ is seen as an m-dimensional $\mathbb{F}_q$-vector space, and $\langle \cdot \rangle$ denotes $\mathbb{F}_q$-linear closure. Moreover, the rank distance between two elements $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ is defined as $d_{\mathcal{R}}(\boldsymbol{x}, \boldsymbol{y}) = w_{\mathcal{R}}(\boldsymbol{x} - \boldsymbol{y})$.

*Corresponding Author. Email: markel.epelde@ehu.eus

Using this definition of rank metric, Gabidulin proposed the following linear codes in [4].

Definition 2 (Gabidulin codes)**.** Let q be a power of a prime number p, $m, k, n \in \mathbb{N}$ such that $k \leq n$, and $\boldsymbol{g} \in \mathbb{F}_{q^m}^n$. The Gabidulin code of length n, dimension k and parameter $\boldsymbol{g}$ over $\mathbb{F}_{q^m}$ is defined as

$$\mathrm{Gab}_{\mathbb{F}_{q^m}}(n, k, \boldsymbol{g}) = \{(f(g_1), f(g_2), \ldots, f(g_n)) \mid f(X) \in \mathcal{P}_k(\mathbb{F}_{q^m})\},$$

where

$$\mathcal{P}_k(\mathbb{F}_{q^m}) = \left\{ \sum_{i=0}^{k-1} p_i X^{p^i} \mid p_i \in \mathbb{F}_{q^m},\ i = 0, \ldots, k-1 \right\}.$$

It can be shown that the dimension of a Gabidulin code is k. Moreover, they are in fact maximum rank distance (MRD) codes, i.e., they attain the largest minimum distance $d = n-k+1$. This implies the ability to detect up to $n-k$ rank errors and correct up to $\lfloor \frac{n-k}{2} \rfloor$. A generator matrix for the Gabidulin code $\mathrm{Gab}_{\mathbb{F}_{p^m}}(n, k, \boldsymbol{g})$ is

$$\begin{pmatrix} g_1 & g_1^p & g_1^{p^2} & \cdots & g_1^{p^{k-1}} \\ g_2 & g_2^p & g_2^{p^2} & \cdots & g_2^{p^{k-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n & g_n^p & g_n^{p^2} & \cdots & g_n^{p^{k-1}} \end{pmatrix}.$$

In the next section we generalize these concepts to a Galois ring $E = GR(p^{rh}, p^r)$, i.e., E is a degree h extension of the residual integer ring $R = \mathbb{Z}/p^r\mathbb{Z}$. In this ring, the set

$$\Gamma(E) = \{a \in R \mid a^{p^h} = a\}$$

is called the Teichmüler coordinate set of E. This set contains a complete set of representatives of additive cosets mod p, is multiplicatively closed, and it is a field isomorphic to $\mathbb{F}_{p^h}$ with respect to the usual multiplication and the addition $a \oplus b \in \Gamma(E)$ such that $\overline{a+b} = \overline{a \oplus b}$ for all $a, b \in \Gamma(E)$, where $\bar{\cdot}$ denotes the projection of E onto $E/pE \cong \mathbb{F}_{p^h}$. This set allows us to write a p-adic decomposition of the elements of E. In fact, for every $x \in E$, there exist unique $x_0, \ldots, x_{r-1} \in \Gamma(E)$ such that

$$x = x_0 + px_1 + \cdots + p^{r-1}x_{r-1}.$$

We denote each coordinate of x as $x_i = \gamma_i(x)$ for every $i = 0, \ldots, r-1$.

Since the direct product of copies of R forms an R-free module, every R-module homomorphism $f : R^m \to R^n$ can be associated with an $n \times m$ sized matrix. We will be using some properties of equivalence of matrices over R. The set of all $n \times m$ sized matrices over R will be denoted by $M_{n,m}(R)$.

Definition 3. We say two matrices $A, B \in M_{n,m}(R)$ are equivalent if they can be associated with the same R-module homomorphism $f : R^m \to R^n$.

Due to R^n and R^m being free modules, we can use change of basis matrices to prove that two matrices $A, B \in M_{n,m}(R)$ are equivalent if and only if there exist $P \in GL_n(R)$ and $Q \in GL_m(R)$ such that $B = PAQ$. It can also be proved that every matrix A is equivalent to its Smith normal form, i.e., that there exist unique $k_0, \ldots, k_{r-1} \in \mathbb{N} \cup \{0\}$ such that A is equivalent to the diagonal matrix

$$\begin{pmatrix} I_{k_0} & & & & & \\ & pI_{k_1} & & & & \\ & & p^2 I_{k_2} & & & \\ & & & \ddots & & \\ & & & & p^{r-1} I_{k_{r-1}} & \\ & & & & & \mathbf{0} \end{pmatrix}, \tag{1}$$

where $\mathbf{0}$ denotes the zero matrix of size $(n - \sum_{i=0}^{r-1} k_i) \times (m - \sum_{i=0}^{r-1} k_i)$ and I_k the $k \times k$ identity matrix.

3. Cardinal rank metric

Our definition of a rank metric over Galois rings shall generalize the concept of rank distance in codes over finite fields. We will introduce a weight function in $GR(p^{rh}, p^r)^n$ such that, if we consider $r = 1$ and compute the weight of an element, the result is exactly the same as with Definition 1. As we shall see, properties of this definition are directly connected to the cardinal of R-submodules of R^n, and so it will be called cardinal rank weight.

3.1. Cardinal rank of matrices over residual integer rings

First of all, let us define the rank weight of a matrix over R, inspired by the rank of matrices over finite fields. Let us consider a matrix $A \in M_{n,m}(R)$ and denote by $\mathcal{M}_A$ the R-submodule generated by the columns of A. As a generalization of the concept of rank over finite fields, we want $\operatorname{rank} A$ to satisfy the following properties.

($\mathcal{R}1$) Two equivalent matrices have the same rank.

($\mathcal{R}2$) The rank of A is 0 if and only if A is the zero matrix, i.e., $\operatorname{rank} A = 0$ if and only if $\mathcal{M}_A = 0$.

($\mathcal{R}3$) The rank is always non-negative, i.e., $\operatorname{rank} A \geq 0$.

($\mathcal{R}4$) The rank of a block diagonal matrix is the sum of the ranks of each block, i.e., if $\mathcal{M}_A = \mathcal{M}_B \times \mathcal{M}_C$ (where $\times$ denotes the external direct product) for some matrices B and C, then $\operatorname{rank} A = \operatorname{rank} B + \operatorname{rank} C$.

($\mathcal{R}5$) If $\mathcal{M}_A \subseteq \mathcal{M}_B$, then $\operatorname{rank} A \leq \operatorname{rank} B$.

($\mathcal{R}6$) If $\mathcal{M}_A$ is a free module of rank k, then $\operatorname{rank} A = k$.

If we want to preserve properties $(\mathcal{R}1) - (\mathcal{R}6)$, our rank function must take the following form.

Proposition 1. *Let $n, m \in \mathbb{N}$ and $\operatorname{rank} : M_{m,n}(R) \to \mathbb{R}$. Then $\operatorname{rank}(\cdot)$ satisfies properties $(\mathcal{R}1) - (\mathcal{R}6)$ if and only if there exist $0 < \lambda_{r-1} \leq \cdots \leq \lambda_1 \leq 1$ such that for any $A \in M_{m,n}(R)$ of Smith normal form (1)*

$$\operatorname{rank} A = k_0 + \sum_{i=1}^{r-1} \lambda_i k_i.$$

Proof. First, a rank satisfies $(\mathcal{R}1)$ if and only if the rank of a matrix depends only on its Smith normal form. Dividing this form into blocks, by $(\mathcal{R}4)$, the rank function has the form

$$\operatorname{rank} A = \sum_{i=0}^{r-1} \lambda_i k_i,$$

where $\lambda_i = \operatorname{rank}\left(p^i\right)$. Property $(\mathcal{R}6)$ is satisfied if and only if $\lambda_0 = 1$, and from $(\mathcal{R}2)$ and $(\mathcal{R}3)$, it follows that $\lambda_i > 0$ for every $i = 0, \ldots, r-1$. Finally, $(\mathcal{R}5)$ is true if and only if $\lambda_i \leq \lambda_{i-1}$ for every $i = 1, \ldots, r-1$. □

With these axioms in mind, we present the following rank function, in connection to the cardinal of the submodule $\mathcal{M}_A$ generated by the columns of A.

Definition 4. Let $n, m \in \mathbb{N}$ and $A \in M_{n,m}(\mathbb{Z}/p^r\mathbb{Z})$. We define the cardinal rank of A as

$$\operatorname{rank} A = \log_{p^r} |\mathcal{M}_A|.$$

In fact, this function satisfies the conditions we wanted.

Proposition 2. *The cardinal rank function from Definition 4 satisfies conditions* $(\mathcal{R}1)$-$(\mathcal{R}6)$.

Proof. Let A have the Smith normal form (1). Then, the cardinal of the module generated by the columns of the Smith normal form of A is exactly $(p^r)^{k_0}(p^{r-1})^{k_1}\dots p^{k_{r-1}}$. From Definition 4, $\operatorname{rank} A = \sum_{i=0}^{r-1} \frac{r-i}{r} k_i = k_0 + \sum_{i=1}^{r-1} \lambda_i k_i$, with $\lambda_i = \frac{r-i}{r}$, for all $i = 1, \dots, r-1$. So, because $0 \leq \lambda_r \leq \dots \leq \lambda_1 \leq 1$, we conclude that, by Proposition 1, it satisfies conditions $(\mathcal{R}1)$-$(\mathcal{R}6)$. □

Remark. With our definition of cardinal rank, the converse of $(\mathcal{R}1)$ is not true in general. Unlike the case of matrices over fields, two matrices of the same size over residual integer rings with the same rank need not be equivalent. For example, we consider the following matrices over $\mathbb{Z}/4\mathbb{Z}$

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Both A and B have the same size and rank 1. However, if A and B were equivalent, we would be able to get A by making elementary invertible transformations on the rows and columns of B, which is not true, as they are their own Smith normal forms and $A \neq B$.

Corollary 1. *Let $n, m \in \mathbb{N}$ and $A \in M_{n,m}(R)$. Then,* $\operatorname{rank} A^\top = \operatorname{rank} A$.

Proof. The cardinal rank of A is exactly the cardinal rank of its Smith normal form $S(A)$. It is straightforward that $\operatorname{rank} S(A) = \operatorname{rank} S(A)^\top$, so from $(\mathcal{R}1)$ we conclude that $\operatorname{rank} A = \operatorname{rank} A^\top$. □

Remark. As a consequence of Corollary 1, we have that Definition 4 of cardinal rank can be given in terms of columns or rows.

Let us prove the triangle inequality for the matrix cardinal rank weight.

Lemma 1. *Let $n, m \in \mathbb{N}$ and $A, B \in M_{n,m}(R)$. Then,*

$$\operatorname{rank}(A + B) \leq \operatorname{rank} A + \operatorname{rank} B.$$

Proof. Since the intersection between $\mathcal{M}_A$ and $\mathcal{M}_B$ need not be zero, we have

$$|\mathcal{M}_A + \mathcal{M}_B| \leq |\mathcal{M}_A \times \mathcal{M}_B| = |\mathcal{M}_A||\mathcal{M}_B|.$$

Moreover, since the columns of $A + B$ belong to the module $\mathcal{M}_A + \mathcal{M}_B$, it follows that $\mathcal{M}_{A+B}$ is a submodule of $\mathcal{M}_A + \mathcal{M}_B$. Hence, $|\mathcal{M}_{A+B}| \leq |\mathcal{M}_A||\mathcal{M}_B|$. Taking the logarithms yields the result. □

As a consequence of Lemma 1, the cardinal rank weight defines a distance over the matrix ring $M_{m,n}(R)$.

Theorem 1. *Let $n, m \in \mathbb{N}$ and $d : M_{n,m}(R) \times M_{n,m}(R) \to \mathbb{R}$ such that $d(A, B) = \operatorname{rank}(A - B)$. Then, d is a metric over the ring $M_{n,m}(\mathbb{Z}/p^r\mathbb{Z})$.*

Proof. Let $A, B \in M_{n,m}(R)$. First, note that the cardinal rank application is always positive or zero, so $d(A, B) \geq 0$. Moreover, $d(A, B) = 0$ if and only if $0 = \operatorname{rank}(A - B) = \log_{p^r} |\mathcal{M}_{A-B}|$, which happens if and only if $A - B = 0$. Furthermore, since -1 is a unit in the ring, $\mathcal{M}_C = \mathcal{M}_{-C}$ for all $C \in M_{m,n}(R)$, and therefore $d(A, B) = \operatorname{rank}(A - B) = \operatorname{rank}(-(A - B)) = d(B, A)$. Finally, by Lemma 1,

$$\begin{aligned} d(A, B) &= \operatorname{rank}(A - B) = \operatorname{rank}(A - C + C - B) \\ &\leq \operatorname{rank}(A - C) + \operatorname{rank}(C - B) = d(A, C) + d(C, B), \end{aligned}$$

for all $C \in M_{n,m}(R)$. □

3.2. Cardinal rank metric over Galois rings

We can extend the notion of a rank weight to n-tuples of elements of the Galois ring E. In fact, if we consider an R-basis of the free module E^n, any tuple $\boldsymbol{x} = (x_1, \dots, x_n)$ of this kind can be written as a matrix whose i-th column is given by the coordinates of x_i with respect to the chosen basis, for $i = 1, \dots, n$.

Definition 5. Let $n \in \mathbb{N}$ and $\mathcal{B}$ be a basis of the free E-module E^n, and $\boldsymbol{x} \in E^n$. We define the matrix associated to $\boldsymbol{x}$ with respect to $\mathcal{B}$, denoted $M_{\mathcal{B}}(\boldsymbol{x}) \in M_{h,n}(R)$, as the matrix formed by the coordinates $(x_{1i}, \dots, x_{hi})_{\mathcal{B}}$ of $\boldsymbol{x}$ as columns, for $i = 1, \dots, n$.

Remark. Note that, given a basis $\mathcal{B}$ of E, then the map $M_{\mathcal{B}} : E^n \to M_{h,n}(R)$ is R-linear, i.e., $M_{\mathcal{B}}(\alpha\boldsymbol{x} + \beta\boldsymbol{y}) = \alpha M_{\mathcal{B}}(\boldsymbol{x}) + \beta M_{\mathcal{B}}(\boldsymbol{x})$ for all $\alpha, \beta \in R$ and $\boldsymbol{x}, \boldsymbol{y} \in E^n$.

Using this bijection, we can easily define the following metric.

Definition 6. Let $\mathcal{B}$ be a basis of the free R-module E. Then, we define the cardinal rank of an element $\boldsymbol{x} \in E$ as $\operatorname{rank}_{\mathcal{B}} \boldsymbol{x} = \operatorname{rank} M_{\mathcal{B}}(\boldsymbol{x})$ and the cardinal rank distance $d_{\mathcal{R}} : E^n \times E^n \to \mathbb{R}$ as $d_{\mathcal{R}}^{\mathcal{B}}(\boldsymbol{x}, \boldsymbol{y}) = d(M_{\mathcal{B}}(\boldsymbol{x}), M_{\mathcal{B}}(\boldsymbol{y})) = \operatorname{rank}(\boldsymbol{x} - \boldsymbol{y})$, where d is the matrix cardinal rank distance defined in Theorem 1.

Remark 1. Note that, by Theorem 1, d is a distance, so $d_{\mathcal{R}}^{\mathcal{B}}$ is also a distance over E^n.

Theorem 2. *The cardinal rank distance $d_{\mathcal{R}}^{\mathcal{B}}$ in Definition 6 is independent of the choice of $\mathcal{B}$.*

Proof. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be two R-bases of E, and $\boldsymbol{z} = (z_1, \dots, z_n) \in E^n$. Let Q be the invertible change of basis matrix between $\mathcal{B}_1$ and $\mathcal{B}_2$. Then, for every $z_i = (z_{i1}, \dots, z_{ih})_{\mathcal{B}_1} = (z'_{i1}, \dots, z'_{ih})_{\mathcal{B}_2}$, we have

$$Q(z_{i1}, \dots, z_{ih})^\top = (z'_{i1}, \dots, z'_{ih}).$$

Thus, there exists an invertible matrix Q such that $M_{\mathcal{B}_2}(\boldsymbol{z}) = QM_{\mathcal{B}_1}(\boldsymbol{z})$. Hence, $M_{\mathcal{B}_2}(\boldsymbol{z})$ and $M_{\mathcal{B}_1}(\boldsymbol{z})$ are equivalent matrices and therefore, by $(\mathcal{R}1)$, they have the same rank, concluding that the cardinal rank of an element does not depend on the chosen basis. Moreover, if we consider $\boldsymbol{x}, \boldsymbol{y} \in E^n$, then, since both $M_{\mathcal{B}_i}$ maps are linear,

$$\begin{aligned} d_{\mathcal{R}}^{\mathcal{B}_2}(\boldsymbol{x}, \boldsymbol{y}) &= \operatorname{rank}(M_{\mathcal{B}_2}(\boldsymbol{x}) - M_{\mathcal{B}_2}(\boldsymbol{y})) = \operatorname{rank} M_{\mathcal{B}_2}(\boldsymbol{x} - \boldsymbol{y}) \\ &= \operatorname{rank} M_{\mathcal{B}_1}(\boldsymbol{x} - \boldsymbol{y}) = \operatorname{rank}(M_{\mathcal{B}_1}(\boldsymbol{x}) - M_{\mathcal{B}_1}(\boldsymbol{y})) \\ &= d_{\mathcal{R}}^{\mathcal{B}_1}(\boldsymbol{x}, \boldsymbol{y}). \end{aligned}$$

□

Notation. From now on, for the sake of simplicity, we will denote the cardinal rank of an element $\boldsymbol{x} \in E^n$ as $\operatorname{rank} \boldsymbol{x}$, and the cardinal rank distance between $\boldsymbol{x}, \boldsymbol{y} \in E^n$ as $d(\boldsymbol{x}, \boldsymbol{y})$, since they do not depend on the chosen basis of E^n. Furthermore, we will simply write a matrix associated to the element $\boldsymbol{x} \in E$ as $M(\boldsymbol{x})$, assuming we are always computing this matrix with respect to the same basis.

Comparing the cardinal rank weight we have defined with the one over finite fields, we have the following result.

Proposition 3. *The cardinal rank of an element $\boldsymbol{x} \in E$ is greater or equal than the rank of its projection $\overline{x}$ over $E/pE \cong \mathbb{F}_{p^h}$.*

Proof. Since both the ring and projection field cardinal rank metrics do not depend on the chosen basis for the corresponding space, we choose $\mathcal{B} = \{b_1, \dots b_h\}$ an R-basis for E and $\overline{\mathcal{B}}$ the corresponding $\mathbb{F}_{p^r}$-basis of $E/pE \cong \mathbb{F}_{p^{rh}}$. Then, $\overline{\lambda_1 b_1 + \cdots + \lambda_h b_h} = \overline{\lambda_1 b_1} + \cdots + \overline{\lambda_h b_h}$ for any choice of the coefficients $\lambda_1, \dots, \lambda_h \in R$. Thus, $M_{\overline{\mathcal{B}}}(\overline{\boldsymbol{x}}) = \overline{M_{\mathcal{B}}(\boldsymbol{x})}$ and therefore $\operatorname{rank} \boldsymbol{x} = \log_{p^r} |\mathcal{M}_{M_{\mathcal{B}}(\boldsymbol{x})}| \geq \log_{p^r} |\mathcal{M}_{M_{\overline{\mathcal{B}}}(\overline{\boldsymbol{x}})}| \geq \log_p |\mathcal{M}_{M_{\overline{\mathcal{B}}}(\overline{\boldsymbol{x}})}|$. This $\mathcal{M}_{M_{\overline{\mathcal{B}}}(\overline{\boldsymbol{x}})}$ submodule is actually a linear subspace, and the p-logarithm of its cardinality is exactly the rank of $\overline{\boldsymbol{x}}$ from Definition 1. □

Remark. In coding theory, given a subset $A \subseteq E^n$ one may wonder what the minimum weight of its nonzero elements is. This number is called the minimum weight of A and is denoted by $w(A)$, However, Proposition 3 does not imply that $w(A) \geq w(\overline{A})$. In fact, there may exist $\boldsymbol{x} \in A$ such that $\overline{\boldsymbol{x}} = \overline{\boldsymbol{0}}$ but $\boldsymbol{x} \neq \boldsymbol{0}$ and $\operatorname{rank} \boldsymbol{x} \leq w(\overline{A})$. We will study these properties in Section 4.1.

3.3. Comparison with other metrics

As we have seen in the previous section, defining a rank metric in E^n can be reduced to giving a rank of matrices of size $h \times n$ over R. In the literature, there have been other proposals for the definition of rank of matrices over residual integer rings R. In Section IV of [2], for instance, a rank function is given over arbitrary commutative rings. In the particular case of residual integer rings, the rank function corresponds to rank $\overline{A}$, where $\overline{A}$ denotes the matrix formed by the projections of the entries of $A \in M_{h,n}(R)$ over $R/pR \cong \mathbb{F}_p$, and rank$(\cdot)$ is the cardinal rank introduced in this paper.

Observe that this definition generalizes the usual rank over matrices over finite fields, and it verifies some of the properties given in the previous section. However, this weight does not satisfy condition $(\mathcal{R}2)$, and therefore does not define a metric $d_1(A, B) = \mathrm{rank}_1(A - B)$ over $M_{h,n}(R)$. Let us illustrate this with an example.

Example 1. We consider the following matrices over $\mathbb{Z}/4\mathbb{Z}$

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & 3 & 0 \\ 3 & 0 & 0 \end{pmatrix}.$$

Then, $d_1(A, B) = \mathrm{rank}_1(A - B) = \mathrm{rank}\, \mathbf{0} = 0$, but $A \neq B$.

This rank weight function was also proposed by Kamche and Mouaha in [8], despite noticing that it does not define a true metric. Kamche and Mouaha also propose the following matrix weight, for a matrix A with Smith normal form (1).

$$\mathrm{rank}_2\, A = \sum_{r=0}^{r-1} k_i.$$

Proposition 1 shows that this rank satisfies properties $(\mathcal{R}1)$-$(\mathcal{R}6)$, and [8] also shows that rank_2 defines a metric d_2 over E^n. However, while it does have the interesting applications shown in [8], does not seem to work as well as our proposed metric from a cryptographic point of view. In fact, let $N(k_0, \ldots, k_{r-1})$ denote the set of matrices of a fixed size $m \times n$ whose Smith normal form is (1). Then, if we consider the balls of radius $t < n$, denoted by $B(\mathbf{0}, t)$ for our metric and $B_2(\mathbf{0}, t)$ for the rank_2 metric, we have

$$B(\mathbf{0}, t) = \sum_{\substack{\mathcal{S} \leq t \\ \mathcal{S}_T \leq n}} N(k_0, \ldots, k_{r-1}) > \sum_{\mathcal{S}_T \leq t} N(k_0, \ldots, k_{r-1}) = B_2(\mathbf{0}, t),$$

where $\mathcal{S} = \sum_{r=0}^{r-1} \frac{r-i}{r} k_i$ and $\mathcal{S}_T = \sum_{r=0}^{r-1} k_i$.

This means that there exist more words in a ball of the same radius in our metric and so, in particular, there exist more words of low weight in E^n with the rank from Definition 6 than with the rank_2 of [8]. In the same line of thought as [4], this might suggest that the cardinal rank decoding problem might be more difficult in our setting, than with the rank_2 metric, because the number of potential supports of a bounded size is bigger. On the other hand, specific structural attacks for this kind of cardinal rank metric codes might weaken a McEliece-cryptosystem based on them. The existence of this kind of attacks is far beyond the scope of this paper, and we leave it as future work.

Moreover, the cardinal rank metric satisfies that, besides $(\mathcal{R}5)$, if $\mathcal{M}_A \subsetneq \mathcal{M}_B$, then $\mathrm{rank}\, A < \mathrm{rank}\, B$, from the strictly decreasing choices for λ_i's in Proposition 1.

Finally, we compare this rank with the Hamming weight over E^n. If we count the number of words in E^n of weight t, it results in a total of $\binom{n}{t}(p^{rh} - 1)$ words. This is the result of choosing the nonzero position of the words and the elements in E that can fill the rest of the components, i.e., the number of nonzero elements of E. With our metric, we observe that the number of elements of rank t is

$$\sum_{\mathcal{S}=t} N(k_0, \ldots k_{r-1}).$$

Since a concrete expression of this number is cumbersome, we will give a bound for $N(t, 0, \ldots, 0)$, which is, by Proposition 1, part of the sum for any rank metric over E^n satisfying conditions $(\mathcal{R}1)$-$(\mathcal{R}6)$.

h	d	$\lvert B(0,d)\rvert$	$\lvert B_2(0,d)\rvert$	$\lvert B_H(0,d)\rvert$
2	0	1	1	1
	1	88	82	31
	2	268	202	241
3	0	1	1	1
	1	400	358	127
	2	4152	3186	4033
4	0	1	1	1
	1	1696	1486	511
	2	65776	55906	65281

h	d	$\lvert B(0,d)\rvert$	$\lvert B_2(0,d)\rvert$	$\lvert B_H(0,d)\rvert$
5	1	1	1	1
	1	6976	6046	2047
	2	1049568	961218	1047553
6	1	1	1	1
	1	28288	24382	8191
	2	16781248	16035202	16773121
7	1	1	1	1
	1	113920	97918	32767
	2	268451712	262322946	268419073

Table 1: A comparison of the balls of different metrics for extensions of degree h of $\mathbb{Z}/4\mathbb{Z}$. Here, $B_H(0,d)$ denotes the ball of radius d with the Hamming metric.

In order to fix the elements $\boldsymbol{x}_1,\dots,\boldsymbol{x}_n \in E$ of A, let us choose first a free module $\mathcal{M}_A$ of rank t. There are exactly $\begin{bmatrix} n \\ t \end{bmatrix}_p$ ways to fix the projection $\overline{\mathcal{M}_A} \cong \mathbb{F}_p^t$, where $\begin{bmatrix} n \\ t \end{bmatrix}_p$ denotes the Gaussian binomial coefficient. In order to fix $\overline{\boldsymbol{x}_1},\dots,\overline{\boldsymbol{x}_t}$, we compute the number of possible ordered bases for $\mathbb{F}_p^t$, which is $P = \prod_{i=1}^{t-1}(p^t - p^i)$. Besides, once fixed $\overline{\boldsymbol{x}_i}$, we can choose $\boldsymbol{x}_i$ in $p^{(r-1)h}$ different ways, which gives us a total of

$$p^{(r-1)ht} P \begin{bmatrix} n \\ t \end{bmatrix}_p$$

possible ordered choices for the linearly independent columns of A. If we add $n-t$ dependent columns in $\mathcal{M}_A$ to fill A and take into account the $\binom{n}{t}$ possible choices for the free columns of A, there are more than

$$p^{(r-1)ht} \binom{n}{t} \begin{bmatrix} n \\ t \end{bmatrix}_p P$$

possible elections for A, which is a way larger number than the result obtained with the Hamming weight.

A comparison of the cardinal of the balls of our cardinal rank metric with those of the metrics mentioned in this section can be seen in Table 1, for $n = 2$ and different extensions of $\mathbb{Z}/4\mathbb{Z}$. As we have mentioned, computations for higher values of n are tricky, but the difference between the metrics is bigger when n is a larger number.

Summarizing, from a cryptographic point of view, the cardinal rank might yield harder instances of the syndrome decoding problem than with the other metrics mentioned in this section. However, as mentioned, the actual security of those cryptographic schemes is yet to be proven and is left for future work.

4. Cardinal rank metric codes over Galois rings

4.1. Definition and properties

Let us begin this section with a simple definition of cardinal rank metric codes over E^n.

Definition 7. Let $n \in \mathbb{N}$. A cardinal rank metric code $\mathcal{C}$ of length n over a Galois ring E is a submodule of the E-module E^n. If this submodule is free, then $\mathcal{C}$ is said to be a free cardinal rank metric code.

As with linear rank metric codes over $\mathbb{F}_{q^h}$, we can just take the minimum rank of codewords, as the minimum distance of the code.

Lemma 2. *Let $\mathcal{C}$ be a cardinal rank distance code over a Galois ring. Then, its minimum distance $d(\mathcal{C})$ satisfies*

$$d(\mathcal{C}) = \min_{\boldsymbol{x} \in \mathcal{C} \setminus \{\boldsymbol{0}\}} \operatorname{rank} \boldsymbol{x}.$$

Proof. It is straightforward. In fact,

$$\begin{aligned} d(\mathcal{C}) &= \min\{d_{\mathcal{R}}(\boldsymbol{x},\boldsymbol{y}) \mid \boldsymbol{x},\boldsymbol{y}\in\mathcal{C}, \boldsymbol{x}\neq\boldsymbol{y}\} \\ &= \min\{\operatorname{rank}(\boldsymbol{x}-\boldsymbol{y}) \mid \boldsymbol{x},\boldsymbol{y}\in\mathcal{C}, \boldsymbol{x}\neq\boldsymbol{y}\} \\ &= \min_{\boldsymbol{x}\neq 0, \boldsymbol{x}\in\mathcal{C}} \operatorname{rank}\boldsymbol{x}. \end{aligned}$$

□

In order to give a proper bound to the minimum distance of cardinal rank metric codes, we prove the following lemmas.

Lemma 3. *Let $U=\{u_i\}_{i=1}^k \subseteq E^n$ be a linearly independent set over E and $M=\langle u \mid u\in U\rangle$ the linear E-closure of U. Then, $M\cap(p^j)=\langle p^j u \mid u\in U\rangle$ for all $j\in\mathbb{N}\cup\{0\}$, where $(p^j)=(p^jE)^n$.*

Proof. The inclusion $\langle p^j u_1,\dots p^j u_k\rangle \subseteq M\cap(p^j)$ is straightforward. Let us prove the converse. Let $\{u_1,\dots,u_k,u_{k+1},\dots,u_n\}$ be a basis of the free E-module E^n. Observe that the extension of U to an E-basis of E^n can be done via Nakayama's lemma, since E is a local ring. Note that if we take an element u of $M\cap(p^j)$, then u can be written as both $p^j\lambda_1u_1+\dots p^j\lambda_nu_n\in(p^j)$ and $\mu_1u_1+\dots\mu_nu_k\in M$, for some $\lambda_1,\dots,\lambda_n,\mu_1,\dots,\mu_k\in E$. Since $\{u_i\}_{i=1}^n$ is a basis, then the coefficients must coincide, and u can be written as

$$u=p^j\lambda_1u_1+\dots p^j\lambda_nu_k\in\langle p^ju_1,\dots p^ju_k\rangle.$$

□

As proved in [1], every E-submodule C of E^n can be written as a direct sum of submodules of the type p^iC_i, where C_i is free. In fact, if we write a generator system of C as the rows of a matrix in a certain order, one can apply Gaussian-like elimination to reduce it to the form $\tilde{G}=\begin{pmatrix}G\\0\end{pmatrix}P$, where P is a permutation matrix,

$$G=\begin{pmatrix} I_{k_0} & C_{0,1} & C_{0,2} & \dots & C_{0,k_{r-2}} & C_{0,k_{r-1}} \\ 0 & pI_{k_1} & pC_{1,2} & \dots & pC_{1,k_{r-2}} & pC_{1,k_{r-1}} \\ 0 & 0 & p^2I_{k_2} & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ddots & p^{r-3}C_{k_{r-3},k_{r-2}} & p^{r-3}C_{k_{r-3},k_{r-1}} \\ \vdots & \vdots & \vdots & \ddots & p^{r-2}I_{k_{r-2}} & p^{r-2}C_{k_{r-2},k_{r-1}} \\ 0 & 0 & 0 & \dots & 0 & p^{r-1}I_{k_{r-1}} \end{pmatrix}, \tag{2}$$

and $|M|=\sum_{i=0}^{r-1}p^{h(r-i)k_i}$. Therefore, C can be written as $\bigoplus_{i=0}^{r-1}p^iC_i$, where each C_i is minimally generated by the corresponding k_i rows of $\tilde{G}$, i.e., k_i is the minimum amount of elements needed to generate C_i. By looking at G, one can also tell that $\bigoplus_{i=0}^{r-1}C_i$ is a free module of rank $k=\sum_{i=0}^{r-1}k_i$. If C is an code over E, GP is said to be a generator matrix of C, i.e. $C=\{(GP)^\top\boldsymbol{x}\mid\boldsymbol{x}\in E^k\}$ (observe that the final rows of $\tilde{G}$ are not needed to generate C). Alternatively, G is called a generator matrix in systematic form of a permutation equivalent code of C.

Lemma 4. *Let $C\subseteq E^n$ be an E-module such that $C=\bigoplus_{i=0}^{r-1}C_i$, where C_i is generated by a minimal generator system $\{p^iu_j^{(i)}\}_{j=1}^{k_i}$ and $U=\{u_j^{(i)}\mid j=1,\dots,k_i,\ i=0,\dots,r-1\}$ is a linearly independent set. Then, the ideal $C\cap(p^{r-1})$ is a $\Gamma(E)$-vector space with basis $\{p^{r-1}u\mid u\in U\}$, and is isomorphic to $\overline{C'}$, where $C'=\langle u\mid u\in U\rangle$.*

Proof. Observe that the E-module $C\cap(p^{r-1})$ can be seen simply as a $\Gamma(E)$-linear space, since for any $\lambda\in E$ there exists $\lambda'\in\Gamma(E)$ such that $\lambda p^{r-1}\boldsymbol{x}=\lambda'p^{r-1}\boldsymbol{x}$. We now check that $\mathcal{B}=\{p^{r-1}u\mid u\in U\}$ is a basis of this $\Gamma(E)$-space. By Lemma 3, $\langle b\mid b\in\mathcal{B}\rangle=C'\cap(p^{r-1})$, so every generator of $C'\cap(p^{r-1})$ belongs to C. Since C is a subspace of C', it follows that $\mathcal{B}$ is also a generator system for $C\cap(p^{r-1})$. Moreover, let $\sum_{u\in U}\lambda_u(p^{r-1}u)=0$ for some values of $\lambda_u\in\Gamma(E)$. Since U is a basis of C', it follows that

$p^{r-1}\lambda_u = 0$ and therefore $\lambda_u \in (p)$. Since we have chosen the λ_u's to lie in $\Gamma(E)$, we conclude that $\lambda_u = 0$ for all $u \in U$.

On the other hand, for every $\boldsymbol{x} \in C \cap (p^{r-1})$, there exists $\boldsymbol{x}' \in \Gamma(E)^n$ such that $\boldsymbol{x} = p^{r-1}\boldsymbol{x}'$. In fact, this $\boldsymbol{x}'$ is unique since, if $\boldsymbol{x} = p^{r-1}\boldsymbol{x}' = p^{r-1}\boldsymbol{x}''$ for an $\boldsymbol{x}'' \in \Gamma(E)^n$, then $\boldsymbol{x} \equiv \boldsymbol{y} \bmod p$, which implies $\boldsymbol{x}' = \boldsymbol{x}''$. Hence, the application $\varphi : C \cap (p^{r-1}) \to \overline{C'}$ given by $\varphi(p^{r-1}\boldsymbol{x}) = \overline{\boldsymbol{x}}$ is well-defined. Moreover, it is easy to check that φ is a $\Gamma(E) \cong \mathbb{F}_p^h$-linear space isomorphism. In fact, the sum in p^{r-1}) works identically to the sum mod p in $\overline{C'}$, and so does the external product by $\Gamma(E) \cong \mathbb{F}_{p^h}$. □

Theorem 3 (Singleton-like bound)**.** *Let $n, k \in \mathbb{N}$ such that $k \leq n$ and $\mathcal{C} \subseteq E^n$ be a cardinal rank metric code generated by $G \in M_{k,n}(E)$. Then,*

$$d(\mathcal{C}) \leq \frac{n-k+1}{r}.$$

Moreover, $d(\mathcal{C}) = \frac{d(\overline{\mathcal{C}'})}{r}$, where $\overline{\mathcal{C}'}$ is the linear code of the previous lemma.

Proof. We will prove the lemma for a code $\mathcal{C}$ with generator matrix in systematic form (2), where $\sum_{i=0}^{r-1} k_i = k$. This type of generator matrix can always be obtained with permutations in the columns without altering the minimum distance of the generated code.

By Lemma 2, there exists $\boldsymbol{x} \in \mathcal{C}$ a nonzero codeword such that $\operatorname{rank} \boldsymbol{x} = d(\mathcal{C})$. Note that $p\boldsymbol{x}$ is also a codeword in $\mathcal{C}$, but

$$\operatorname{rank} p\boldsymbol{x} = \log_{p^r} |\langle px_1, \ldots, px_n \rangle| < \log_{p^r} |\langle x_1, \ldots, x_n \rangle| = \operatorname{rank} \boldsymbol{x}.$$

By the election of $\boldsymbol{x}$, this is only possible if $p\boldsymbol{x} = \boldsymbol{0}$, which means $\boldsymbol{x} \in (p^{r-1}) \cap \mathcal{C}$. This space, by Lemma 4, is isomorphic as a $\Gamma(E)$-module to the linear code $\overline{\mathcal{C}'}$ generated by

$$\overline{G'} = \begin{pmatrix} \overline{I_{k_0}} & \overline{C_{0,1}} & \overline{C_{0,2}} & \cdots & \overline{C_{0,k-2}} & \overline{C_{0,k_{r-1}}} \\ \overline{0} & \overline{I_{k_1}} & \overline{C_{1,2}} & \cdots & \overline{C_{1,k_{r-2}}} & \overline{C_{1,k_{r-1}}} \\ \overline{0} & \overline{0} & \overline{I_{k_2}} & \ddots & \vdots & \vdots \\ \overline{0} & \overline{0} & \overline{0} & \ddots & \overline{C_{k_{r-3},k_{r-2}}} & \overline{C_{k_{r-3},k_{r-1}}} \\ \vdots & \vdots & \vdots & \ddots & \overline{I_{k_{r-2}}} & \overline{C_{k_{r-2},k_{r-1}}} \\ \overline{0} & \overline{0} & \overline{0} & \cdots & \overline{0} & \overline{p^{r-1}I_{k_{r-1}}} \end{pmatrix},$$

If $\boldsymbol{x} = p^{r-1}\boldsymbol{y}$ is the word of minimum weight, then $\overline{\boldsymbol{y}}$ must be the word of minimum weight in $\overline{\mathcal{C}'}$, so $|\langle x_1, \ldots x_n \rangle| = |\langle \overline{y}_1, \ldots \overline{y}_n \rangle| = p^{d(\overline{\mathcal{C}'})}$, which by the Singleton bound implies $\operatorname{rank} \boldsymbol{x} = \frac{d(\overline{\mathcal{C}'})}{r} \leq \frac{n-k+1}{r}$. □

Corollary 2. *Let $\mathcal{C}$ and $\tilde{\mathcal{C}}$ be two codes of length n over E. If $\mathcal{C} \cap (p^{r-1}) = \tilde{\mathcal{C}} \cap (p^{r-1})$, then $d(\mathcal{C}) = d(\tilde{\mathcal{C}})$. In particular, $d(\mathcal{C}) = d(\mathcal{C}') = d(\mathcal{C} \cap (p^{r-1}))$.*

Let us define the equivalent notion, in our cardinal rank metric, to MRD codes over Galois rings.

Definition 8 (MCRD codes)**.** Cardinal rank metric codes $\mathcal{C}$ of length n over and generator matrix $G \in M_{k,n}(E)$ which satisfy $d(\mathcal{C}) = \frac{n-k+1}{r}$ are called *Maximum Cardinal Rank Distance (MCRD) codes.*

As a consequence of Theorem 3, we have the following result on MCRD codes.

Corollary 3. *Let $\mathcal{C} \subseteq E^n$ be a free code of rank k. Then, $d(\mathcal{C}) = \frac{d(\overline{\mathcal{C}})}{r} \leq \frac{n-k+1}{r}$. Moreover, $\mathcal{C}$ is MCRD if and only if $\overline{\mathcal{C}}$ is MRD.*

Proof. By Lemma 4, $\mathcal{C}$ being a free code implies $\mathcal{C}' = \mathcal{C}$. Because of this, $\overline{\mathcal{C}}$ has dimension k and, by Theorem 3, $d(\mathcal{C}) = \frac{n-k+1}{r}$ if and only if $d(\overline{C}) = n - k + 1$, which proves the result. □

When $\mathcal{C}$ is not free, there is no general relation between $\overline{\mathcal{C}}$ being MRD and $\mathcal{C}$ being MCRD. This is due to the loss of minimum weight codewords when projecting to $\mathbb{F}_q^n$.

5. Gabidulin codes

5.1. Definition and properties

In order to define Gabidulin codes over Galois rings, let us introduce the family of linearized polynomials over E.

Definition 9. Let $E = GR(p^{rh}, p^r)$ be an extension of the Galois ring $R = \mathbb{Z}/p^r\mathbb{Z}$ and $\tau \in \mathrm{Aut}(E \mid R)$ an automorphism of E fixing R. The elements of the set $\mathcal{P}_t(\tau, E) = \left\{\sum_{i=0}^{t-1} f_i \tau^i(X) \mid f_i \in E, i = 0, \ldots, n\right\}$ are said to be the the linearized polynomials of degree lower than t over E with respect to τ. We will denote by $\mathcal{P}_t^*(\tau, E)$ the set of monic linearized polynomials of degree $t-1$ over E, i.e.,

$$\mathcal{P}_t^*(\tau, E) = \{f(X) + \tau^{t-1}(X) \mid f \in \mathcal{P}_{t-1}(\tau, E))\}.$$

Remark. With the notation of the previous definition, the group of automorphisms $\mathrm{Aut}(E \mid R)$ is a cyclic group generated by the generalization of the Frobenius automorphism of the field extension $\mathbb{F}_{p^h} \mid \mathbb{F}_p$. Namely,

$$\tau(x) = \gamma_0(x)^p + p\gamma_1(x)^p + \cdots + p^{r-1}\gamma_{r-1}(x)^p.$$

In fact, the i-th power of τ is precisely

$$\tau^i(x) = \gamma_0(x)^{p^i} + p\gamma_1(x)^{p^i} + \cdots + p^{r-1}\gamma_{r-1}(x)^{p^i}.$$

From now on, we will work with the Frobenius-like automorphism τ, and for simplicity, we will simply write $\mathcal{P}_t(E)$ ($\mathcal{P}_t^*(E)$) to denote the (monic) linearized polynomials with respect to τ.

Now, we are ready to define the Gabidulin codes in our context.

Definition 10 (Gabidulin codes over Galois rings)**.** Let $n, k, p, r, h \in \mathbb{N}$ be such that p is prime and $k \leq n$. Let $\boldsymbol{g} = (g_1, \ldots, g_n) \in E = GR(p^{rh}, p^r)^n$ such that its components are $\mathbb{Z}/p^r\mathbb{Z}$-linearly independent. We define the set

$$\mathrm{Gab}_E(n, k, \boldsymbol{g}) = \{(f(g_1), \ldots, f(g_n)) \mid f \in \mathcal{P}_k(E)\}$$

as the *E-Gabidulin code of length n and parameters $\boldsymbol{g}$ and k.*

As generalizations of the usual Gabidulin codes, the first thing we note is that their projections over the corresponding finite fields are actually classic Gabidulin codes.

Lemma 5. *The projection over $\mathbb{F}_{p^h}^n$ of the $GR(p^{rh}, p^r)$-Gabidulin code $\mathrm{Gab}_E(n, k, \boldsymbol{g})$ is the $\mathbb{F}_{p^h}$-Gabidulin code $\mathrm{Gab}_{\mathbb{F}_{p^h}}(n, k, \overline{\boldsymbol{g}})$.*

Proof. The proof is straightforward. In fact, note that for any $i \in \mathbb{N}$ and $x \in E = GR(p^{rh}, p^r)$,

$$\overline{\tau^i(x)} = \overline{x}^{p^i}.$$

Therefore, since the components of $\overline{g}$ are also $\mathbb{Z}/p\mathbb{Z}$-linearly independent,

$$\overline{\mathrm{Gab}_E(n, k, \boldsymbol{g})} = = \{(f(\overline{g_1}), \ldots, f(\overline{g_n})) \mid f \in \mathcal{P}_k(\overline{E})\} = \mathrm{Gab}_{\mathbb{F}_{p^h}}(n, k, \overline{\boldsymbol{g}}),$$

which is, by definition, the Gabidulin code of length n, parameter $\overline{\boldsymbol{g}}$ and dimension k over $\mathbb{F}_{p^h}$. □

Now, let us give a generator matrix for the code.

Proposition 4. *Let $E = GR(p^{rh}, p^r)$ and let $\mathcal{C} = \mathrm{Gab}_E(n, k, \boldsymbol{g})$ be an E-Gabidulin code. Then, $|\mathcal{C}| = p^{rhk}$ and a generator matrix for $\mathcal{C}$ is*

$$G = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ \tau(g_1) & \tau(g_2) & \cdots & \tau(g_n) \\ \tau^2(g_1) & \tau^2(g_2) & \cdots & \tau^2(g_n) \\ \vdots & \vdots & \cdots & \vdots \\ \tau^{k-1}(g_1) & \tau^{k-1}(g_2) & \cdots & \tau^{k-1}(g_n) \end{pmatrix}.$$

Proof. It is straightforward, by the definition of $\mathcal{P}_t(E)$, that

$$\mathcal{C} = \{G^\top \boldsymbol{x} \mid \boldsymbol{x} \in E^k\}.$$

Moreover, note that the projection of G over $\mathbb{K} = \mathbb{F}_{p^h}$ is a generator matrix for $\mathrm{Gab}_{\mathbb{K}}(n, k, \overline{g})$, which has dimension k. Thus, the k columns of $\overline{G}$ are linearly independent over $\mathbb{K}$, and therefore the columns of G are also E-free, generating a code of cardinality $(p^{rh})^k$. □

Next, we observe that Gabidulin codes over rings generalize the distance properties of their classic counterparts.

Theorem 4. *The minimum distance of a Gabidulin code $\mathcal{C} = \mathrm{Gab}_E(n, k, \boldsymbol{g})$ is $d(\mathcal{C}) = \frac{n-k+1}{r}$.*

Proof. Note that, by Corollary 3, $\mathcal{C}$ is MCRD if and only if $\overline{\mathcal{C}}$ is MRD, which by Lemma 5 we know it is the case of a classic MRD Gabidulin code. We conclude that $d(\mathcal{C}) = \frac{n-k+1}{r}$. □

Regarding the error correction capability, we conclude the following result.

Corollary 4. *Let $\mathcal{C} = \mathrm{Gab}_E(n, k, \boldsymbol{g})$ be an E-Gabidulin code. Then, $\mathcal{C}$ can detect errors of* $\mathrm{rank} \leq \frac{n-k}{r}$ *and correct errors of* $\mathrm{rank} \leq \frac{n-k}{2r}$.

Proof. Let $\boldsymbol{x} \in \mathcal{C}$. If $\mathrm{rank}\, \boldsymbol{e} < \frac{n-k+1}{r} = d(\mathcal{C})$, it follows that the distance from $\boldsymbol{x} + \boldsymbol{e}$ to $\boldsymbol{x}$ verifies

$$d(\boldsymbol{x} + \boldsymbol{e}, \boldsymbol{x}) = \mathrm{rank}(\boldsymbol{e}) < d(\mathcal{C}).$$

Moreover, if $\mathrm{rank}\, \boldsymbol{e} < d(\mathcal{C})/2$, we assume there exist $\boldsymbol{e}'$ of weight also under $d(\mathcal{C})/2$ and $\boldsymbol{x}' \in \mathcal{C}$ such that $\boldsymbol{x} + \boldsymbol{e} = \boldsymbol{x}' + \boldsymbol{e}'$. In that case,

$$\begin{aligned} d(\boldsymbol{x}, \boldsymbol{x}') &\leq d(\boldsymbol{x}, \boldsymbol{x} + \boldsymbol{e}) + d(\boldsymbol{x} + \boldsymbol{e}, \boldsymbol{x}') \\ &= d(\boldsymbol{x}, \boldsymbol{x} + \boldsymbol{e}) + d(\boldsymbol{x}' + \boldsymbol{e}', \boldsymbol{x}') = \mathrm{rank}\, \boldsymbol{e} + \mathrm{rank}\, \boldsymbol{e}' \\ &< d(C), \end{aligned}$$

which is a contradiction. □

Corollary 5. *For all values of n, k such that $k \leq n \leq h$, there exists a MCRD code over E of cardinality p^{rhk} and length n.*

Proof. If $k \leq n \leq h$, we can choose n R-linearly independent elements in E to form $\boldsymbol{g}$. Moreover, since $k \leq n$, there exists a subcode $\mathrm{Gab}_E(n, k, \boldsymbol{g})$ of E^n with p^{rhk} elements, which is MCRD by Theorem 4. □

5.2. Decoding algorithm

Similar to the decoding methodology of usual Gabidulin codes, a decoding algorithm can be found over Galois rings. Following the reduction process in [9], we introduce two related problems and reduce the decoding problem to solving a linear system of equations.

In this section we will work with fixed Galois rings E and R. We will work with parameters $\boldsymbol{y}, \boldsymbol{g} \in E^n$ and $k \leq n$ assuming there exists $\boldsymbol{x} \in \mathrm{Gab}_E(n, k, \boldsymbol{g})$ satisfying $\mathrm{rank}(\boldsymbol{y} - \boldsymbol{x}) \leq t = \frac{n-k}{2r}$, i.e., there exists $f \in \mathcal{P}_k(E)$ such that

$$\mathrm{rank}(\boldsymbol{y} - (f(g_1), \ldots, f(g_n))) \leq t.$$

Notation. For simplicity, in this section we will use bold letters to denote the tuple formed by the evaluation of the function in each component, e.g., $\boldsymbol{f}(\boldsymbol{g})$ will denote $(f(g_1), \ldots f(g_n))$.

We define the Gabidulin Decoding Problem as follows.

Definition 11 (Gabidulin Decoding Problem)**.** The Gabidulin Decoding Problem $\mathrm{GDP}(\boldsymbol{y}, \boldsymbol{g}, k)$ consists in, given arguments $\boldsymbol{y}$, $\boldsymbol{g}$ and k, finding $\boldsymbol{x} \in \mathrm{Gab}_E(n, k, \boldsymbol{g})$ with $\mathrm{rank}(\boldsymbol{y} - \boldsymbol{x}) \leq \frac{n-k}{2r}$.

We also introduce the following problem.

Definition 12 (First Reconstruction Problem)**.** The First Reconstruction Problem FRP($\boldsymbol{y}, \boldsymbol{g}, k$) consists in finding $(V, q) \in \mathcal{P}^*_{\lfloor rt \rfloor+1}(E) \times \mathcal{P}_k(E)$ such that $\boldsymbol{V}(\boldsymbol{y}) = \boldsymbol{V}(\boldsymbol{q}(\boldsymbol{g}))$.

We want to reduce the GDP to the FRP, so let us prove the following two lemmas.

Lemma 6. *Let $f \in \mathcal{P}_k(E)$ be a nonzero linearized polynomial, $\{m_1, \ldots, m_n\} \subseteq E$ be a linearly independent set over R, and $M = \langle m_1, \ldots, m_n \rangle$. Then,*

(i) A bound for the cardinal of the kernel of f in M is

$$|\operatorname{Ker} f \cap M| \leq (p^r)^{n - \frac{r-j}{r}(n-k+1)},$$

where $p^j | f(X)$ but $p^{j+1} \nmid f(X)$. In particular,

$$|\operatorname{Ker} f \cap M| \leq (p^r)^{n - \frac{1}{r}(n-k+1)}.$$

(ii) There exists $F \in \mathcal{P}^*_{n+1}(E)$ such that $\operatorname{Ker} F = M$.

Proof. Let us begin with part (i). Since p^j divides every coefficient of f, we may write the image of an element $x \in E$ as

$$f(x) = \sum_{i=0}^{k-1} p^j f_i'(x_0^{p^i} + p x_1^{p^i} + \cdots + p^{r-j-1} x_{r-j-1}^{p^i}),$$

where $f_i' \in E$ for all $i = 0, \ldots, k-1$, $x_i = \gamma_i(x)$ for all $i = 0, \ldots, r-j-1$, and there exists $i_0 \in \{0, \ldots, k-1\}$ where f_{i_0}' is a unit. Moreover, if we set $f'(X) = \sum_{i=0}^{k-1} f_i' \tau^i(X)$, then x is a zero of f if and only if $f'(x) \equiv 0 \mod p^{r-j}$, which happens if and only if

$$f'(x) \equiv 0 \pmod{p^s} \tag{3}$$

for all $s = 1, \ldots, r-j$. Observe that, since p does not divide f', it follows that $f' \neq 0$ modulo p^s for any $s = 1, \ldots, r-j$.

If we consider (3) with $s = 1$, observe that $f'(X)$ is a nonzero polynomial modulo p^s with degree at most p^{k-1}. Hence, if we want x to be a root of f, $x_0 \in \Gamma(E)$ can take at most p^{k-1} possible values. Moreover, we have that $f'(x_0)$ must belong to the ideal (p), so there exists $c_0 \in E$ such that $f'(x_0) = pc_0$.

Suppose now, by induction, that for a $s \in \{1, \ldots, r-j-1\}$ there are p^{k-1} options to choose x_{s-1} in order x to satisfy (3), and that there exists $c_{s-1} \in E$ such that $f'(x_0 + px_1 + \cdots + p^{s-1}x_{s-1}) = p^s c_{s-1}$.

Then, considering Equation 3 again for $s+1$, it follows that $f'(x_0 + px_1 + \cdots + p^s x_s)$ must belong to (p^{s+1}). Due to the linearity of f' and the induction hypothesis, expression (3) (for $s+1$) can be written as

$$p^s(c_{s-1} + f'(x_s)) \equiv 0 \pmod{p^{s+1}},$$

which means in fact that $c_{s-1} + f'(x_s)$ must belong to (p). But again, since $f'(X)$ is not zero modulo p, $c_{s-1} + f'(X)$ is a nonzero polynomial of degree p^{k-1} modulo p and x_s must be a root of $c_{s-1} + f'(X)$ mod p, which means we have up to p^{k-1} options to choose x_s. Moreover, there exists a $c_s \in E$ such that $f'(x_0 + px_1 + \cdots + p^{s+1}x_s) = p^{s+1}c_s$.

Hence, we have at most $(p^{k-1})^{r-j}$ options to choose $(x_1, \ldots, x_{r-j-1})$.

Now, let $z, z' \in M$ be two zeros of f. Then they can be written as $z = z_0 + p^{r-j}z_1$ and $z' = z_0' + p^{r-j}z_1'$ where $z_0, z_0' \notin (p^{r-j})$. Note that if $z_0 = z_0'$ then $z - z' = p^{r-j}(z_1 - z_1')$ belongs to both (p^{r-j}) and M, so there exists $m \in M$ such that $z = z' + m$. By Lemma 3, $M \cap (p^{r-j}) = \langle p^{r-j}u_1, \ldots, p^{r-j}u_n \rangle$, with cardinality p^{jn}. Summing up, once chosen $(x_0, \ldots, x_{r-j-1})$, there are exactly p^{jn} options for completing the p-adic expression of x. We conclude that an upper bound for the zeros of f in M is (since f is nonzero, we must take $j = r-1$)

$$|M \cap \operatorname{Ker} f| \leq p^{(k-1)(r-j)+nj} \leq p^{nr-(n-k+1)}.$$

Part (ii) can be proved by induction on n. Let $n = 1$. Since m_1 is linearly independent, $p \nmid m_1$ and the linearized polynomial

$$F_1(X) = \tau(X) - \tau(m_1)m_1^{-1}\tau^0(X) \in \mathcal{P}^*_2(E)$$

satisfies $\operatorname{Ker} F_1 = \langle m_1 \rangle$.

Suppose now that there exists $F_{n-1}(X) \in \mathcal{P}_n^*(X)$ such that $\operatorname{Ker} F_{n-1} = \langle m_1, \ldots, m_{n-1} \rangle$. Note that if $p^{r-1}F_{n-1}(m_n) = 0$, then $F_{n-1}(p^{r-1}m_n) = 0$ and therefore by Lemma 4 $p^{r-1}m_n \in \langle m_1, \ldots, m_{n-1} \rangle$, which is a contradiction because the set $\{m_1, \ldots, m_n\}$ is linearly independent. Thus, p does not divide $F_{n-1}(m_n)$ and the latter is a unit. We conclude that the linearized polynomial

$$\begin{aligned} F_n(X) &= (\tau - \tau(F_{n-1}(m_n))F_{n-1}(m_n)^{-1}\tau^0) \circ F_{n-1})(X) \\ &= \tau(F_{n-1}(X)) - \tau(F_{n-1}(m_n))F_{n-1}(m_n)^{-1}F_{n-1}(X) \end{aligned}$$

has $\operatorname{Ker} F_n = M$. □

Theorem 5. *Let $\mathrm{Gab}_E(n, k, \boldsymbol{g})$ be a Gabidulin code and $\boldsymbol{y} \in E^n$ a decodable word. In this case, the Gabidulin Decoding Problem and the First Reconstruction Problem are equivalent.*

Proof. Let $\mathcal{S}_D$ and $\mathcal{S}_1$ be the set of solutions of $\mathrm{GDP}(\boldsymbol{y}, \boldsymbol{g}, k)$ and $\mathrm{FRP}(\boldsymbol{y}, \boldsymbol{g}, k)$, respectively.

Let $\boldsymbol{x} \in \mathcal{S}_D$. There exists $f \in \mathcal{P}_k(E)$ such that $\boldsymbol{x} = \boldsymbol{f}(\boldsymbol{g})$. Since $\operatorname{rank}(\boldsymbol{y} - \boldsymbol{f}(\boldsymbol{g})) \leq t$, the submodule $S = \langle y_1 - f(g_1), \ldots, y_n - f(g_n) \rangle$ has a minimal generator system of $\lfloor rt \rfloor$ elements in the worst case. By Lemma 4, there exists a free submodule $S' \subseteq E$ of rank at most $\lfloor rt \rfloor$ such that $S \subseteq S'$. As a result of Lemma 6, there exists $V \in \mathcal{P}^*_{\lfloor rt \rfloor + 1}(E)$ such that $S \subseteq \ker V$. Hence, there exists V such that $\boldsymbol{V}(\boldsymbol{y} - \boldsymbol{f}(\boldsymbol{g})) = \boldsymbol{0}$. Since V is linear, $(V, f) \in \mathcal{S}_1$.

Let $(V, q) \in \mathcal{S}_1$. Since $\boldsymbol{y}$ is decodable, there exists $f \in \mathcal{P}_k(E)$ such that $\boldsymbol{x} = \boldsymbol{f}(\boldsymbol{g}) \in \mathrm{Gab}_E(n, k, \boldsymbol{g})$ and $\operatorname{rank}(\boldsymbol{y} - \boldsymbol{x}) \leq t$. Then, since $(V, q) \in \mathcal{S}_1$ and V is linear,

$$\operatorname{rank}(\boldsymbol{V} \circ (\boldsymbol{q} - \boldsymbol{f}))(\boldsymbol{g}) = \operatorname{rank} \boldsymbol{V}(\boldsymbol{y} - \boldsymbol{f}(\boldsymbol{g})) \leq \operatorname{rank}(\boldsymbol{y} - \boldsymbol{f}(\boldsymbol{g})) \leq t.$$

As a consequence of $\langle (V \circ (q - f))(g_i) \mid i \in \{1, \ldots, n\} \rangle$ having at most p^{rt} elements, it also has at most $\lfloor rt \rfloor$ generators, and by Lemmas 4 and 6 there exists $F \in \mathcal{P}^*_{\lfloor rt \rfloor + 1}(E)$ such that

$$((\boldsymbol{F} \circ \boldsymbol{V}) \circ (\boldsymbol{q} - \boldsymbol{f}))(\boldsymbol{g}) = \boldsymbol{0}.$$

Note that, by Lemma 6, if $(F \circ V) \circ (q - f) \neq \boldsymbol{0}$ then it would have at most $p^{2\lfloor rt \rfloor + k - 1}p^{(r-1)n}$ zeros, but since the elements in $\boldsymbol{g}$ are linearly independent, it actually has at least p^{rn} zeros. By the definition of t,

$$2\lfloor rt \rfloor + k - 1 + (r-1)n \leq 2rt + k - 1 + rn - n = rn - 1 < rn.$$

As a consequence, $(F \circ V) \circ (p - f) = 0$. Moreover, since both F and V belong to $\mathcal{P}^*_{\lfloor rt \rfloor + 1}(E)$, $F \circ V$ lies in $\mathcal{P}^*_{2\lfloor rt \rfloor + 1}(E)$. Hence, if we denote b_i the coefficient of τ^i in $(q - f)(X)$, the coefficient of $\tau^{2\lfloor rt \rfloor + k - 1}$ in $(F \circ V) \circ (q - f)$ is $\tau^{2\lfloor rt \rfloor}(b_{k-1})$, implying $b_{k-1} = 0$ and $(q - f) \in \mathcal{P}_{k-1}(E)$. Similarly, the coefficient b_{k-2} is now forced to be zero, and with the same argument we conclude that $q - f = 0$, so $q = f$, and $\boldsymbol{q}(\boldsymbol{g}) = \boldsymbol{x} \in \mathcal{S}_D$. □

The FRP does not seem computationally easy to solve at first sight. We now introduce the final reconstruction problem, which will lead us to a solution of the GDP.

Definition 13 (Second Reconstruction Problem)**.** The second reconstruction problem $SRP(\boldsymbol{y}, \boldsymbol{g}, k)$ consists in finding $(V, N) \in \mathcal{P}^*_{\lfloor rt \rfloor + 1}(E) \times \mathcal{P}_{\lfloor rt \rfloor + k}(E)$ such that $\boldsymbol{V}(\boldsymbol{y}) = \boldsymbol{N}(\boldsymbol{g})$.

Now, we prove that both Reconstruction Problems are equivalent.

Theorem 6. *Let $\mathrm{Gab}_E(n, k, \boldsymbol{g})$ be a Gabidulin code and $\boldsymbol{y} \in E^n$ a decodable word. In this case, the First and Second Reconstruction Problems are equivalent.*

Proof. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ denote the solutions of $\mathrm{FRP}(\boldsymbol{y}, \boldsymbol{g}, k)$ and $\mathrm{SRP}(\boldsymbol{y}, \boldsymbol{g}, k)$, respectively. Then, let $(V, q) \in \mathcal{S}_1$. Observe that $V \circ q \in \mathcal{P}_{\lfloor rt \rfloor + k}(E)$ and satisfies $\boldsymbol{V}(\boldsymbol{y}) = (\boldsymbol{V} \circ \boldsymbol{q})(\boldsymbol{g})$, so $(V, V \circ q) \in \mathcal{S}_2$.

Now, let $(V, N) \in \mathcal{S}_2$. From the definition of $\boldsymbol{y}$ it follows that there exists $f \in \mathcal{P}_k(E)$ such that $\operatorname{rank}(\boldsymbol{y} - \boldsymbol{f}(\boldsymbol{g})) \leq t$. Therefore, since both N and V are linear,

$$\operatorname{rank}(\boldsymbol{N} - \boldsymbol{V} \circ \boldsymbol{f})(\boldsymbol{g}) = \operatorname{rank}(\boldsymbol{V}(\boldsymbol{y}) - \boldsymbol{V}(\boldsymbol{f}(\boldsymbol{g})) = \operatorname{rank}(\boldsymbol{V}(\boldsymbol{y} - \boldsymbol{f}(\boldsymbol{g})) \leq t,$$

so by Lemmas 4 and 6 there exists $F \in \mathcal{P}^*_{\lfloor rt \rfloor+1}(E)$ such that $\boldsymbol{F} \circ (\boldsymbol{N} - \boldsymbol{V}(\boldsymbol{f})) = \boldsymbol{0}$. But, since $F \in \mathcal{P}^*_{\lfloor rt \rfloor+1}(E)$ it follows that every coefficient $N - V \circ f$ is zero. We conclude that there exists f such that $N = V \circ f$. □

We therefore propose the following decoding algorithm.

Theorem 7 (Decoding of Gabidulin codes)**.** *Let $\mathcal{C} = \mathrm{Gab}_E(n.k, \boldsymbol{g})$ be a Gabidulin code and $\boldsymbol{y}$ a received message where $d(\boldsymbol{y}, \mathcal{C}) \leq \frac{n-k}{2r} = t$. Let $\boldsymbol{c} = (n_0, \ldots, n_{\lfloor rt \rfloor+k-1}, v_0, \ldots, v_{\lfloor rt \rfloor-1}) \in E^{2\lfloor rt \rfloor+k}$ such that $A\boldsymbol{c} = \boldsymbol{b}$, where $\boldsymbol{b} = (\tau^{\lfloor rt \rfloor}(y_1), \ldots, \tau^{\lfloor rt \rfloor}(y_n))$ and*

$$A = \begin{pmatrix} g_1 & \tau(g_1) & \ldots & \tau^{\lfloor rt \rfloor+k-1}(g_1) & -y_1 & -\tau(y_1) & \ldots & -\tau^{\lfloor rt \rfloor-1}(y_1) \\ g_2 & \tau(g_2) & \ldots & \tau^{\lfloor rt \rfloor+k-1}(g_2) & -y_2 & -\tau(y_2) & \ldots & -\tau^{\lfloor rt \rfloor-1}(y_2) \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ g_n & \tau(g_n) & \ldots & \tau^{\lfloor rt \rfloor+k-1}(g_n) & -y_1 & -\tau(y_n) & \ldots & -\tau^{\lfloor rt \rfloor-1}(y_n) \end{pmatrix}.$$

If we denote as f the result of the left Euclidean division of $\sum_{i=0}^{\lfloor rt \rfloor+k-1} n_i \tau^i(X)$ by $\sum_{i=0}^{\lfloor rt \rfloor-1} v_i \tau^i(X) + \tau^{\lfloor rt \rfloor}(X)$, then $\boldsymbol{y}$ decodes to $(f(g_1), \ldots, f(g_n))$ in $\mathcal{C}$.

Proof. If $d(\boldsymbol{y}, \mathcal{C}) \leq \frac{n-k}{2r}$, then by Corollary 4 there exists $\boldsymbol{x} \in \mathcal{C}$ such that $\boldsymbol{x} \in \mathrm{Gab}_E(n, k, \boldsymbol{g})$ and $\boldsymbol{y}$ decodes to $\boldsymbol{x}$. By Theorem 5, there exists a solution of $\mathrm{FRP}(\boldsymbol{y}, \boldsymbol{g}, k)$. By Theorem 6 there also exists a solution for $\mathrm{SRP}(\boldsymbol{y}, \boldsymbol{g}, k)$. Therefore, there exist N and V solutions of this problem satisfying $\boldsymbol{N}(\boldsymbol{y}) - \boldsymbol{V}(\boldsymbol{g}) = 0$. The coefficients of N and V are exactly the solutions $\boldsymbol{c}$ of the linear system $A\boldsymbol{c} = \boldsymbol{b}$. Besides, since there exists a solution of $\mathrm{SRP}(\boldsymbol{y}, \boldsymbol{g}, k)$, by the proof of Theorem 6 there exists a solution of the type (V, f), where f is the left Euclidean division of N by V in the ring of linearized polynomials. By the proof of Theorem 5, f also satisfies $\boldsymbol{x} = \boldsymbol{f}(\boldsymbol{g}) \in \mathrm{Gab}_E(n, k, \boldsymbol{g})$ and $\mathrm{rank}(\boldsymbol{y} - \boldsymbol{x}) \leq t$. □

This decoding method requires finding the solution of a system of linear equations with a total of $2\lfloor rt \rfloor + k$ unknown values. If one has to correct several errors, part of the matrices may be precomputed. In fact, one can divide A into blocks

$$\begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

such that A_{11} is square of size $\lfloor rt \rfloor + k$. Then, A_{11} is invertible and A_{11} and A_{12} are fixed for the same code. We can also let $\boldsymbol{N} = (n_0, \ldots, n_{\lfloor rt \rfloor+k-1})$, $\boldsymbol{V} = (v_0, \ldots, v_{\lfloor rt \rfloor-1})$ and $\boldsymbol{b} = (\boldsymbol{b}_1, \boldsymbol{b}_2)$, where $\boldsymbol{b}_1 \in E^{\lfloor rt \rfloor+k}$. Thus, we can solve the following system of equations:

$$\begin{cases} (A_{22} - A_{21}A_{11}^{-1}A_{12})\,\boldsymbol{V} = \boldsymbol{b}_2 - A_{21}A_{11}^{-1}\boldsymbol{b}_1 \\ \boldsymbol{N} = A_{11}^{-1}\boldsymbol{b}_1 - A_{11}^{-1}A_{12}\,\boldsymbol{V} \end{cases},$$

where A_{11}^{-1} and $A_{21}A_{11}^{-1}$ can be computed beforehand.

Furthermore, other techniques such us the iterative algorithm to construct N and V from SRP in [9] can also be used to build solutions. This algorithm uses techniques from polynomial interpolation, along with Lemma 6 to build two sequences of linearized polynomials $(N_0^{(i)}, V_0^{(i)})$, $(N_1^{(i)}, V_1^{(i)})$ such that $V_j^{(i)}(y_s) - N_j^{(i)}(g_s) = 0$ for all $s = 1, \ldots, i$, $i = 1, \ldots, n$, $s = 1, 2$. In each iteration we can either construct the next polynomial by the induction process of the proof of part (ii) from Lemma 6, or by crossing both sequences of linearized polynomials in order not to increase the degree and make one of the pairs get to step n with their corresponding degrees.

6. Conclusions and future work

Coding theory over rings from a cryptographic point of view has also been studied previously [3]. However, in this paper we have focused on cardinal rank metric codes over Galois rings, using a metric that, as explained in Section 3.3, is potentially interesting from a cryptographic perspective. This metric

generalizes its well known analog over finite fields. We presented its properties, as well as the notion of cardinal rank metric codes. We have also proved the existence of MCRD codes, among which we can find the generalization of Gabidulin codes. This code has an efficient decoding algorithm, reducing its decoding problem to a linear system of equations. A study of the security of a McEliece-like cryptosystem based on these codes, and in particular the existence of structural attacks in such a setting, is left as a future work.

Acknowledgments

This work is partially supported by MTM-2017-83506-C2-2-P and FC-GRUPIN-IDI/2018/000193. The authors also thank the anonymous referees for their suggestions and comments.

References

[1] Bini, G., Flamini, F. 'Finite Commutative Rings and Their Applications'. The Springer International Series in Engineering and Computer Science, Springer, 2002. https://doi.org/10.1007/978-1-4615-0957-8 ISBN978-1-4020-7039-6

[2] Brown, W. 'Matrices over Commutative Rings'. Chapman & Hall, November 1992. ISBN13-9780824787554

[3] Epelde, M., Larrucea, X., Rúa, I. F. 'On quaternary Goppa codes'. Discrete Mathematics, Volume 343, Issue 9, September 2020. https://doi.org/10.1016/j.disc.2020.111962

[4] Gabidulin, E. M., 'Theory of codes with maximum rank distance'. Problems of Information Transmission, 21 (1): 1–12, 1985.

[5] Gabidulin, E. M., Paramonov, A. V., Tretjakov, O. V. 'Ideals over a non-commutative ring and their application in cryptology'. EUROCRYPT 1991: Advances in Cryptology - EUROCRYPT '91 pp 482-489, 1991. DOI https://doi.org/10.1007/3-540-46416-6_41

[6] Gaborit, P., Ruatta, O., Schreck, J., Tillich, J., Zémor, G. 'Rank based Cryptography: a credible post-quantum alternative to classical crypto'. NIST 2015: Workshop on Cybersecurity in a Post-Quantum World 2015. April 2015.

[7] Gibson, J. K. 'Severely denting the Gabidulin version of the McEliece public key cryptosystem'. Designs, Codes and Cryptography volume 6, pg. 37–45, 1995. https://doi.org/10.1007/BF01390769

[8] Kamche, H. T., Mouaha, C. 'Rank-Metric Codes Over Finite Principal Ideal Rings and Applications'. IEEE Transactions on Information Theory, Volume 65, Issue 12, December 2019. https://doi.org/10.1109/TIT.2019.2933520

[9] Loidreau, P. 'A Welch–Berlekamp Like Algorithm for Decoding Gabidulin Codes'. Coding and Cryptography. WCC, Lecture Notes in Computer Science, vol 3969, 2005. https://doi.org/10.1007/11779360_4

[10] McEliece, R. J. 'A Public-Key Cryptosystem Based On Algebraic Coding Theory'. Deep Space Network Progress Report 44, 114–16, January 1978. https://doi.org/10.1007%2F978-3-642-22792-9_43

[11] Shannon, C. E. 'A Mathematical Theory of Communication' Bell System Technical Journal. 27 (3-4): 379–423. July-August 1948. doi:10.1002/j.1538-7305.1948.tb01338.x., doi:10.1002/j.1538-7305.1948.tb00917.x.