Rank error-correcting pairs

Noname manuscript No.
(will be inserted by the editor)

Rank error-correcting pairs

Umberto Martínez-Peñas · Ruud Pellikaan

Received: date / Accepted: date

Abstract Error-correcting pairs were introduced as a general method of decoding linear codes with respect to the Hamming metric using coordinatewise products of vectors, and are used for many well-known families of codes. In this paper, we define new types of vector products, extending the coordinatewise product, some of which preserve symbolic products of linearized polynomials after evaluation and some of which coincide with usual products of matrices. Then we define rank error-correcting pairs for codes that are linear over the extension field and for codes that are linear over the base field, and relate both types. Bounds on the minimum rank distance of codes and MRD conditions are given. Finally we show that some well-known families of rank-metric codes admit rank error-correcting pairs, and show that the given algorithm generalizes the classical algorithm using error-correcting pairs for the Hamming metric.

Keywords Decoding · error-correcting pairs · linearized polynomials · rank metric · vector products.

Mathematics Subject Classification (2000) 15B33 · 94B35 · 94B65

1 Introduction

Error-correcting pairs were introduced independently by Pellikaan in [20,21] and by Kötter in [14]. These are pairs of linear codes satisfying some conditions with respect to the coordinatewise product and a given linear code, for which they define

Supported by The Danish Council for Independent Research (Grant No. DFF-4002-00367)

Umberto Martínez-Peñas
Department of Mathematical Sciences, Aalborg University, Denmark
E-mail: umberto@math.aau.dk

Ruud Pellikaan
Department of Mathematics and Computing Science, Eindhoven University of Technology, The Netherlands
E-mail: g.r.pellikaan@tue.nl

an error-correcting algorithm with respect to the Hamming metric in polynomial time.

Linear codes with an error-correcting pair include many well-known families, such as (generalized) Reed-Solomon codes, many cyclic codes (such as BCH codes), Goppa codes and algebraic geometry codes (see [7,21,22]).

Error-correcting codes with respect to the rank metric [9] have recently gained considerable attention due to their applications in network coding [26]. In the rank metric, maximum rank distance (MRD) Gabidulin codes, as defined in [9, 15], have been widely used, and decoding algorithms using linearized polynomials are given in [9,15,17]. A related construction, the so-called q-cyclic or skew cyclic codes, were introduced by Gabidulin in [9] for square matrices and generalized independently by himself in [10] and by Ulmer et al. in [2].

However, more general methods of decoding with respect to the rank metric are lacking, specially for codes that are linear over the base field instead of the extension field.

The contributions of this paper are organized as follows. In Section 3, we introduce some families of vector products that coincide with usual products of matrices for some sizes. One of these products preserves symbolic products of linearized polynomials after evaluation and is the unique product with this property for some particular sizes. In Section 4, we introduce the concept of rank error-correcting pair and give efficient decoding algorithms based on them. Subsection 4.1 treats linear codes over the extension field, and Subsection 4.2 treats linear codes over the base field. In Section 5, we prove that the latter type of rank error-correcting pairs generalize the former type. In Section 6, we derive bounds on the minimum rank distance and give MRD conditions based on rank error-correcting pairs. Finally, in Section 7, we study some families of codes that admit rank error-correcting pairs, showing that the given algorithm generalizes the classical algorithm using error-correcting pairs for the Hamming metric.

2 Preliminaries

2.1 Notation

Fix a prime power q and positive integers m and n, and fix from now on a basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. $\mathbb{F}_{q^m}^n$ denotes the $\mathbb{F}_{q^m}$-linear vector space of row vectors over $\mathbb{F}_{q^m}$ with n components, and $\mathbb{F}_q^{m \times n}$ denotes the $\mathbb{F}_q$-linear vector space of $m \times n$ matrices over $\mathbb{F}_q$.

We will also use the following notation. Given a subset $\mathcal{A} \subseteq \mathbb{F}_{q^m}^n$, we denote by $\langle \mathcal{A} \rangle_{\mathbb{F}_q}$ and $\langle \mathcal{A} \rangle_{\mathbb{F}_{q^m}}$ the $\mathbb{F}_q$-linear and $\mathbb{F}_{q^m}$-linear vector spaces generated by $\mathcal{A}$, respectively. For an $\mathbb{F}_{q^m}$-linear (respectively $\mathbb{F}_q$-linear) code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ (respectively $\mathcal{C} \subseteq \mathbb{F}_q^n$), we denote its dimension over $\mathbb{F}_{q^m}$ (respectively over $\mathbb{F}_q$) by $\dim(\mathcal{C})$. If $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ or $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ is $\mathbb{F}_q$-linear, we denote its dimension over $\mathbb{F}_q$ by $\dim_{\mathbb{F}_q}(\mathcal{C})$.

2.2 Rank-metric codes

In the literature, it is usual to consider two types of rank-metric codes: $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, and $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{m \times n}$.

We will use the following classical matrix representation of vectors in $\mathbb{F}_{q^m}^n$ to connect both types of codes. Let $\mathbf{c} \in \mathbb{F}_{q^m}^n$, there exist unique $\mathbf{c}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, such that $\mathbf{c} = \sum_{i=1}^m \alpha_i \mathbf{c}_i$. Let $\mathbf{c}_i = (c_{i,1}, c_{i,2}, \ldots, c_{i,n})$ or, equivalently, $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and $c_j = \sum_{i=1}^m \alpha_i c_{i,j}$. Then we define the $m \times n$ matrix, with coefficients in $\mathbb{F}_q$,

$$M(\mathbf{c}) = (c_{i,j})_{1 \leq i \leq m, 1 \leq j \leq n}. \tag{1}$$

The map $M : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ is an $\mathbb{F}_q$-linear vector space isomorphism. Unless it is necessary, we will not write subscripts for M regarding the values m, n, or the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ (which of course change the map M).

By definition [9], the rank weight of $\mathbf{c}$ is $\mathrm{wt_R}(\mathbf{c}) = \mathrm{Rk}(M(\mathbf{c}))$, the rank of the matrix $M(\mathbf{c})$, for every $\mathbf{c} \in \mathbb{F}_{q^m}^n$. We also define the rank support of $\mathbf{c}$ as the row space of the matrix $M(\mathbf{c})$, that is, $\mathrm{RSupp}(\mathbf{c}) = \mathrm{Row}(M(\mathbf{c})) \subseteq \mathbb{F}_q^n$. We may identify any non-linear or $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with $M(\mathcal{C}) \subseteq \mathbb{F}_q^{m \times n}$ and write $d_R(\mathcal{C}) = d_R(M(\mathcal{C}))$ for their minimum rank distance [9].

2.3 Hamming-metric codes as rank-metric codes

We briefly discuss how to see Hamming-metric codes as rank-metric codes. We define the map $D : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^{n \times n}$ as follows. For every vector $\mathbf{c} \in \mathbb{F}_q^n$, define the matrix

$$D(\mathbf{c}) = \mathrm{diag}(\mathbf{c}) = (c_i \delta_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}, \tag{2}$$

that is, the diagonal $n \times n$ matrix with coefficients in $\mathbb{F}_q$ whose diagonal vector is $\mathbf{c}$. The map D is $\mathbb{F}_q$-linear and one to one. Moreover, the Hamming weight of a vector $\mathbf{c} \in \mathbb{F}_q^n$ is $\mathrm{wt_H}(\mathbf{c}) = \mathrm{Rk}(D(\mathbf{c}))$.

This gives a way to represent error-correcting codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ in the Hamming metric as error-correcting codes $D(\mathcal{C}) \subseteq \mathbb{F}_q^{n \times n}$ in the rank metric, where the Hamming weight distribution of $\mathcal{C}$ corresponds bijectively to the rank weight distribution of $D(\mathcal{C})$. In particular, the minimum Hamming distance of $\mathcal{C}$ satisfies $d_H(\mathcal{C}) = d_R(D(\mathcal{C}))$.

On the other hand, let $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ be an $\mathbb{F}_q$-linear Hamming-metric equivalence between $\mathbb{F}_q$-linear codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$. It is well-known that ϕ is a monomial map, that is, there exist $a_1, a_2, \ldots, a_n \in \mathbb{F}_q^*$ and a permutation σ with $\phi(\mathbf{c}) = (a_1 c_{\sigma(1)}, a_2 c_{\sigma(2)}, \ldots, a_n c_{\sigma(n)})$, for all $\mathbf{c} \in \mathcal{C}_1$. We may trivially extend this map to a rank-metric equivalence $\phi' : D(\mathcal{C}_1) \longrightarrow D(\mathcal{C}_2)$ by the same formula. Hence Hamming-metric equivalent codes correspond to rank-metric equivalent codes.

2.4 Error-correcting pairs for the Hamming metric

We conclude by defining error-correcting pairs (ECPs) for the Hamming metric, introduced independently by Pellikaan in [20,21] and by Kötter in [14]. Define the coordinatewise product $*$ of vectors in $\mathbb{F}_q^n$ by

$$\mathbf{a} * \mathbf{b} = (a_1 b_1, a_2 b_2, \ldots, a_n b_n),$$

for all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$. For two linear subspaces $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_q^n$, we define the linear subspace $\mathcal{A} * \mathcal{B} = \langle \{\mathbf{a} * \mathbf{b} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\} \rangle \subseteq \mathbb{F}_q^n$.

Definition 1 Let $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^n$ be linear codes and t a positive integer. The pair $(\mathcal{A}, \mathcal{B})$ is called a t-error-correcting pair (t-ECP) for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{A} * \mathcal{B} \subseteq \mathcal{C}^\perp$.
2. $\dim(\mathcal{A}) > t$.
3. $d_H(\mathcal{B}^\perp) > t$.
4. $d_H(\mathcal{A}) + d_H(\mathcal{C}) > n$.

In [20,21] it is shown that, if $\mathcal{C}$ has a t-ECP, then it has a decoding algorithm with complexity $O(n^3)$ that can correct up to t errors in the Hamming metric (and therefore, $d_H(\mathcal{C}) \geq 2t+1$). This algorithm is analogous to the ones that we will describe in Subsections 4.1 and 4.2. Actually, as we will see in Subsection 7.1, the algorithm presented in Subsection 4.2 extends the classical algorithm for Hamming-metric codes.

3 Vector products for the rank metric

In this section, we define and give the basic properties of a family of products of vectors in $\mathbb{F}_{q^m}^n$, which will play the same role as the coordinatewise product $*$ for vectors in $\mathbb{F}_q^n$.

Definition 2 We first define the product $\star : \mathbb{F}_{q^m}^m \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ in the following way. For every $\mathbf{c} \in \mathbb{F}_{q^m}^m$ and every $\mathbf{d} \in \mathbb{F}_{q^m}^n$, we define

$$\mathbf{c} \star \mathbf{d} = \sum_{i=1}^{m} c_i \mathbf{d}_i,$$

where $\mathbf{d} = \sum_{i=1}^m \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$, and $\mathbf{c} = (c_1, c_2, \ldots, c_m)$. Note that the second argument of $\star$ and its codomain are the same, whereas its first argument is different if $m \neq n$.

On the other hand, given a map $\varphi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$, we define the product $\star_\varphi : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ in the following way. For every $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, we define

$$\mathbf{c} \star_\varphi \mathbf{d} = \varphi(\mathbf{c}) \star \mathbf{d} = \sum_{i=1}^{m} \varphi(\mathbf{c})_i \mathbf{d}_i,$$

where $\mathbf{d} = \sum_{i=1}^m \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$, and $\varphi(\mathbf{c}) = (\varphi(\mathbf{c})_1, \varphi(\mathbf{c})_2, \ldots, \varphi(\mathbf{c})_m)$.

Remark 1 The following basic properties of the previous products hold:

1. The product $\star$ depends on the choice of the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q^n$, whereas the coordinatewise product $*$ does not.
2. The product $\star$ is $\mathbb{F}_{q^m}$-linear in the first component and $\mathbb{F}_q$-linear in the second component.
3. If φ is $\mathbb{F}_q$-linear, then the product $\star_\varphi$ is $\mathbb{F}_q$-bilinear.
4. On the other hand, if φ is $\mathbb{F}_{q^m}$-linear, then the product $\star_\varphi$ is $\mathbb{F}_{q^m}$-linear in the first component and $\mathbb{F}_q$-linear in the second component.

It is of interest to see if two maps give the same product:

Lemma 1 *Given maps $\varphi, \psi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$, it holds that $\star_\varphi = \star_\psi$ if, and only if, $\varphi = \psi$.*

Proof Fix i and take $\mathbf{d} \in \mathbb{F}_{q^m}^n$ such that $\mathbf{d}_i = \mathbf{e}_1$, the first vector in the canonical basis of $\mathbb{F}_q^n$ and $\mathbf{d}_j = \mathbf{0}$, for $j \neq i$. Since $\mathbf{c}\star_\varphi \mathbf{d} = \mathbf{c}\star_\psi \mathbf{d}$, it follows that $\varphi(\mathbf{c})_i = \psi(\mathbf{c})_i$. This is valid for an arbitrary i, hence $\varphi(\mathbf{c}) = \psi(\mathbf{c})$, for any $\mathbf{c} \in \mathbb{F}_{q^m}^n$, which implies that $\varphi = \psi$. The reverse implication is trivial.

One of the most important properties of the coordinatewise product $*$ is that it preserves multiplications of polynomials after evaluation. We now define a natural product that will preserve symbolic multiplications of linearized polynomials after evaluation.

Definition 3 (q-linearized polynomials) A q-linearized polynomial over $\mathbb{F}_{q^m}$ is a polynomial of the form

$$F = a_0 x + a_1 x^{[1]} + \cdots + a_d x^{[d]},$$

where $a_0, a_1, \ldots, a_d \in \mathbb{F}_{q^m}$ and $[i] = q^i$, for all $i \geq 0$.

These polynomials induce $\mathbb{F}_q$-linear maps in any extension field of $\mathbb{F}_{q^m}$.

Definition 4 (Evaluation map) For a vector $\mathbf{b} \in \mathbb{F}_{q^m}^n$, we will define the evaluation map

$$\mathrm{ev}_{\mathbf{b}} : \mathcal{L}_q\mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}^n$$

by $\mathrm{ev}_{\mathbf{b}}(F) = (F(b_1), F(b_2), \ldots, F(b_n))$, for $F \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$.

We start by the following interpolation lemma, where we denote by $\mathcal{L}_q\mathbb{F}_{q^m}[x]$ the set of q-linearized polynomials over $\mathbb{F}_{q^m}$.

Lemma 2 *If $n \leq m$, and $\mathbf{c} \in \mathbb{F}_{q^m}^n$, there exists a unique q-linearized polynomial $F \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$ of degree strictly less than $q^n = [n]$ such that $F(\alpha_i) = c_i$, for all $i = 1, 2, \ldots, n$.*

Proof Consider the evaluation map $\mathrm{ev}_{\boldsymbol{\alpha}} : \mathcal{L}_q\mathbb{F}_{q^m}[x] \longrightarrow \mathbb{F}_{q^m}^n$ for the vector $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Since it is $\mathbb{F}_{q^m}$-linear and the $\mathbb{F}_{q^m}$-linear space of q-linearized polynomials of degree less than $[n]$ has dimension n, it is enough to prove that, if $F(\alpha_i) = 0$, for $i = 1, 2, \ldots, n$, then $F = 0$.

By the linearity of F, we have that $F(\sum_i \lambda_i \alpha_i) = \sum_i \lambda_i F(\alpha_i) = 0$, for every $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{F}_q$. Therefore, F has q^n different roots and degree strictly less than q^n, hence $F = 0$, and we are done.

Now we may define the desired products:

Definition 5 If $n \leq m$, we denote by $F_{\mathbf{c}}$ the q-linearized polynomial of degree less than $[n]$ corresponding to $\mathbf{c} \in \mathbb{F}_{q^m}^n$.

For $\mathbf{c} \in \mathbb{F}_{q^m}^n$ and $n \leq m$, we define the vector $\varphi_n(\mathbf{c}) \in \mathbb{F}_{q^m}^m$ as $\varphi_n(\mathbf{c})_i = F_{\mathbf{c}}(\alpha_i)$, for $i = 1, 2, \ldots, m$. If $n \geq m$, we define $\varphi_n(\mathbf{c}) = (c_1, c_2, \ldots, c_m)$.

Finally, we will define the product $\star = \star_{\varphi_n} : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ (see Definition 2).

Note that if $m = n$, both definitions of φ_n lead to $\varphi_n(\mathbf{c}) = \mathbf{c}$. Also note that φ_n depends on the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ for $n < m$, while it does not for $n \geq m$.

When $m = n$, the product $\star$ in the previous definition coincides with the product $\star$ in Definition 2, whereas if $m \neq n$, then there is no confusion between these products, since the first argument is different. Hence the meaning of $\star$ is clear from the context.

In the following remark we show how to perform interpolation using symbolic multiplications of linearized polynomials. Recall that the symbolic multiplication of two linearized polynomials $F, G \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$ is defined as their composition $F \circ G$, which lies in $\mathcal{L}_q\mathbb{F}_{q^m}[x]$.

Remark 2 Interpolation as presented in Lemma 2 can be performed as follows. First, we see that the map $\mathbf{c} \in \mathbb{F}_{q^m}^n \mapsto F_\mathbf{c}$ is $\mathbb{F}_{q^m}$-linear. Therefore,

$$F_\mathbf{c} = \sum_{i=1}^{n} c_i F_{\mathbf{e}_i},$$

where $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ is the i-th vector in the canonical basis of $\mathbb{F}_{q^m}^n$ over $\mathbb{F}_{q^m}$, for $i = 1, 2, \ldots, n$. On the other hand, it holds that

$$F_{\mathbf{e}_i} = \frac{G_i}{G_i(\alpha_i)}, \quad \text{where} \quad G_i = \prod_{\beta \in \langle \alpha_j \mid j \neq i \rangle} (x - \beta),$$

and where $1 \leq j \leq n$. The polynomial $G_i / G_i(\alpha_i)$ in this expression is well-defined since α_i does not belong to the $\mathbb{F}_q$-linear vector space generated by the elements α_j, for $j \neq i$, and the expression in the numerator is a q-linearized polynomial by [16, Theorem 3.52] and has degree less than q^n. However, the complexity of constructing G_i in this way is of $O(q^{n-1})$ conventional multiplications. The following expression shows how to compute G_i with $O(n-1)$ symbolic multiplications:

$$G_i = L_{i,n} \circ L_{i,n-1} \circ \cdots \circ \widehat{L}_{i,i} \circ \cdots \circ L_{i,2} \circ L_{i,1},$$

where $L_{i,1} = x^{[1]} - (\alpha_1^{[1]}/\alpha_1)x$ and, for $j = 2, 3, \ldots, n$,

$$L_{i,j} = x^{[1]} - (\widetilde{L}_{i,j}(\alpha_j)^{[1]} / \widetilde{L}_{i,j}(\alpha_j))x$$

and $\widetilde{L}_{i,j} = L_{i,j-1} \circ \cdots \circ \widehat{L}_{i,i} \circ \cdots \circ L_{i,2} \circ L_{i,1}$. The notation $\widehat{L}_{i,i}$ means that the polynomial $L_{i,i}$ is omitted.

Next we see the linearity properties of the maps φ_n and hence of the product $\star$.

Lemma 3 *For any values of m and n, the map $\varphi_n : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$ is $\mathbb{F}_{q^m}$-linear.*

Proof For $n \geq m$, it is clear. For $n \leq m$, it is enough to note that $F_{\gamma\mathbf{c}+\delta\mathbf{d}} = \gamma F_\mathbf{c} + \delta F_\mathbf{d}$ as in the remark above, for all $\gamma, \delta \in \mathbb{F}_{q^m}$ and all $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$.

The interesting property of the product $\star$ is that it preserves symbolic multiplications of linearized polynomials, as we will see now, and in the case $n \leq m$, it is the unique product with this property.

From now on, we denote $\boldsymbol{\alpha}_n = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ if $n \leq m$, and we complete the vector with other elements if $n > m$, $\boldsymbol{\alpha}_n = (\alpha_1, \alpha_2, \ldots, \alpha_m, \gamma_1, \gamma_2, \ldots, \gamma_n)$. We will also denote $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$. Observe that $\varphi_n(\boldsymbol{\alpha}_n) = \boldsymbol{\alpha}$ in all cases, and moreover, $\varphi_n(\boldsymbol{\alpha}_n^{[j]}) = \boldsymbol{\alpha}^{[j]}$, if $j < n$.

Proposition 1 *The following properties hold:*

1. $\boldsymbol{\alpha}^{[j]} \star \mathbf{c} = \mathbf{c}^{[j]}$, *for all* $\mathbf{c} \in \mathbb{F}_{q^m}^n$ *and all* j. *In particular,*
$$\mathrm{ev}_{\mathbf{b}}(F \circ G) = \mathrm{ev}_{\boldsymbol{\alpha}}(F) \star \mathrm{ev}_{\mathbf{b}}(G),$$
for all $\mathbf{b} \in \mathbb{F}_{q^m}^n$ *and all* $F, G \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$.
2. $\boldsymbol{\alpha}_n^{[j]} \star \mathbf{c} = \mathbf{c}^{[j]}$, *for all* $\mathbf{c} \in \mathbb{F}_{q^m}^n$ *and all* $j < n$. *In particular,*
$$\mathrm{ev}_{\mathbf{b}}(F \circ G) = \mathrm{ev}_{\boldsymbol{\alpha}_n}(F) \star \mathrm{ev}_{\mathbf{b}}(G),$$
for all $\mathbf{b} \in \mathbb{F}_{q^m}^n$ *and all* $F, G \in \mathcal{L}_q\mathbb{F}_{q^m}[x]$, *where* F *has degree strictly less than* $[n]$.
3. *If* $n \leq m$, *then* $\star$ *is associative, that is,* $\mathbf{a} \star (\mathbf{b} \star \mathbf{c}) = (\mathbf{a} \star \mathbf{b}) \star \mathbf{c}$, *for all* $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_{q^m}^n$.

Moreover, if $n \leq m$, *and if* $\odot$ *is another product that satisfies item 2 for* $\mathbf{b} = \boldsymbol{\alpha}_n$ *(or item 1 for* $\mathbf{b} = \boldsymbol{\alpha}$*), then* $\odot = \star$. *In particular, by Lemma 1, if* $\star_\varphi$ *satisfies this property, then* $\varphi = \varphi_n$.

Proof 1. The first part follows from the following chain of equalities:

$$\boldsymbol{\alpha}^{[j]} \star \mathbf{c} = \sum_{i=1}^{m} \alpha_i^{[j]} \mathbf{c}_i = \left(\sum_{i=1}^{m} \alpha_i \mathbf{c}_i \right)^{[j]} = \mathbf{c}^{[j]}.$$

The second part follows from the first part, since $\boldsymbol{\alpha}^{[j]} = \mathrm{ev}_{\boldsymbol{\alpha}}(x^{[j]})$ and therefore,

$$\mathrm{ev}_{\boldsymbol{\alpha}}(x^{[j]}) \star \mathrm{ev}_{\mathbf{b}}(G) = \mathrm{ev}_{\mathbf{b}}(G)^{[j]} = \mathrm{ev}_{\mathbf{b}}(G^{[j]}) = \mathrm{ev}_{\mathbf{b}}(x^{[j]} \circ G).$$

Hence the item follows since $\star$ is $\mathbb{F}_{q^m}$-linear in the first component, by Remark 1 and Lemma 3.
2. It follows from item 1, since $\varphi_n(\boldsymbol{\alpha}_n^{[j]}) = \boldsymbol{\alpha}^{[j]}$, if $j < n$.
3. It follows from item 2, since $\mathrm{ev}_{\boldsymbol{\alpha}_n}$ is surjective (by Lemma 2) and symbolic multiplication of linearized polynomials is associative.

If $n \leq m$, the last part of the proposition follows from the fact that $\mathrm{ev}_{\boldsymbol{\alpha}_n}$ (or $\mathrm{ev}_{\boldsymbol{\alpha}}$) is surjective, which follows from Lemma 2.

We will now give a matrix representation of the products $\star_\varphi$, and show that the product $\star$ actually extends the product $*$. For that purpose, we define the "extension" map $E : \mathbb{F}_q^n \longrightarrow \mathbb{F}_{q^n}^n$ by $E = M^{-1} \circ D$ (recall Subsection 2.2 and Subsection 2.3), which is $\mathbb{F}_q$-linear and one to one. In other words,

$$E(\mathbf{c}) = (\alpha_1 c_1, \alpha_2 c_2, \ldots, \alpha_n c_n), \tag{3}$$

for all $\mathbf{c} \in \mathbb{F}_q^n$, which satisfies that $\mathrm{wt}_{\mathrm{R}}(E(\mathbf{c})) = \mathrm{wt}_{\mathrm{H}}(\mathbf{c})$. We gather in the next proposition the relations between the products $\star_\varphi$ and $*$, and the maps M, D and E. The proof is straightforward.

Proposition 2 *For all values of m and n, all maps φ and all vectors $\mathbf{c}' \in \mathbb{F}_{q^m}^m$ and $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, we have that*

$$M(\mathbf{c}' \star \mathbf{d}) = M(\mathbf{c}')M(\mathbf{d}) \quad \textit{and} \quad M(\mathbf{c} \star_\varphi \mathbf{d}) = M(\varphi(\mathbf{c}))M(\mathbf{d}).$$

On the other hand, if $m = n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, then

$$D(\mathbf{a} * \mathbf{b}) = D(\mathbf{a})D(\mathbf{b}) \quad \textit{and} \quad E(\mathbf{a} * \mathbf{b}) = E(\mathbf{a}) \star E(\mathbf{b}).$$

Hence, the product $\star : \mathbb{F}_{q^m}^m \times \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^n$ is just the usual product of $m \times m$ matrices with $m \times n$ matrices over $\mathbb{F}_q$, whereas the products $\star_\varphi$ are also products of matrices after expanding the $m \times n$ matrix in the first argument to an $m \times m$ matrix over $\mathbb{F}_q$.

4 Rank error-correcting pairs

We will define in this section error-correcting pairs (ECPs) for the rank metric, using the products $\star$ and $\star_\varphi$ (recall Definition 2 and Definition 5). However, which inner product to use for defining orthogonality and duality in $\mathbb{F}_{q^m}^n$, or in $\mathbb{F}_q^{m\times n}$, is not clear. First of all, we will always use the standard ($\mathbb{F}_q$-bilinear) inner product $\cdot$ in $\mathbb{F}_q^n$. On the other hand, we will first present ECPs in $\mathbb{F}_{q^m}^n$ that use the ($\mathbb{F}_{q^m}$-bilinear) "extension" inner product,

$$\mathbf{c} \cdot \mathbf{d} = c_1 d_1 + c_2 d_2 + \cdots + c_n d_n \in \mathbb{F}_{q^m}, \tag{4}$$

for all $\mathbf{c} = (c_1, c_2, \ldots, c_n), \mathbf{d} = (d_1, d_2, \ldots, d_n) \in \mathbb{F}_{q^m}^n$, and afterwards we will use the ($\mathbb{F}_q$-bilinear) "base" (or "trace") inner product in $\mathbb{F}_q^{m\times n}$,

$$\langle C, D \rangle = \mathbf{c}_1 \cdot \mathbf{d}_1 + \mathbf{c}_2 \cdot \mathbf{d}_2 + \cdots + \mathbf{c}_m \cdot \mathbf{d}_m = \mathrm{Tr}(CD^T) = \sum_{i,j} c_{i,j} d_{i,j} \in \mathbb{F}_q, \tag{5}$$

for $C, D \in \mathbb{F}_q^{m\times n}$,where $\mathbf{c}_i, \mathbf{d}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$, are the rows of C and D, respectively, and $c_{i,j}, d_{i,j} \in \mathbb{F}_q$ are the entries of C and D, respectively. Tr denotes the usual trace of a square matrix.

Whereas the product $\cdot$ is the standard $\mathbb{F}_{q^m}$-bilinear product in $\mathbb{F}_{q^m}^n$, the product $\langle , \rangle$ corresponds to the standard $\mathbb{F}_q$-bilinear product in $\mathbb{F}_q^{mn} \cong \mathbb{F}_q^{m\times n}$. A duality theory for the product $\langle , \rangle$ and $\mathbb{F}_q$-linear rank-metric codes is developed originally in [5] and further in [23], where it is also shown that duals of $\mathbb{F}_{q^m}$-linear codes with respect to the "extension" inner product are equivalent to duals with respect to the "base" inner product (see [23, Theorem 21]). We will come back to this in Section 5, where we will relate both kinds of error-correcting pairs.

Now we will give some relations between the product $\star$ and the previous inner products that we will use later. If $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$, $\mathbf{d} = \sum_{i=1}^m \alpha_i \mathbf{d}_i$ and $\mathbf{d}_i \in \mathbb{F}_q^n$, for all $i = 1, 2, \ldots, m$, then we define

$$\mathbf{c}(\mathbf{d}) = (\mathbf{c} \cdot \mathbf{d}_1, \mathbf{c} \cdot \mathbf{d}_2, \ldots, \mathbf{c} \cdot \mathbf{d}_m) \in \mathbb{F}_{q^m}^m. \tag{6}$$

Lemma 4 *Given $\mathbf{c}, \mathbf{d} \in \mathbb{F}_{q^m}^n$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^m$, and given $C, D \in \mathbb{F}_q^{m\times n}$ and $A, B \in \mathbb{F}_q^{m\times m}$, the following properties hold:*

1. $M(\mathbf{c}(\mathbf{d})) = M(\mathbf{c})M(\mathbf{d})^T$.

2. $\langle B, A^T \rangle = \langle B^T, A\rangle$.
3. $(\mathbf{b} \star \mathbf{c}) \cdot \mathbf{d} = \mathbf{b} \cdot \mathbf{d}(\mathbf{c})$.
4. $\langle BC, D\rangle = \langle B, DC^T\rangle = \langle B^T, CD^T\rangle = \langle B^T D, C\rangle$.
5. $\mathbf{c}(\mathbf{d}) = \mathbf{0}$ *if, and only if,* $\mathbf{d}(\mathbf{c}) = \mathbf{0}$ *if, and only if,* $\mathrm{RSupp}(\mathbf{c}) \subseteq \mathrm{RSupp}(\mathbf{d})^\perp$.
6. $CD^T = 0$ *if, and only if,* $DC^T = 0$ *if, and only if,* $\mathrm{Row}(C) \subseteq \mathrm{Row}(D)^\perp$.

Proof They are straightforward computations. For item 1, observe that

$$\mathbf{c}(\mathbf{d}) = (\mathbf{c} \cdot \mathbf{d}_1, \mathbf{c} \cdot \mathbf{d}_2, \ldots, \mathbf{c} \cdot \mathbf{d}_m) = \sum_{i=1}^{m} \alpha_i (\mathbf{c}_i \cdot \mathbf{d}_1, \mathbf{c}_i \cdot \mathbf{d}_2, \ldots, \mathbf{c}_i \cdot \mathbf{d}_m).$$

Hence

$$M(\mathbf{c}(\mathbf{d}))_{i,k} = \mathbf{c}_i \cdot \mathbf{d}_k = \sum_{j=1}^{n} c_{i,j} d_{k,j} = \sum_{j=1}^{n} M(\mathbf{c})_{i,j} M(\mathbf{d})^T_{j,k}.$$

Therefore, $M(\mathbf{c}(\mathbf{d})) = M(\mathbf{c})M(\mathbf{d})^T$.

For item 3,

$$(\mathbf{b} \star \mathbf{c}) \cdot \mathbf{d} = \left(\sum_{i=1}^{m} b_i \mathbf{c}_i\right) \cdot \mathbf{d} = \sum_{i=1}^{m} b_i (\mathbf{c}_i \cdot \mathbf{d}) = \mathbf{b} \cdot \mathbf{d}(\mathbf{c}).$$

The first equivalence in Item 5 follows from item 1. Now, the second equivalence follows from the following chain of equivalences:

$$\mathbf{c}(\mathbf{d}) = \mathbf{0} \Longleftrightarrow \mathbf{c}_k \cdot \mathbf{d}_i = 0, \forall i, k \Longleftrightarrow \mathrm{RSupp}(\mathbf{c}) \subseteq \mathrm{RSupp}(\mathbf{d})^\perp.$$

4.1 Using the extension inner product

Denote by $\mathcal{D}^\perp$ the dual of an $\mathbb{F}_{q^m}$-linear code $\mathcal{D} \subseteq \mathbb{F}_{q^m}^n$ with respect to the extension product $\cdot$. Fix $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$ such that $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$, where $\mathcal{B} \star \mathcal{A}$ is defined as

$$\mathcal{B} \star \mathcal{A} = \langle \{\mathbf{b} \star \mathbf{a} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\}\rangle_{\mathbb{F}_{q^m}}. \tag{7}$$

In many cases, $\mathcal{B} = \varphi(\mathcal{B}')$, where $\varphi : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_{q^m}^m$ and $\mathcal{B}' \subseteq \mathbb{F}_{q^m}^n$ are both $\mathbb{F}_{q^m}$-linear. In that case, we denote $\mathcal{B}' \star_\varphi \mathcal{A} = \varphi(\mathcal{B}') \star \mathcal{A}$.

Observe that, since $\mathcal{B}$ is $\mathbb{F}_{q^m}$-linear and $\star$ is $\mathbb{F}_{q^m}$-linear in the first component, it holds that $\langle \{\mathbf{b} \star \mathbf{a} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\}\rangle_{\mathbb{F}_{q^m}} = \langle \{\mathbf{b} \star \mathbf{a} \mid \mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}\}\rangle_{\mathbb{F}_q}$.

We next compute generators of this space:

Proposition 3 *If* $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_r$ *generate* $\mathcal{A}$ *and* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s$ *generate* $\mathcal{B}$*, as* $\mathbb{F}_{q^m}$*-linear spaces, then the vectors*

$$\mathbf{b}_i \star (\alpha_l \mathbf{a}_j),$$

for $1 \leq i \leq s$*,* $1 \leq j \leq r$ *and* $1 \leq l \leq m$*, generate* $\mathcal{B} \star \mathcal{A}$ *as an* $\mathbb{F}_{q^m}$*-linear space.*

In the case $\mathcal{B} = \varphi(\mathcal{B}')$ and $\mathbf{b}'_1, \mathbf{b}'_2, \ldots, \mathbf{b}'_s$ generate $\mathcal{B}'$ as an $\mathbb{F}_{q^m}$-linear space, then the elements $\mathbf{b}'_i \star_\varphi (\alpha_l \mathbf{a}_j)$ generate $\mathcal{B}' \star_\varphi \mathcal{A}$ as an $\mathbb{F}_{q^m}$-linear space.

Regarding the dimension of $\mathcal{B} \star \mathcal{A}$ (or $\mathcal{B} \star_\varphi \mathcal{A}$), that is, how many of the elements $\mathbf{b}_i \star (\alpha_l \mathbf{a}_j)$ are linearly independent, the next example shows that any number may be possible in the case $n \leq m$, where the previous proposition says that an upper bound in the general case is $\min\{\dim(\mathcal{A}) \dim(\mathcal{B}) m, n\}$:

Example 1 Assume that $n \leq m$, fix $1 \leq t \leq n$, and define $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_{q^m}^n$ and $\mathbf{b} = \mathbf{a} + \mathbf{a}^{[1]} + \cdots + \mathbf{a}^{[t-1]} \in \mathbb{F}_{q^m}^n$. Let $\gamma \in \mathbb{F}_{q^m}$ be such that $\gamma, \gamma^{[1]}, \ldots, \gamma^{[t-1]}$ are pairwise distinct, and write $\gamma_i = \gamma^{[i]}$, for $i = 0, 1, \ldots, t-1$. Let $\mathcal{A}$ and $\mathcal{B}$ be the $\mathbb{F}_{q^m}$-linear spaces generated by $\mathbf{a}$ and $\mathbf{b}$, respectively. By Proposition 1, item 2, we have that

$$\mathbf{b} \star (\gamma^j \mathbf{a}) = \sum_{i=0}^{t-1} \mathbf{a}^{[i]} \star (\gamma^j \mathbf{a}) = \gamma_0^j \mathbf{a} + \gamma_1^j \mathbf{a}^{[1]} + \cdots + \gamma_{t-1}^j \mathbf{a}^{[t-1]} \in \mathcal{B} \star \mathcal{A},$$

for $j = 0, 1, 2, \ldots, t-1$, and these elements are linearly independent over $\mathbb{F}_{q^m}$, since the coefficients γ_i^j of the vectors $\mathbf{a}^{[i]}$ form a Vandermonde matrix. Furthermore, $\mathcal{B} \star \mathcal{A}$ is contained in the subspace generated by $\mathbf{a}, \mathbf{a}^{[1]}, \ldots, \mathbf{a}^{[t-1]}$, hence they are equal. Therefore, $\dim(\mathcal{A}) = \dim(\mathcal{B}) = 1$, whereas $\dim(\mathcal{B} \star \mathcal{A}) = t$.

Let $\mathbf{d} \in \mathbb{F}_{q^m}^n$ and define

$$\mathcal{K}(\mathbf{d}) = \{\mathbf{a} \in \mathcal{A} \mid (\mathbf{b} \star \mathbf{a}) \cdot \mathbf{d} = 0, \forall \mathbf{b} \in \mathcal{B}\}.$$

Then $\mathcal{K}(\mathbf{d})$ is $\mathbb{F}_q$-linear and the condition defining it may be verified just on a basis of $\mathcal{B}$ as $\mathbb{F}_{q^m}$-linear space. Observe that (precomputing the values $\varphi(\mathbf{b}')$, where the vectors $\mathbf{b}'$ are in a basis of $\mathcal{B}'$, in the case $\mathcal{B} = \varphi(\mathcal{B}')$), we can efficiently verify whether $\mathbf{a} \in \mathcal{K}(\mathbf{d})$. On the other hand, if $\mathcal{L} \subseteq \mathbb{F}_q^n$ is a linear subspace, define

$$\mathcal{A}(\mathcal{L}) = \{\mathbf{a} \in \mathcal{A} \mid \mathrm{RSupp}(\mathbf{a}) \subseteq \mathcal{L}^\perp\},$$

as in [12,13]. We briefly connect this definition with the so-called rank-shortened codes in [19, Definition 6], where $\mathcal{A}_{\mathcal{L}^\perp} = \mathcal{A} \cap \mathcal{V}_{\mathcal{L}}^\perp$ and $\mathcal{V}_{\mathcal{L}} = \mathcal{L} \otimes \mathbb{F}_{q^m}$ is defined as the $\mathbb{F}_{q^m}$-linear vector space in $\mathbb{F}_{q^m}^n$ generated by $\mathcal{L}$:

Lemma 5 *It holds that $\mathcal{A}(\mathcal{L}) = \mathcal{A}_{\mathcal{L}^\perp}$. In particular, it is an $\mathbb{F}_{q^m}$-linear space.*

Proof Fix a basis $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_w$ of $\mathcal{L}$, and take $\mathbf{a} = \sum_{i=1}^m \alpha_i \mathbf{a}_i \in \mathcal{A}$, where $\mathbf{a}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$. The result follows from the following chain of equivalent conditions

$$\mathrm{RSupp}(\mathbf{a}) \in \mathcal{L}^\perp \iff \mathbf{a}_i \in \mathcal{L}^\perp, \forall i \iff \mathbf{a}_i \cdot \mathbf{v}_j = 0, \forall i, j \iff \mathbf{a} \cdot \mathbf{v}_j = 0, \forall j \iff \mathbf{a} \in \mathcal{V}^\perp.$$

The following properties are the basic tools for the decoding algorithm of error correcting pairs:

Proposition 4 *Let $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in \mathcal{C}$ and $\mathrm{wt}_\mathrm{R}(\mathbf{e}) \leq t$. Define also $\mathcal{L} = \mathrm{RSupp}(\mathbf{e}) \subseteq \mathbb{F}_q^n$. The following properties hold:*

1. *$\mathcal{K}(\mathbf{r}) = \mathcal{K}(\mathbf{e})$.*
2. *$\mathcal{A}(\mathcal{L}) \subseteq \mathcal{K}(\mathbf{e})$.*
3. *If $t < d_R(\mathcal{B}^\perp)$, then $\mathcal{A}(\mathcal{L}) = \mathcal{K}(\mathbf{e})$. In this case, $\mathcal{K}(\mathbf{e})$ is $\mathbb{F}_{q^m}$-linear.*

Proof 1. It follows from $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$.
2. Let $\mathbf{a} \in \mathcal{A}(\mathcal{L})$. It follows from the definitions (recall (6)) that $\mathbf{e}(\mathbf{a}) = \mathbf{0}$. Hence, by Lemma 4, $(\mathbf{b} \star \mathbf{a}) \cdot \mathbf{e} = \mathbf{b} \cdot \mathbf{e}(\mathbf{a}) = 0$, for all $\mathbf{b} \in \mathcal{B}$. Thus $\mathbf{a} \in \mathcal{K}(\mathbf{e})$.

3. By the previous item, we only need to prove that $\mathcal{K}(\mathbf{e}) \subseteq \mathcal{A}(\mathcal{L})$.
   Let $\mathbf{a} \in \mathcal{K}(\mathbf{e})$. It follows from Lemma 4 that $\mathbf{e}(\mathbf{a}) \in \mathcal{B}^{\perp}$. Moreover, since $M(\mathbf{e}(\mathbf{a})) = M(\mathbf{e})M(\mathbf{a})^T$ by the same lemma, it holds that $\mathrm{wt_R}(\mathbf{e}(\mathbf{a})) \leq \mathrm{wt_R}(\mathbf{e}) \leq t$.
   Let $\mathbf{a} = \sum_{i=1}^{m} \alpha_i \mathbf{a}_i$, with $\mathbf{a}_i \in \mathbb{F}_q^n$, for $i = 1, 2, \ldots, m$. Since $t < d_R(\mathcal{B}^{\perp})$, it follows that $\mathbf{e}(\mathbf{a}) = \mathbf{0}$ or, in other words, $\mathbf{a}_i \cdot \mathbf{e} = 0$, which implies that $\mathbf{a}_i \in \mathcal{L}^{\perp}$, for all $i = 1, 2, \ldots, m$, and therefore, $\mathrm{RSupp}(\mathbf{a}) \subseteq \mathcal{L}^{\perp}$.

We now come to the definition of t-rank error-correcting pairs of type I, where we use the extension inner product $\cdot$.

Definition 6 Given the $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$, the pair $(\mathcal{A}, \mathcal{B})$ is called a t-rank error-correcting pair (t-RECP) of type I for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^{\perp}$.
2. $\dim(\mathcal{A}) > t$.
3. $d_R(\mathcal{B}^{\perp}) > t$.
4. $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$.

If $\mathcal{B} = \varphi(\mathcal{B}')$, where φ and $\mathcal{B}' \subseteq \mathbb{F}_{q^m}^n$ are $\mathbb{F}_{q^m}$-linear, we say that $(\mathcal{A}, \mathcal{B}')$ is a t-RECP of type I for φ and $\mathcal{C}$, and if $\varphi = \varphi_n$, we will call it simply a t-RECP of type I for $\mathcal{C}$.

In order to describe a decoding algorithm for $\mathcal{C}$ using $(\mathcal{A}, \mathcal{B})$, we will need [19, Proposition 17], slightly modified (the proof is the same), which basically states that error correction is equivalent to erasure correction if the rank support of the error is known:

Lemma 6 ([19]) *Assume that $\mathbf{c} \in \mathcal{C}$ and $\mathbf{r} = \mathbf{c} + \mathbf{e}$, where $\mathrm{RSupp}(\mathbf{e}) \subseteq \mathcal{L}$ and $\dim(\mathcal{L}) < d_R(\mathcal{C})$. Then, $\mathbf{c}$ is the only vector in $\mathcal{C}$ such that $\mathrm{RSupp}(\mathbf{r} - \mathbf{c}) \subseteq \mathcal{L}$.*

Moreover, if G is a generator matrix of $\mathcal{L}^{\perp}$, then $\mathbf{c}$ is the unique solution in $\mathcal{C}$ of the system of equations $\mathbf{r}G^T = \mathbf{x}G^T$, where $\mathbf{x}$ is the unknown vector. And if H is a parity check matrix for $\mathcal{C}$ over $\mathbb{F}_{q^m}$, then $\mathbf{e}$ is the unique solution to the system $\mathbf{r}H^T = \mathbf{x}H^T$ with $\mathrm{RSupp}(\mathbf{x}) \subseteq \mathcal{L}$.

Now we present, in the proof of the following theorem, a decoding algorithm for $\mathcal{C}$ using $(\mathcal{A}, \mathcal{B})$.

Theorem 1 *If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$, then $\mathcal{C}$ verifies that $d_R(\mathcal{C}) \geq 2t + 1$ and admits a decoding algorithm able to correct errors $\mathbf{e}$ with $\mathrm{wt_R}(\mathbf{e}) \leq t$ of complexity $O(n^3)$ over the field $\mathbb{F}_{q^m}$.*

Proof We will explicitly describe the decoding algorithm. As a consequence, we will derive that $d_R(\mathcal{C}) \geq 2t + 1$. Assume that the received codeword is $\mathbf{r} = \mathbf{c} + \mathbf{e}$, with $\mathbf{c} \in \mathcal{C}$, $\mathrm{RSupp}(\mathbf{e}) = \mathcal{L}$ and $\dim(\mathcal{L}) \leq t$.

Compute the space $\mathcal{K}(\mathbf{r})$, which is equal to $\mathcal{K}(\mathbf{e})$ by the first condition of t-RECP and Proposition 4, item 1. Observe that $\mathcal{K}(\mathbf{r})$ can be described by a system of $O(n)$ linear equations by Proposition 3.

By the third condition of t-RECP and Proposition 4, we have that $\mathcal{A}(\mathcal{L}) = \mathcal{K}(\mathbf{e}) = \mathcal{K}(\mathbf{r})$. Therefore, we have computed the space $\mathcal{A}(\mathcal{L})$.

By the second condition of t-RECP and Lemma 5, we have that $\mathcal{A}(\mathcal{L}) = \mathcal{A} \cap \mathcal{V}_{\mathcal{L}}^{\perp} \neq 0$, where $\mathcal{V}_{\mathcal{L}} = \mathcal{L} \otimes \mathbb{F}_{q^m}$, and therefore we may take a nonzero $\mathbf{a} \in \mathcal{A}(\mathcal{L})$. Define $\mathcal{L}' = \mathrm{RSupp}(\mathbf{a})^{\perp}$. Since $\mathbf{a} \in \mathcal{A}(\mathcal{L})$, we have that $\mathcal{L} \subseteq \mathcal{L}'$.

Now, by the fourth condition of t-RECP, we have that

$$\dim(\mathcal{L}') = n - \mathrm{wt_R}(\mathbf{a}) \leq n - d_R(\mathcal{A}) < d_R(\mathcal{C}).$$

Hence, by Lemma 6, we may compute $\mathbf{e}$ or $\mathbf{c}$ by solving a system of linear equations using a generator matrix G of $\mathcal{L}'^{\perp}$, or a parity check matrix H of $\mathcal{C}$, respectively. This has complexity $O(n^3)$ over $\mathbb{F}_{q^m}$.

Finally, assume that $d_R(\mathcal{C}) \leq 2t$ and take two different vectors $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$ and $\mathbf{e}, \mathbf{e}' \in \mathbb{F}_{q^m}^n$ such that $\mathbf{r} = \mathbf{c} + \mathbf{e} = \mathbf{c}' + \mathbf{e}'$ and $\mathrm{wt_R}(\mathbf{e}), \mathrm{wt_R}(\mathbf{e}') \leq t$. The previous algorithm gives as output both vectors $\mathbf{e}$ and $\mathbf{e}'$, but the output is unique, hence $\mathbf{e} = \mathbf{e}'$. This implies that $\mathbf{c} = \mathbf{c}'$, contradicting the hypothesis. Therefore, $d_R(\mathcal{C}) \geq 2t + 1$.

If $m = n$, then the order of complexity over $\mathbb{F}_q$ increases, although it still is polynomial in n. On the other hand, if m is considerably smaller than n, then the complexity is $O(n^3)$ also over $\mathbb{F}_q$.

Gabidulin codes [9] have decoding algorithms of cubic complexity (see for instance [9]), and an algorithm of quadratic complexity was obtained in [17]. As we will see in Section 7, the previous decoding algorithm may be applied to a wider variety of rank-metric codes.

Remark 3 Observe that, from the proof of the previous theorem, if the pair $(\mathcal{A}, \mathcal{B})$ satisfies the first three properties in Definition 6, then we may use it to find a subspace $\mathcal{L}' \subseteq \mathbb{F}_q^n$ that contains the rank support of the error vector.

Therefore, we say in this case that $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type I for $\mathcal{C}$.

4.2 Using the base inner product

Now we turn to the case where we use the base inner product $\langle , \rangle$. We will denote by $\mathcal{D}^*$ the dual of an $\mathbb{F}_q$-linear code $\mathcal{D} \subseteq \mathbb{F}_q^{m \times n}$ with respect to $\langle , \rangle$.

We will use the same notation as in the previous subsection, although now $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m \times m}$ are $\mathbb{F}_q$-linear, and $\mathcal{BA} \subseteq \mathcal{C}^*$, where

$$\mathcal{BA} = \langle \{ BA \mid A \in \mathcal{A}, B \in \mathcal{B} \} \rangle_{\mathbb{F}_q}. \tag{8}$$

Observe that $M(\mathcal{B}' \star \mathcal{A}') = M(\mathcal{B}')M(\mathcal{A}')$, if $\mathcal{A}', \mathcal{B}' \subseteq \mathbb{F}_{q^m}^n$ are $\mathbb{F}_q$-linear spaces, by Proposition 2. Generators of the space (8) are now simpler to compute:

Proposition 5 *If $A_1, A_2, \ldots, A_r$ generate $\mathcal{A}$ and $B_1, B_2, \ldots, B_s$ generate $\mathcal{B}$, as $\mathbb{F}_q$-linear spaces, then the matrices*

$$B_i A_j,$$

for $1 \leq i \leq s$ and $1 \leq j \leq r$, generate $\mathcal{BA}$ as an $\mathbb{F}_q$-linear space.

Let $D \in \mathbb{F}_q^{m\times n}$ and define

$$\mathcal{K}(D) = \{A \in \mathcal{A} \mid \langle BA, D\rangle = 0, \forall B \in \mathcal{B}\}.$$

Then $\mathcal{K}(D)$ is again $\mathbb{F}_q$-linear and the condition may be verified just on a basis of $\mathcal{B}$ as $\mathbb{F}_q$-linear space. On the other hand, if $\mathcal{L} \subseteq \mathbb{F}_q^n$ is a linear subspace, we define in the same way

$$\mathcal{A}(\mathcal{L}) = \{A \in \mathcal{A} \mid \mathrm{Row}(A) \subseteq \mathcal{L}^\perp\},$$

which is $\mathbb{F}_q$-linear (recall that we use the classical product $\cdot$ in $\mathbb{F}_q^n$), since we still have that $M^{-1}(\mathcal{A}(\mathcal{L})) = M^{-1}(\mathcal{A}) \cap \mathcal{V}_\mathcal{L}^\perp$, $\mathcal{V}_\mathcal{L} = \mathcal{L} \otimes \mathbb{F}_{q^m}$.

The following properties still hold:

Proposition 6 *Let $R = C + E$, where $C \in \mathcal{C}$ and $\mathrm{Rk}(E) \leq t$. Define also $\mathcal{L} = \mathrm{Row}(E) \subseteq \mathbb{F}_q^n$. Then*

1. *$\mathcal{K}(R) = \mathcal{K}(E)$.*
2. *$\mathcal{A}(\mathcal{L}) \subseteq \mathcal{K}(E)$.*
3. *If $t < d_R(\mathcal{B}^*)$, then $\mathcal{A}(\mathcal{L}) = \mathcal{K}(E)$.*

Proof 1. It also follows from $\mathcal{BA} \subseteq \mathcal{C}^*$.

2. Take $A \in \mathcal{A}(\mathcal{L})$. Hence by definition, it holds that $EA^T = 0$, since $\mathrm{Row}(E) = \mathcal{L}$ and $\mathrm{Row}(A) \subseteq \mathcal{L}^\perp$. Therefore, for every $B \in \mathcal{B}$, we have that

$$\langle BA, E\rangle = \langle B, EA^T\rangle = 0,$$

by Lemma 4. Then item 2 follows.

3. By the previous item, we only need to prove that $\mathcal{K}(E) \subseteq \mathcal{A}(\mathcal{L})$.
Let $A \in \mathcal{K}(E)$. It follows from Lemma 4 that $EA^T \in B^*$. Moreover, it holds that $\mathrm{Rk}(EA^T) \leq \mathrm{Rk}(E) \leq t$. Since $t < d_R(\mathcal{B}^*)$, it follows that $EA^T = 0$, which implies that $\mathrm{Row}(A) \in \mathcal{L}^\perp$.

We now define t-rank error-correcting pairs of type II, where we use the base product $\langle , \rangle$, in contrast with the t-RECP of last subsection.

Definition 7 Given the $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m\times m}$, the pair $(\mathcal{A}, \mathcal{B})$ is called a t-rank error-correcting pair (t-RECP) of type II for $\mathcal{C}$ if the following properties hold:

1. $\mathcal{BA} \subseteq \mathcal{C}^*$.
2. $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$.
3. $d_R(\mathcal{B}^*) > t$.
4. $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$.

The same decoding algorithm, with the corresponding modifications, works in this case with polynomial complexity:

Theorem 2 *If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{C}$, then $\mathcal{C}$ satisfies that $d_R(\mathcal{C}) \geq 2t + 1$ and admits a decoding algorithm able to correct errors E with $\mathrm{Rk}(E) \leq t$ with polynomial complexity in (m, n) over the field $\mathbb{F}_q$.*

Proof The proof is the same as in Theorem 1, with the corresponding modifications. Note that in this case, if $\mathcal{L} = \mathrm{Row}(E)$ and $\mathcal{V}_{\mathcal{L}} = \mathcal{L} \otimes \mathbb{F}_{q^m}$, then $\dim_{\mathbb{F}_q}(\mathcal{V}_{\mathcal{L}}) = m \dim(\mathcal{L}) \leq mt$. On the other hand, $M^{-1}(\mathcal{A}(\mathcal{L})) = M^{-1}(\mathcal{A}) \cap \mathcal{V}_{\mathcal{L}}$, as in the previous subsection. Hence the condition $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$ ensures that $\mathcal{A}(\mathcal{L}) \neq 0$.

Remark 4 As in Remark 3, if the pair $(\mathcal{A}, \mathcal{B})$ satisfies the first three properties in Definition 7, then we may use it to find a subspace $\mathcal{L}' \subseteq \mathbb{F}_q^n$ that contains the rank support of the error vector. We say in this case that $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type II for $\mathcal{C}$.

5 The connection between the two types of RECPs

So far we have three types of error-correcting pairs: classical ECPs for linear codes in $\mathbb{F}_q^n$ that correct errors in the Hamming metric, ECPs for $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$ (RECPs of type I), and ECPs for general $\mathbb{F}_q$-linear codes in $\mathbb{F}_{q^m}^n$ or $\mathbb{F}_q^{m \times n}$ (RECPs of type II), where the two latter types correct errors in the rank metric. In this section we will see that RECPs of type II generalize RECPs of type I. In Section 7 we will see that, in some way, RECPs of type II also generalize ECPs for the Hamming metric.

We will need the following:

Definition 8 Given the basis $\alpha_1, \alpha_2, \ldots, \alpha_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, we say that it is orthogonal (or dual) to another basis $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$ if

$$\mathrm{Tr}(\alpha_i \alpha'_j) = \delta_{i,j},$$

for all $i, j = 1, 2, \ldots, m$. Here, Tr denotes the trace of the extension $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$.

It is well-known that, for a given basis $\alpha_1, \alpha_2, \ldots, \alpha_m$, there exists a unique orthogonal basis (see for instance the discussion after [16, Definition 2.50]). We will denote it as in the previous definition: $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$. In particular, the dual basis of $\alpha'_1, \alpha'_2, \ldots, \alpha'_m$ is $\alpha_1, \alpha_2, \ldots, \alpha_m$.

Now denote by $M_\alpha, M_{\alpha'} : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m \times n}$ the matrix representation maps (recall (1)) associated to the previous bases, respectively. The following lemma is [23, Theorem 21]:

Lemma 7 ([23]) *Given an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$, it holds that*

$$M_{\alpha'}(\mathcal{C}^\perp) = M_\alpha(\mathcal{C})^*.$$

On the other hand, we have the following:

Lemma 8 *For every $\mathbb{F}_{q^m}$-linear code $\mathcal{D} \subseteq \mathbb{F}_{q^m}^n$, it holds that*

$$d_R(\mathcal{D}^\perp) = d_R(M_\alpha(\mathcal{D})^*) = d_R(M_{\alpha'}(\mathcal{D})^*).$$

Proof It follows from the fact that $d_R(\mathcal{D}^\perp) = d_R(M_{\alpha'}(\mathcal{D}^\perp)) = d_R(M_\alpha(\mathcal{D})^*)$, and analogously interchanging the roles of α and α'.

Therefore, we may now prove that RECPs of type II generalize RECPs of type I:

Theorem 3 *Take $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ and $\mathcal{B} \subseteq \mathbb{F}_{q^m}^m$. If $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$ (in the basis α), then $(M_\alpha(\mathcal{A}), M_\alpha(\mathcal{B}))$ is a t-RECP of type II for $M_{\alpha'}(\mathcal{C})$.*

Proof Using Lemma 7 and Proposition 2, we obtain that

$$M_\alpha(\mathcal{B}) M_\alpha(\mathcal{A}) = M_\alpha(\mathcal{B} \star \mathcal{A}) \subseteq M_\alpha(\mathcal{C}^\perp) = M_{\alpha'}(\mathcal{C})^*,$$

and the first condition is satisfied.

The second condition follows from the fact that $\dim_{\mathbb{F}_q}(\mathcal{A}) = m \dim_{\mathbb{F}_{q^m}}(\mathcal{A})$, and M_α is an $\mathbb{F}_q$-linear vector space isomorphism.

Finally, the third condition follows from Lemma 8 and the fourth condition remains unchanged. Hence the result follows.

Observe that in the same way, t-rank error-locating pairs of type II generalize t-rank error-locating pairs of type I.

6 MRD codes and bounds on the minimum rank distance

In this section we will give bounds on the minimum rank distance of codes that follow from the properties of rank error-correcting pairs, in a similar way to the bounds in [22]. We will also see that, in some cases, MRD conditions on two of the codes imply that the third is also MRD.

We will fix $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ and $\mathcal{B} \subseteq \mathbb{F}_q^{m \times m}$. Due to Lemmas 7 and 8, and Proposition 2, the results in this section may be directly translated into results where we consider the "extension" inner product $\cdot$ and $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$.

We will make use of the following consequence of the Singleton bound:

Lemma 9 *For every $\mathbb{F}_q$-linear code $\mathcal{D} \subseteq \mathbb{F}_q^{m \times n}$ it holds that*

$$d_R(\mathcal{D}) + d_R(\mathcal{D}^*) \leq n + 2.$$

Proof The Singleton bound implies that

$$\dim_{\mathbb{F}_q}(\mathcal{D})/m \leq n - d_R(\mathcal{D}) + 1, \quad \text{and} \quad \dim_{\mathbb{F}_q}(\mathcal{D}^*)/m \leq n - d_R(\mathcal{D}^*) + 1.$$

Adding both inequalities up and using that $\dim_{\mathbb{F}_q}(\mathcal{D}) + \dim_{\mathbb{F}_q}(\mathcal{D}^*) = mn$, the result follows.

Proposition 7 *Assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$. If $d_R(\mathcal{A}^*) > a > 0$ and $d_R(\mathcal{B}^*) > b > 0$, then $d_R(\mathcal{C}) \geq a + b$.*

Proof Take $C \in \mathcal{C}$ and $A \in \mathcal{A}$, and define $\mathcal{L} = \mathrm{Row}(C) \subseteq \mathbb{F}_q^n$. By Lemma 4, we have that

$$0 = \langle BA, C \rangle = \langle B^T, AC^T \rangle,$$

for all $B \in \mathcal{B}$ and all $A \in \mathcal{A}$, which means that the $\mathbb{F}_q$-linear space $\mathcal{A}(C) = \{AC^T \mid A \in \mathcal{A}\} \subseteq (\mathcal{B}^T)^*$, and hence $d_R(\mathcal{A}(C)) > b$.

Let G be a $t \times n$ generator matrix over $\mathbb{F}_q$ of $\mathcal{L}$ (where $t = \mathrm{Rk}(C)$). Taking a subset of rows of C that generate $\mathcal{L}$, we see that $\mathcal{A}(C)$ is $\mathbb{F}_q$-linearly isomorphic and rank-metric equivalent to $\mathcal{A}_1 = \{AG^T \mid A \in \mathcal{A}\} \subseteq \mathbb{F}_q^{m\times t}$. Take $D \in \mathcal{A}_1^*$. For every $A \in \mathcal{A}$, it holds that

$$\langle A, DG \rangle = \langle AG^T, D \rangle = 0,$$

by Lemma 4. Therefore, $DG \in \mathcal{A}^*$. Moreover, $\mathrm{Rk}(D) = \mathrm{Rk}(DG)$ since G is full rank, and hence $\mathrm{Rk}(D) > a$. Therefore, $d_R(\mathcal{A}_1^*) > a$. Together with $d_R(\mathcal{A}_1) > b$ and the previous lemma, we obtain that

$$a + 1 + b + 1 \leq d_R(\mathcal{A}_1) + d_R(\mathcal{A}_1^*) \leq t + 2,$$

that is, $t \geq a + b$, and the result follows.

We obtain the following corollary on MRD codes:

Corollary 1 *Assume that $n \leq m$ (otherwise, take transposed matrices), $d_R(\mathcal{A}) = n - t$, $\dim_{\mathbb{F}_q}(\mathcal{A}) = m(t+1)$, $d_R(\mathcal{B}) = m - t + 1$ and $\dim_{\mathbb{F}_q}(\mathcal{B}) = mt$. Then, for all $\mathcal{D} \subseteq (\mathcal{B}\mathcal{A})^*$, it holds that $d_R(\mathcal{D}) \geq 2t+1$ and $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{D}$.*

Proof $\mathcal{A}$ and $\mathcal{B}$ are MRD codes, since their minimum rank distance attains the Singleton bound. By [5, Theorem 5.5] (see also [23, Corollary 41]), $\mathcal{A}^*$ and $\mathcal{B}^*$ are also MRD, which implies that

$$d_R(\mathcal{A}^*) > t + 1, \quad \text{and} \quad d_R(\mathcal{B}^*) > t.$$

By the previous proposition, it holds that $d_R(\mathcal{D}) \geq 2t + 1$. We see that the properties of RECPs of type II are satisfied, and the result follows.

Now we obtain bounds on $d_R(\mathcal{A})$ from bounds on $d_R(\mathcal{B}^*)$ and $d_R(\mathcal{C}^*)$:

Proposition 8 *Assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$. If $d_R(\mathcal{B}^*) > b > 0$ and $d_R(\mathcal{C}^*) > c > 0$, then $d_R(\mathcal{A}) \geq b + c$.*

Proof The proof is analogous to the proof of Proposition 7. In this case, we fix $A \in \mathcal{A}$, with $\mathcal{L} = \mathrm{Row}(A)$, $t = \mathrm{Rk}(A)$, and consider $A(\mathcal{C}) = \{AC^T \mid C \in \mathcal{C}\}$. The rest of the proof follows the same lines, interchanging the roles of $\mathcal{A}$ and $\mathcal{C}$, and using the fact that $\langle BA, C \rangle = \langle B^T C, A \rangle$, from Lemma 4, and $d_R(\mathcal{B}^*) = d_R((\mathcal{B}^T)^*)$.

Again, we may give the following corollary on MRD codes:

Corollary 2 *Assume that $\mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*$ and $n \leq m$. If $d_R(\mathcal{C}) = 2t + 1$, $\dim_{\mathbb{F}_q}(\mathcal{C}) = m(n - 2t)$ and $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{C}$, then $d_R(\mathcal{A}) \geq n - t$ and $mt < \dim_{\mathbb{F}_q}(\mathcal{A}) \leq m(t + 1)$. If $\dim_{\mathbb{F}_q}(\mathcal{A})$ is a multiple of m (in particular, if $M^{-1}(\mathcal{A})$ is $\mathbb{F}_{q^m}$-linear), then $\mathcal{A}$ is MRD.*

Proof By the properties of RECPs of type II, we have that $d_R(\mathcal{B}^*) > t$, and since $\mathcal{C}$ is MRD, then $\mathcal{C}^*$ is also MRD and we have that $d_R(\mathcal{C}^*) = n - 2t + 1$. Therefore, $d_R(\mathcal{A}) \geq n - t$ by the previous proposition. By the properties of RECPs of type II, $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$, and we are done. The last statement follows from the Singleton bound for $\mathcal{A}$.

We now turn to a bound analogous to [22, Proposition 3.1]. The BCH bound on the minimum Hamming distance of cyclic codes is generalized by the Hartmann-Tzeng bounds [11] and further generalized by the Roos bound [24, 25]. The next proposition is the rank-metric equivalent of the Roos bound [24, 25] for the Hamming metric, as mentioned in [8, Proposition 5].

Proposition 9 *Assume the following properties for $a, b > 0$:*

$$(1)\ \mathcal{B}\mathcal{A} \subseteq \mathcal{C}^*, \quad (2)\ \dim_{\mathbb{F}_q}(\mathcal{A}) > ma, \quad (3)\ d_R(\mathcal{B}^*) > b,$$

$$(4)\ d_R(\mathcal{A}) + a + b > n, \quad \textit{and} \quad (5)\ d_R(\mathcal{A}^*) > 1.$$

Then it holds that $d_R(\mathcal{C}) > a + b$.

Proof Take $C \in \mathcal{C}$ and let $\mathcal{L} = \mathrm{Row}(C) \subseteq \mathbb{F}_q^n$ and $t = \mathrm{Rk}(C)$. Conditions (1), (3) and (5) imply that $t > b$ by Proposition 7.

Assume that $b < t \leq a + b$. Take linear subspaces $\mathcal{L}_-, \mathcal{L}_+, \mathcal{U} \subseteq \mathbb{F}_q^n$ such that $\mathcal{L}_- \subseteq \mathcal{L} \subseteq \mathcal{L}_+$, $\mathcal{L}_+ = \mathcal{U} \oplus \mathcal{L}_-$, $b = \dim(\mathcal{L}_-)$ and $a + b = \dim(\mathcal{L}_+)$. Since $m \dim(\mathcal{U}) = ma < \dim_{\mathbb{F}_q}(\mathcal{A})$ by condition (2), we have that $\mathcal{A}(\mathcal{U}) \neq 0$, and therefore there exists a non-zero $A \in \mathcal{A}$ with $\mathrm{Row}(A) \subseteq \mathcal{U}^\perp$.

It holds that every row in C is in $\mathcal{L}_+$. Since the rows in A are in $\mathcal{U}^\perp$, it holds that $AC^T = AN^T$, where N is obtained from C by substituting every row by its projection from $\mathcal{U} \oplus \mathcal{L}_-$ to $\mathcal{L}_-$.

Therefore $\mathrm{Rk}(AC^T) \leq \mathrm{Rk}(N) \leq \dim(\mathcal{L}_-) = b$, but $AC^T \in (\mathcal{B}^T)^*$ by condition (1) and Lemma 4, and hence $AC^T = 0$ by condition (3). This means that $\mathrm{Row}(A) \subseteq \mathcal{L}_-^\perp \cap \mathcal{U}^\perp = \mathcal{L}_+^\perp$. Thus, $\mathrm{Rk}(A) \leq n - a - b < d_R(\mathcal{A})$, which is absurd by condition (4), since $A \neq 0$. We conclude that $t > a + b$ and we are done.

Taking $a = b = t$ for some $t > 0$, where a and b are as in the previous proof, we obtain the following particular case:

Corollary 3 *For all $\mathbb{F}_q$-linear codes $\mathcal{D} \subseteq (\mathcal{B}\mathcal{A})^*$ such that $\dim_{\mathbb{F}_q}(\mathcal{A}) > mt$, $d_R(\mathcal{B}^*) > t$, $d_R(\mathcal{A}) > n - 2t$ and $d_R(\mathcal{A}^*) > 1$, it holds that $d_R(\mathcal{D}) \geq 2t + 1$ and $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type II for $\mathcal{D}$.*

Observe that the previous result states that, if some conditions on $\mathcal{A}$ and $\mathcal{B}$ hold, then they form a t-RECP of type II for all $\mathbb{F}_q$-linear codes contained in $(\mathcal{B}\mathcal{A})^*$. That is, we have found a t-rank error-correcting algorithm for all $\mathbb{F}_q$-linear subcodes of $(\mathcal{B}\mathcal{A})^*$.

7 Some codes with a t-RECP

In this section, we study families of codes that admit a t-RECP of some type.

7.1 Hamming-metric codes with ECPs

Take $\mathbb{F}_q$-linear codes $\mathcal{A}, \mathcal{B}, \mathcal{C} \subseteq \mathbb{F}_q^n$ such that $(\mathcal{A}, \mathcal{B})$ is a t-ECP for $\mathcal{C}$ in the Hamming metric. We will see that the algorithm presented in Theorem 2 is actually an extension of the decoding algorithm in the Hamming metric using t-ECPs [20, 21]. We observe the following (recall the definition of D in (2)):

Remark 5 For all $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$, it holds that

$$\mathbf{a} \cdot \mathbf{b} = \langle D(\mathbf{a}), D(\mathbf{b}) \rangle.$$

Moreover, it holds that

$$D(\mathcal{B})D(\mathcal{A}) \subseteq D(\mathcal{C})^*.$$

Therefore, from the previous remark and the properties of D, the $\mathbb{F}_q$-linear codes $D(\mathcal{A}), D(\mathcal{B}), D(\mathcal{C}) \subseteq \mathbb{F}_q^{n \times n}$ satisfy the following conditions:

1. $D(\mathcal{B})D(\mathcal{A}) \subseteq D(\mathcal{C})^*$.
2. $\dim_{\mathbb{F}_q}(D(\mathcal{A})) > t$.
3. $d_R(D(\mathcal{B})^*) = 1$.
4. $d_R(D(\mathcal{A})) + d_R(D(\mathcal{C})) > n$.

That is, $(D(\mathcal{A}), D(\mathcal{B}))$ satisfy the same conditions as t-RECPs of type II for $D(\mathcal{C})$, except that conditions 2 and 3 are weakened. However, the previous conditions are enough to correct any error $D(\mathbf{e}) \in \mathbb{F}_q^{n \times n}$, where $\mathbf{e} \in \mathbb{F}_q^n$ and $\mathrm{wt_H}(\mathbf{e}) \leq t$,

Assume the received vector is $R = D(\mathbf{c}) + D(\mathbf{e})$, with $\mathbf{c} \in \mathcal{C}$ and $\mathrm{wt_H}(\mathbf{e}) \leq t$. Correcting the diagonal of $R = D(\mathbf{c}) + D(\mathbf{e})$ for the Hamming metric is the same as correcting the matrix $R = D(\mathbf{c}) + D(\mathbf{e})$ itself for the rank metric. We will next show that the algorithm in Theorem 2 is exactly the same as the algorithm for ECPs in the Hamming metric.

Define $I \subseteq \{1, 2, \ldots, n\}$ as the Hamming support of $\mathbf{e} \in \mathbb{F}_q^n$, that is, $I = \mathrm{HSupp}(\mathbf{e}) = \{i \in \{1, 2, \ldots, n\} \mid e_i \neq 0\}$, and define

$$\mathcal{K}_H(\mathbf{e}) = \{\mathbf{a} \in \mathcal{A} \mid (\mathbf{b} * \mathbf{a}) \cdot \mathbf{e} = 0, \forall \mathbf{b} \in \mathcal{B}\}, \text{ and}$$

$$\mathcal{A}(I) = \{\mathbf{a} \in \mathcal{A} \mid \mathrm{HSupp}(\mathbf{a}) \subseteq I^c\},$$

where I^c denotes the complementary of I. It holds that $\mathrm{Row}(D(\mathbf{e})) = \mathcal{L}_I \subseteq \mathbb{F}_q^n$, the space generated by the vectors $\mathbf{e}_i$ in the canonical basis, for $i \in I$. Therefore, by Remark 5, the properties of D, Proposition 2 and the fact that $\mathcal{L}_I^\perp = \mathcal{L}_{I^c}$, it holds that

$$\mathcal{K}(R) = \mathcal{K}(D(\mathbf{e})) = D(\mathcal{K}_H(\mathbf{e})) \quad \text{and} \quad (D(\mathcal{A}))(\mathcal{L}_I) = D(\mathcal{A}(I)).$$

Moreover, since $\mathcal{A}(I) = \mathcal{K}_H(\mathbf{e})$ by the properties of ECPs in the Hamming metric, we also have that

$$\mathcal{K}(R) = D(\mathcal{K}_H(\mathbf{e})) = D(\mathcal{A}(I)) = (D(\mathcal{A}))(\mathcal{L}_I).$$

Hence, computing $\mathcal{K}(R)$ implies computing $(D(\mathcal{A}))(\mathcal{L}_I)$. Finally, since $\mathcal{A}(I) \neq 0$ by the properties of ECPs, we have that $(D(\mathcal{A}))(\mathcal{L}_I) \neq 0$. The rest of the algorithm goes in the same way as in Theorem 2. That is, the decoding algorithm in Theorem 2 actually extends the decoding algorithm given by ECPs in the Hamming metric.

7.2 Gabidulin codes

Gabidulin codes, introduced in [9], are a well-known family of MRD $\mathbb{F}_{q^m}$-linear codes in $\mathbb{F}_{q^m}^n$, when $n \leq m$. In [15], a generalization of these codes is given, also formed by MRD codes.

Fix $n \leq m$. They can be defined as follows. For each $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_{q^m}^n$, where $b_1, b_2, \ldots, b_n$ are linearly independent over $\mathbb{F}_q$, each $k = 1, 2, \ldots, n$ and each integer r such that r and m are coprime, we define the (generalized) Gabidulin code of dimension k in $\mathbb{F}_{q^m}^n$ as

$$\mathrm{Gab}_{k,m,n}(r, \mathbf{b}) = \{(F(b_1), F(b_2), \ldots, F(b_n)) \mid F \in \mathcal{L}_{q,r,k}\mathbb{F}_{q^m}[x]\},$$

where $\mathcal{L}_{q,r,k}\mathbb{F}_{q^m}[x]$ denotes the $\mathbb{F}_{q^m}$-linear space of q-linearized polynomials of the form

$$F(x) = a_0 x + a_1 x^{[r]} + a_2 x^{[2r]} + a_3 x^{[3r]} + \cdots + a_{k-1} x^{[(k-1)r]},$$

for some $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^m}$. Observe that classical Gabidulin codes as defined in [9] are obtained by setting $r = 1$. Also observe that, for any invertible matrix $P \in \mathbb{F}_q^{n \times n}$, it holds that

$$\mathrm{Gab}_{k,m,n}(r, \mathbf{b})P = \mathrm{Gab}_{k,m,n}(r, \mathbf{b}P),$$

and hence $\mathbb{F}_{q^m}$-linearly rank-metric equivalent codes to Gabidulin codes are again Gabidulin codes.

The following lemma follows from Proposition 1:

Lemma 10 *For every positive integers k, l with $k + l - 1 \leq n$, it holds that*

$$\mathrm{Gab}_{k,m,m}(r, \boldsymbol{\alpha}) \star \mathrm{Gab}_{l,m,n}(r, \mathbf{b}) = \mathrm{Gab}_{k+l-1,m,n}(r, \mathbf{b}).$$

In the case $r = 1$, it holds that

$$\mathrm{Gab}_{k,m,n}(1, \boldsymbol{\alpha}_n) \star \mathrm{Gab}_{l,m,n}(1, \mathbf{b}) = \mathrm{Gab}_{k+l-1,m,n}(1, \mathbf{b}).$$

On the other hand, for $r = 1$ and the maps φ_n, the following lemma follows from the definitions:

Lemma 11 *It holds that*

$$\varphi_n(\mathrm{Gab}_{k,m,n}(1, \boldsymbol{\alpha}_n)) = \mathrm{Gab}_{k,m,m}(1, \boldsymbol{\alpha}).$$

With these two lemmas, we can prove that Gabidulin codes have t-RECP of type I. Recall from [15] that

$$\mathrm{Gab}_{k,m,n}(r, \mathbf{b})^\perp = \mathrm{Gab}_{n-k,m,n}(r, \mathbf{b}'),$$

for some $\mathbf{b}' \in \mathbb{F}_{q^m}^n$ that can be computed from $\mathbf{b}$.

Theorem 4 *If $t > 0$, $\mathcal{A} = \mathrm{Gab}_{t+1,m,n}(r, \mathbf{b})$, $\mathcal{B} = \mathrm{Gab}_{t,m,m}(r, \boldsymbol{\alpha})$ and $\mathcal{C} = \mathrm{Gab}_{2t,m,n}(r, \mathbf{b})^\perp$, then $(\mathcal{A}, \mathcal{B})$ is a t-RECP of type I for $\mathcal{C}$. In the case $r = 1$, we may take $\mathcal{B} = \mathrm{Gab}_{t,m,n}(r, \boldsymbol{\alpha}_n)$.*

Proof The first condition follows from Lemma 10. On the other hand, $\dim_{\mathbb{F}_{q^m}}(\mathcal{A}) = t+1$, so the second condition follows. The third condition is trivial, and for the case $r = 1$ and $\mathcal{B} = \mathrm{Gab}_{t,m,n}(1, \boldsymbol{\alpha}_n)$ it follows from Lemma 11. Finally, the fourth condition follows from the following computation:

$$d_R(\mathcal{A}) + d_R(\mathcal{C}) = n - t + 2t + 1 = n + t + 1.$$

We see that $d_R(\mathcal{A}) = n - t > n - 2t$. Hence, the pair $(M_\alpha(\mathcal{A}), M_\alpha(\mathcal{B}))$, with notation as in Section 5, can be used by Corollary 3 to efficiently correct any error of rank at most t for every $\mathbb{F}_q$-linear subcode of a (generalized) Gabidulin code. Such efficient decoding algorithms seem not to have been obtained yet.

Corollary 4 *Let $t, \mathcal{A}, \mathcal{B}$ and $\mathcal{C}$ be as in the previous theorem. Then, for every $\mathbb{F}_q$-linear subcode $\mathcal{D} \subseteq \mathcal{C}$, the pair $(M_\alpha(\mathcal{A}), M_\alpha(\mathcal{B}))$ is a t-RECP of type II for $M_{\alpha'}(\mathcal{D})$.*

Proof It follows from the previous theorem, Theorem 3 and Corollary 3.

On the other hand, decoding algorithms for generalized Gabidulin codes with $r \neq 1$ seem to have been obtained only in [15], also of cubic complexity.

7.3 Skew cyclic codes

Skew cyclic codes (or q^r-cyclic codes) play the same role as cyclic codes in the theory of error-correcting codes for the rank metric. They were originally introduced in [9] for $r = 1$ and $m = n$, and further generalized in [10] for $r = 1$ and any m and n, and for any r in the work by Ulmer et al. [2,3]. In this subsection we will only treat the case $r = 1$.

Assume that $n = sm$ is a multiple of m. We will see in this subsection that, in that case, some $\mathbb{F}_{q^m}$-linear q-cyclic codes have rank error-locating pairs of type I, in analogy to the ideas in [7]. We say that an $\mathbb{F}_{q^m}$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ is q-cyclic if the q-shifted vector

$$(c_{n-1}^q, c_0^q, c_1^q, \ldots, c_{n-2}^q)$$

lies in $\mathcal{C}$, for every $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$. As in [18], we say that an $\mathbb{F}_q$-linear subspace $\mathcal{T} \subseteq \mathbb{F}_{q^n}$ is a q-root space (over $\mathbb{F}_{q^m}$) if it is the root space in $\mathbb{F}_{q^n}$ of a linearized polynomial in $\mathcal{L}_q\mathbb{F}_{q^m}[x]$.

By [18, Theorem 3], $\mathbb{F}_{q^m}$-linear q-cyclic codes are codes in $\mathbb{F}_{q^m}^n$ with a parity check matrix over $\mathbb{F}_{q^n}$ of the form

$$\mathcal{M}(\beta_1, \beta_2, \ldots, \beta_{n-k}) = \begin{pmatrix} \beta_1 & \beta_1^{[1]} & \beta_1^{[2]} & \ldots & \beta_1^{[n-1]} \\ \beta_2 & \beta_2^{[1]} & \beta_2^{[2]} & \ldots & \beta_2^{[n-1]} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_{n-k} & \beta_{n-k}^{[1]} & \beta_{n-k}^{[2]} & \ldots & \beta_{n-k}^{[n-1]} \end{pmatrix},$$

where $\beta_1, \beta_2, \ldots, \beta_{n-k}$ is a basis of $\mathcal{T}$ over $\mathbb{F}_q$, for some q-root space $\mathcal{T}$. Moreover by [18, Corollary 2], $\mathbb{F}_{q^m}$-linear q-cyclic codes are in bijection with q-root spaces over $\mathbb{F}_{q^m}$.

The next bound, which is given in [18, Corollary 4], is an extension of the rank-metric version of the BCH bound (by setting $w = 0$ and $c = 1$) found in [3, Proposition 1]:

Lemma 12 (Rank-HT bound) *Let b, c, δ and w be positive integers with $\delta + w \leq m$ and $d = \gcd(c,n) < \delta$, and $\alpha \in \mathbb{F}_{q^n}$ be such that the set $\mathcal{A} = \{\alpha^{[b+i+jc]} \mid 0 \leq i \leq \delta - 2, 0 \leq j \leq w\}$ is a linearly independent set of vectors.*

If $\mathcal{C}$ is the $\mathbb{F}_{q^m}$-linear q-cyclic code corresponding to the q-root space $\mathcal{T}$ and $\mathcal{A} \subseteq \mathcal{T}$, then $d_R(\mathcal{C}) \geq \delta + w$.

To use it, we need to deal with normal bases. First, it is well-known [16] that the orthogonal (or dual) basis of a normal basis $\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]} \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is again a normal basis $\beta, \beta^{[1]}, \ldots, \beta^{[n-1]} \in \mathbb{F}_{q^n}$. Define $\boldsymbol{\alpha} = (\alpha, \alpha^{[1]}, \ldots, \alpha^{[n-1]})$ and $\boldsymbol{\beta} = (\beta, \beta^{[1]}, \ldots, \beta^{[n-1]})$. Then it holds that

$$\boldsymbol{\alpha}^{[i]} \cdot \boldsymbol{\beta}^{[j]} = \mathrm{Tr}(\alpha^{[i]}\beta^{[j]}) = \delta_{i,j}$$

by definition. On the other hand, for a subset $I \subseteq \{1, 2, \ldots, n\}$, define the matrix

$$\mathcal{M}_{\boldsymbol{\alpha}}(I) = \mathcal{M}(\alpha^{[i]} \mid i \in I),$$

and similarly for $\boldsymbol{\beta}$.

Define the $\mathbb{F}_{q^m}$-linear codes $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_{q^m}^n$ as the subfield subcodes of the codes in $\mathbb{F}_{q^n}^n$ with generator matrices $\mathcal{M}_{\boldsymbol{\alpha}}(I)$ and $\mathcal{M}_{\boldsymbol{\alpha}}(J)$, for some subsets $I, J \subseteq \{1, 2, \ldots, n\}$, respectively.

In order to obtain q-cyclic codes, we will assume that the space generated by $\{\alpha^{[i]} \mid i \in I\}$ is a q-root space, and similarly for J. Due to the cyclotomic space description of q-root spaces in [18, Proposition 2], this holds if the following condition holds: if $i \in I$, then $i + m \in I$ (modulo n), and similarly for J.

Define the $\mathbb{F}_{q^m}$-linear q-cyclic code $\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ with parity check matrix $\mathcal{M}_{\boldsymbol{\alpha}}(I + J)$. Observe that $I + J$ also gives a q-root space by the previous paragraph. We have the following lemmas:

Lemma 13 *$\mathcal{A}$ and $\mathcal{B}$ are the q-cyclic codes with parity check matrices $\mathcal{M}_{\boldsymbol{\beta}}(I^c)$ and $\mathcal{M}_{\boldsymbol{\beta}}(J^c)$ over $\mathbb{F}_{q^n}$, respectively.*

Proof We prove it for $\mathcal{A}$. Define $\widetilde{\mathcal{A}}$ as the $\mathbb{F}_{q^n}$-linear code in $\mathbb{F}_{q^n}^n$ with generator matrix $\mathcal{M}_{\boldsymbol{\alpha}}(I)$. It is enough to prove that $\mathcal{M}_{\boldsymbol{\beta}}(I^c)$ is a parity check matrix for $\widetilde{\mathcal{A}}$.

However, since $\boldsymbol{\alpha}^{[i]} \cdot \boldsymbol{\beta}^{[j]} = 0$, for every $i \in I$ and $j \notin I$, it holds that $\mathcal{M}_{\boldsymbol{\alpha}}(I)\mathcal{M}_{\boldsymbol{\beta}}(I^c)^T = 0$. On the other hand, these two matrices are full rank and the number of rows in $\mathcal{M}_{\boldsymbol{\alpha}}(I)$ together with the number of rows in $\mathcal{M}_{\boldsymbol{\beta}}(I^c)$ is $\#I + \#(I^c) = n$, and the result follows.

Lemma 14 *It holds that $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$.*

Proof By Proposition 1, item 2, we see that $\mathcal{B} \star \mathcal{A}$ is contained in the $\mathbb{F}_{q^n}$-linear code with generator matrix $\mathcal{M}_{\boldsymbol{\alpha}}(I+J)$. Denote such code by $\mathcal{D}$, that is, $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{D}$ and $\mathcal{D} \subseteq \mathbb{F}_{q^n}^n$.

By definition, $\mathcal{C} = \mathcal{D}^\perp \cap \mathbb{F}_{q^m}^n$, and by [18, Corollary 3], $\mathcal{D}$ is Galois closed over $\mathbb{F}_{q^m}$, which means that $\mathcal{D}^\perp \cap \mathbb{F}_{q^m}^n = (\mathcal{D} \cap \mathbb{F}_{q^m}^n)^\perp$ by [19, Proposition 2] and Delsarte's theorem [6, Theorem 2]. Hence

$$\mathcal{B} \star \mathcal{A} \subseteq \mathcal{D} \cap \mathbb{F}_{q^m}^n = (\mathcal{D}^\perp \cap \mathbb{F}_{q^m}^n)^\perp = \mathcal{C}^\perp.$$

We may now prove that $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type I (see Remark 3) for $\mathcal{C}$, and with some stronger hypotheses, it is also a t-rank error-correcting pair for $\mathcal{C}$.

Theorem 5 *Fix a positive integer t and assume that $\#I > t$ and J contains $\delta - 1$ consecutive elements, for some $\delta > t$. Then $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair for $\mathcal{C}$. If moreover, $d_R(\mathcal{A}) + d_R(\mathcal{C}) > n$, then $(\mathcal{A}, \mathcal{B})$ is a t-rank error-correcting pair of type I for $\mathcal{C}$.*

Proof From the previous lemma, we have that $\mathcal{B} \star \mathcal{A} \subseteq \mathcal{C}^\perp$. On the other hand, $\mathcal{A}$ satisfies that $\dim(\mathcal{A}) = \#I > t$, and $\mathcal{B}$ satisfies that $d_R(\mathcal{B}^\perp) \geq \delta > t$ by Lemma 12. Then $(\mathcal{A}, \mathcal{B})$ is a t-rank error-locating pair of type I for $\mathcal{C}$.

Observe that we may obtain the bound $d_R(\mathcal{C}) \geq \delta + w$ by Proposition 7 assuming that I contains the elements ic, for $0 \leq i \leq w$. This means that, for q-cyclic codes constructed with a normal basis, the rank-HT bound found in [18, Corollary 4] is implied by Proposition 7, as in the classical case. Further cases are left open.

Acknowledgements Rank error-correcting pairs of type II have been obtained in the case $m = n$ independently by Alain Couvreur [4]. The authors wish to thank him for this communication and for useful discussions and comments.

The authors also gratefully acknowledge the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367). This paper was started during the visit of the second author to Aalborg University, Denmark, which was supported by the previous grant.

References

1. T.P. Berger. Isometries for rank distance and permutation group of Gabidulin codes. *IEEE Transactions Information Theory*, 49(11):3016–3019, 2003.
2. D. Boucher, W. Geiselmann, and F. Ulmer. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing*, 18(4):379–389, 2007.
3. L. Chaussade, P. Loidreau, and F. Ulmer. Skew codes of prescribed distance or rank. *Designs, Codes and Cryptography*, 50(3):267–284, 2009.
4. A. Couvreur. About error correcting pairs. Personal communication. September 15, 2015.
5. P. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *Journal of Combinatorial Theory, Series A*, 25(3):226 – 241, 1978.
6. P. Delsarte. On subfield subcodes of modified reed-solomon codes (corresp.). *IEEE Transactions Information Theory*, 21(5):575–576, September 2006.
7. I.M. Duursma and R. Kötter. Error-locating pairs for cyclic codes. *IEEE Transactions on Information Theory*, 40(4):1108–1121, 1994.
8. I.M. Duursma and R. Pellikaan. A symmetric Roos bound for linear codes. *Journal of Combinatorial Theory, Series A*, 113(8):1677–1688, 2006.
9. E.M. Gabidulin. Theory of codes with maximum rank distance. *Problems Information Transmission*, 21, 1985.
10. E.M. Gabidulin. Rank q-cyclic and pseudo-q-cyclic codes. In *IEEE International Symposium on Information Theory, 2009. ISIT 2009*, pages 2799–2802, 2009.
11. C.R.P. Hartmann and K.K. Tzeng. Generalizations of the BCH bound. *Information and Control*, 20(5):489 – 498, 1972.
12. R.P.M.J. Jurrius and R. Pellikaan. The extended and generalized rank weight enumerator. ACA 2014, Applications of Computer Algebra, 9 July 2014, Fordham University, New York, Computer Algebra in Coding Theory and Cryptography, 2014.
13. R.P.M.J. Jurrius and R. Pellikaan. On defining generalized rank weights. *arXiv:1506.02865*, 2015.
14. R. Kötter. A unified description of an error locating procedure for linear codes. *Proceedings of Algebraic and Combinatorial Coding Theory*, pages 113 – 117, 1992. Voneshta Voda.

15. A. Kshevetskiy and E.M. Gabidulin. The new construction of rank codes. In *IEEE International Symposium on Information Theory, 2005. ISIT 2005*, pages 2105–2108, 2005.
16. R. Lidl and H. Niederreiter. *Finite Fields.*, volume 20. Encyclopedia of Mathematics and its Applications. Addison-Wesley, Amsterdam, 1983.
17. Pierre Loidreau. A WelchBerlekamp like algorithm for decoding Gabidulin codes. In yvind Ytrehus, editor, *Coding and Cryptography*, volume 3969 of *Lecture Notes in Computer Science*, pages 36–45. Springer Berlin Heidelberg, 2006.
18. U. Martínez-Peñas. On the roots and minimum rank distance of skew cyclic codes. *arXiv:1511.09329*, 2015.
19. U. Martínez-Peñas. On the similarities between generalized rank and Hamming weights and their applications to network coding. *IEEE Transactions on Information Theory*, 62(7):1–15, 2016.
20. R. Pellikaan. On decoding linear codes by error correcting pairs. *Preprint. Eindhoven University of Technology*, 1988.
21. R. Pellikaan. On decoding by error location and dependent sets of error positions. *Discrete Mathematics*, 106:369–381, 1992.
22. R. Pellikaan. On the existence of error-correcting pairs. *Journal of Statistical Planning and Inference*, 51(2):229 – 242, 1996. Shanghai Conference Issue on Designs, Codes, and Finite Geometries, Part I.
23. A. Ravagnani. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography*, pages 1–20, 2015.
24. C. Roos. A generalization of the BCH bound for cyclic codes, including the Hartmann-Tzeng bound. *Journal Combinatorial Theory (Series A)*, 33:229–232, 1982.
25. C. Roos. A new lower bound for the minimum distance of a cyclic code. *IEEE Transactions Information Theory*, IT-29:330–332, 1982.
26. D. Silva and F.R. Kschischang. On metrics for error correction in network coding. *IEEE Transactions Information Theory*, 55(12):5479–5490, 2009.