$\mathbb{F}_{q^n}$-linear rank distance codes and their distinguishers[*]

Luca Giuzzi[1][0000−0003−3975−7281] and Ferdinando Zullo[2][0000−0002−5087−2363]

[1] D.I.C.A.T.A.M. (Section of Mathematics), University of Brescia, Brescia, Italy
luca.giuzzi@unibs.it
[2] Department of Mathematics and Physics, University of Campania "*Luigi Vanvitelli*", Caserta, Italy
ferdinando.zullo@unicampania.it

Abstract. For any admissible value of the parameters there exist Maximum Rank distance (shortly MRD) $\mathbb{F}_{q^n}$-linear codes of $\mathbb{F}_q^{n \times n}$ (see Subsection 1.1 for the definition). It has been shown in [19] (see also [2]) that, if field extensions large enough are considered, then *almost all* (rectangular) rank distance codes are MRD. On the other hand, very few families of $\mathbb{F}_{q^n}$-linear codes are currently known up to equivalence. One of the possible applications of MRD-codes is for McEliece–like public key cryptosystems, as proposed by Gabidulin, Paramonov and Tretjakov in [8]. In this framework it is very important to obtain new families of MRD-codes endowed with fast decoding algorithms. Several decoding algorithms exist for Gabidulin codes as shown in [7], see also [15,20,24]. In this work, we will survey the known families of $\mathbb{F}_{q^n}$-linear MRD-codes, study some invariants of MRD-codes and evaluate their value for the known families, providing a characterization of generalized twisted Gabidulin codes as done in [9].

Keywords: Rank distance codes · Distinguishers · Linearized polynomials.

1 Introduction

Delsarte [6] introduced rank-distance (RD) codes in 1978 as the q-analogs of the usual linear error correcting codes endowed with Hamming distance. The set of $m \times n$ matrices $\mathbb{F}_q^{m \times n}$ over $\mathbb{F}_q$ is a rank metric $\mathbb{F}_q$-space where the rank metric distance is given by

$$d(A, B) = \operatorname{rk}(A - B)$$

for $A, B \in \mathbb{F}_q^{m \times n}$.

A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ is called a *rank distance code* (RD-code for short). The minimum distance of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min_{A,B \in \mathcal{C},\ A \neq B} \{d(A,B)\}.$$

We say that $\mathcal{C}$ has parameters $(n,m,q;d)$, where d is the minimum distance of $\mathcal{C}$. When $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m \times n}$, we say that $\mathcal{C}$ is an $\mathbb{F}_q$-*linear* RD-code and its dimension $\dim_{\mathbb{F}_q} \mathcal{C}$ is defined the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$. In [6], Delsarte also showed that the parameters of these RD-codes must obey a Singleton-like bound:

Theorem 1. *Let $\mathcal{C}$ be an RD-code of $\mathbb{F}_q^{m \times n}$ and let d its minimum distance, then*

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

When the equality holds, $\mathcal{C}$ is a *maximum rank distance* (*MRD* for short) code. Examples of MRD-codes were first found by Delsarte in [6] and rediscovered by Gabidulin in [7] and by Roth in [22]. For $m \neq n$ two RD-codes $\mathcal{C}$ and $\mathcal{C}'$ are said to be equivalent if and only if there exist $X \in \mathrm{GL}(m,q)$, $Y \in \mathrm{GL}(n,q)$, $Z \in \mathbb{F}_q^{m \times n}$ and a field automorphism σ of $\mathbb{F}_q$ such that

$$\mathcal{C}' = \{XC^\sigma Y + Z \colon C \in \mathcal{C}\}.$$

When $m = n$ we have two possible definitions:

1. $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if there are invertible matrices $X, Y \in \mathbb{F}_q^{n \times n}$, $Z \in \mathbb{F}_q^{n \times n}$ and a field automorphism σ of $\mathbb{F}_q$ such that

$$\mathcal{C}' = \{XC^\sigma Y + Z \colon C \in \mathcal{C}\}.$$

2. $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if there are invertible matrices $A, B \in \mathbb{F}_q^{n \times n}$, $Z \in \mathbb{F}_q^{n \times n}$ and a field automorphism σ of $\mathbb{F}_q$ such that

$$\mathcal{C}' = \{XC^\sigma Y + Z \colon C \in \mathcal{C}\} \text{ or } \mathcal{C}' = \{X(C^t)^\sigma Y + Z \colon C \in \mathcal{C}\}.$$

From now on when we will talk about the equivalence between two RD-codes of $\mathbb{F}_q^{n \times n}$ we will mean the first kind of equivalence mentioned above, otherwise we will talk about *strong equivalence*. Clearly, when $\mathcal{C}$ and $\mathcal{C}'$ are $\mathbb{F}_q$-linear, we may always assume that Z is the zero matrix. For further details on the equivalence of RD-codes see also [1,18].

Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ be an RD-code; the *adjoint code* of $\mathcal{C}$ is

$$\mathcal{C}^\top = \{C^t \colon C \in \mathcal{C}\}.$$

Consider the symmetric bilinear form $\langle \cdot, \cdot \rangle$ on $\mathbb{F}_q^{m \times n}$ given by

$$\langle M, N \rangle = \mathrm{Tr}(MN^t).$$

The *Delsarte-dual code* of an $\mathbb{F}_q$-linear RD-code $\mathcal{C}$ is

$$\mathcal{C}^{\perp} = \{N \in \mathbb{F}_q^{m \times n} \colon \langle M, N \rangle = 0 \text{ for each } M \in \mathcal{C}\}.$$

By using the machinery of association schemes, Delsarte in [6] proved the following result.

Lemma 1. *[6, Theorem 5.5] Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ be an $\mathbb{F}_q$-linear MRD-code of dimension k with $d > 1$. Then the Delsarte dual code $\mathcal{C}^{\perp} \subseteq \mathbb{F}_q^{m \times n}$ is an MRD-code of dimension $mn - k$.*

An elementary proof of the above result can be found in [21].

In general, it is difficult to determine whether two RD-codes are equivalent or not. The notion of *idealiser* provides a useful criterion.

Let $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$ be an RD-code; its *left* and *right idealisers* $L(\mathcal{C})$ and $R(\mathcal{C})$ are defined as
$$L(\mathcal{C}) = \{Y \in \mathbb{F}_q^{m \times m} \colon YC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$
$$R(\mathcal{C}) = \{Z \in \mathbb{F}_q^{n \times n} \colon CZ \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}.$$

These notions have been introduced by Liebhold and Nebe in [14, Definition 3.1]. The idealisers are subgroups of the automorphism group, which are easier to calculate. Such sets appear also in the paper of Lunardon, Trombetti and Zhou [16], where they are respectively called *middle nucleus* and *right nucleus*; therein the authors investigate these sets and, in particular, prove the following results.

Proposition 1. *[16, Proposition 4.1] If $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent $\mathbb{F}_q$-linear RD-codes of $\mathbb{F}_q^{m \times n}$, then their left (resp. right) idealisers are also equivalent as RD-codes.*

Theorem 2. *[16, Theorem 5.4 & Corollary 5.6] Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MRD-code of $\mathbb{F}_q^{m \times n}$ with minimum distance $d > 1$. If $m \leq n$, then $L(\mathcal{C})$ is a finite field with $|L(\mathcal{C})| \leq q^m$. If $m \geq n$, then $R(\mathcal{C})$ is a finite field with $|R(\mathcal{C})| \leq q^n$. In particular, when $m = n$ then $L(\mathcal{C})$ and $R(\mathcal{C})$ are both finite fields.*

1.1 Representation of RD-codes as q-polynomials

Any $\mathbb{F}_q$-linear RD-code over $\mathbb{F}_q$ can be equivalently regarded either as a subspace of matrices in $\mathbb{F}_q^{m \times n}$ or as a subspace of $\mathrm{Hom}(V_n, V_m)$. In the present section we shall recall a specialized representation for these codes in terms of linearized polynomials which we shall use in the rest of this abstract.

Consider two vector spaces V_n and V_m over $\mathbb{F}_q$ with dimension respectively n and m. If $n \geq m$ we can always regard V_m as a subspace of V_n and identify $\mathrm{Hom}(V_n, V_m)$ with the subspace of those $\varphi \in \mathrm{Hom}(V_n, V_n)$ such that $\mathrm{Im}(\varphi) \subseteq V_m$. Also, $V_n \cong \mathbb{F}_{q^n}$, when $\mathbb{F}_{q^n}$ is considered as an $\mathbb{F}_q$-vector space of dimension n. Let now $\mathrm{Hom}_q(\mathbb{F}_{q^n}) := \mathrm{Hom}_q(\mathbb{F}_{q^n}, \mathbb{F}_{q^n})$ be the set of all $\mathbb{F}_q$–linear maps of $\mathbb{F}_{q^n}$

in itself. It is well known that each element of $\text{Hom}_q(\mathbb{F}_{q^n})$ can be represented in a unique way as a q–polynomial over $\mathbb{F}_{q^n}$; see e.g. [13]. In other words, for any $\varphi \in \text{Hom}_q(\mathbb{F}_{q^n})$ there is an unique polynomial $f(x)$ of the form

$$f(x) := \sum_{i=0}^{n-1} a_i x^{q^i}$$

with $a_i \in \mathbb{F}_{q^n}$ such that

$$\forall x \in \mathbb{F}_{q^n} : \varphi(x) = f(x) = a_0 x + a_1 x^q + \cdots + a_{n-1} x^{q^{n-1}}.$$

The set $\tilde{\mathcal{L}}_{n,q}$ of such q-polynomials over $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_{q^n}$ of dimension n with respect to the usual sum and scalar multiplication. When it is regarded as a vector space over $\mathbb{F}_q$, its dimension is n^2 and it is isomorphic to $\mathbb{F}_q^{n \times n}$. Actually, $\tilde{\mathcal{L}}_{n,q}$ endowed with the product $\circ$ induced by the functional composition in $\text{Hom}_q(\mathbb{F}_{q^n})$ is an algebra over $\mathbb{F}_q$.

Using the above remarks, it is straightforward to see that any $\mathbb{F}_q$-linear RD-code might be regarded as a suitable $\mathbb{F}_q$-subspace of $\tilde{\mathcal{L}}_{n,q}$, when $m = n$. This approach shall be extensively used in the present work. In order to fix the notation and ease the reader, we shall reformulate some of the notions recalled before in terms of q-polynomials. Also, in the remainder of this work we shall always silently identify the elements of $\tilde{\mathcal{L}}_{n,q}$ with the morphisms of $\text{Hom}_q(\mathbb{F}_{q^n})$ they represent and speak also of *kernel* and *rank* of a linearized polynomial.

The notion of Delsarte dual code can be written in terms of q-polynomials as follows, see for example [17, Section 2]. Let $b : \tilde{\mathcal{L}}_{n,q} \times \tilde{\mathcal{L}}_{n,q} \to \mathbb{F}_q$ be the bilinear form given by

$$b(f, g) = \text{Tr}_{q^n/q} \left(\sum_{i=0}^{n-1} f_i g_i \right)$$

where $f(x) = \sum_{i=0}^{n-1} f_i x^{q^i}$ and $g(x) = \sum_{i=0}^{n-1} g_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ and denote by $\text{Tr}_{q^n/q}$ the trace function $\mathbb{F}_{q^n} \to \mathbb{F}_q$. The Delsarte dual code $\mathcal{C}^\perp$ of a set of q-polynomials $\mathcal{C}$ is

$$\mathcal{C}^\perp = \{f \in \tilde{\mathcal{L}}_{n,q} : b(f, g) = 0, \ \forall g \in \mathcal{C}\}.$$

The adjoint code $\mathcal{C}^\top$ of a set of q-polynomials $\mathcal{C}$ is

$$\mathcal{C}^\top = \{\hat{f} \in \tilde{\mathcal{L}}_{n,q} : f \in \mathcal{C}\},$$

where $\hat{f}$ is the adjoint of $f(x)$ with respect to the bilinear form b.

Also, two RD-codes $\mathcal{C}$ and $\mathcal{C}'$ are equivalent if and only if there exist two invertible q-polynomials h and g and a field automorphism σ such that $\{h \circ f^\sigma \circ g : f \in \mathcal{C}\} = \mathcal{C}'$, where if $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ then $f^\sigma(x) = \sum_{i=0}^{n-1} a_i^\sigma x^{q^i}$; furthermore, $\mathcal{C}$ and $\mathcal{C}'$ are strongly equivalent if and only if $\mathcal{C}'$ is equivalent to either $\mathcal{C}$ or to $\mathcal{C}^\top$.

The left and right idealisers of a code $\mathcal{C} \subseteq \tilde{\mathcal{L}}_{n,q}$ can be written as

$$L(\mathcal{C}) = \{\varphi(x) \in \tilde{\mathcal{L}}_{n,q} \colon \varphi \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\};$$

$$R(\mathcal{C}) = \{\varphi(x) \in \tilde{\mathcal{L}}_{n,q} \colon f \circ \varphi \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}.$$

Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MRD-code of dimension nk with parameters $(n, n, q; n-k+1)$. If $L(\mathcal{C})$ has maximum cardinality q^n, then we may always assume (up to equivalence) that

$$L(\mathcal{C}) = \mathcal{F}_n = \{\tau_\alpha = \alpha x \colon \alpha \in \mathbb{F}_{q^n}\} \simeq \mathbb{F}_{q^n};$$

the same holds for the right idealiser (see e.g. [11]).

Hence, when the left idealiser is $\mathcal{F}_n$, $\mathcal{C}$ turns out to be closed with respect to the left composition with $\mathbb{F}_{q^n}$-linear maps, while if the right idealiser is $\mathcal{F}_n$, then $\mathcal{C}$ is closed with respect to the right composition with the $\mathbb{F}_{q^n}$-linear maps. For this reason, when $L(\mathcal{C})$ (resp. $R(\mathcal{C})$) is equal to $\mathcal{F}_n$ we say that $\mathcal{C}$ is $\mathbb{F}_{q^n}$-*linear on the left* (resp. *right*) (or simply $\mathbb{F}_{q^n}$-*linear* if it is clear from the context). In the literature it is quite common to find the term $\mathbb{F}_{q^n}$-linear instead of $\mathbb{F}_{q^n}$-linear on the left. We can state the following result.

Proposition 2. *[3, Theorem 6.1][4, Theorem 2.2] Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MRD-code of dimension nk with parameters $(n, n, q; n-k+1)$. Then $L(\mathcal{C})$ (resp. $R(\mathcal{C})$) has maximum order q^n if and only if there exists an MRD-code $\mathcal{C}'$ equivalent to $\mathcal{C}$ which is $\mathbb{F}_{q^n}$-linear on the left (resp. on the right).*

For more details see also [25].

2   Known examples of $\mathbb{F}_{q^n}$-linear MRD-codes

This section is devoted to list the known examples of MRD-codes, by using their representation as sets of linearized polynomials of $\tilde{\mathcal{L}}_{n,q}$. In [6], Delsarte gives the first construction for linear MRD-codes (he calls such sets *Singleton systems*) from the perspective of bilinear forms. Few years later, Gabidulin in [7, Section 4] presents the same class of MRD-codes by using linearized polynomials. Although these codes have been originally discovered by Delsarte, they are called *Gabidulin codes* and they can be written as follows

$$\mathcal{G}_k = \langle x, x^q, \dots, x^{q^{k-1}} \rangle_{\mathbb{F}_{q^n}},$$

with $k \leq n - 1$. Kshevetskiy and Gabidulin in [12] generalize the previous construction obtaining the so-called *generalized Gabidulin codes*

$$\mathcal{G}_{k,s} = \langle x, x^{q^s}, \dots, x^{q^{s(k-1)}} \rangle_{\mathbb{F}_{q^n}},$$

with $\gcd(s, n) = 1$ and $k \leq n-1$. $\mathcal{G}_{k,s}$ is an $\mathbb{F}_q$-linear MRD-code with parameters $(n, n, q; n-k+1)$ and $L(\mathcal{G}_{k,s}) = R(\mathcal{G}_{k,s}) \simeq \mathbb{F}_{q^n}$, see [14, Lemma 4.1 & Theorem 4.5] and [18, Theorem IV.4]. Note that, as proved in [7,12], this family is closed

by the Delsarte duality and by the adjoint operation, more precisely $\mathcal{G}_{k,s}^{\perp}$ is equivalent to $\mathcal{G}_{n-k,s}$ and $\mathcal{G}_{k,s}^{\top}$ is equivalent to itself.

More recently, Sheekey in [23] proves that with $\gcd(s,n) = 1$, the set

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 x + a_1 x^{q^s} + \ldots + a_{k-1} x^{q^{s(k-1)}} + a_0^{q^h} \eta x^{q^{sk}} : a_i \in \mathbb{F}_{q^n}\},$$

with $k \leq n-1$ and $\eta \in \mathbb{F}_{q^n}$ such that $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$, is an $\mathbb{F}_q$-linear MRD-code of dimension nk with parameters $(n, n, q; n-k+1)$. This code is called *generalized twisted Gabidulin code*. Lunardon, Trombetti and Zhou in [17], generalizing the results of [23], determined the automorphism group of the generalized twisted Gabidulin codes and proved that, up to equivalence, the generalized Gabidulin codes and the twisted Gabidulin codes are both proper subsets of this class. Clearly, for $\eta = 0$ we have exactly the generalized Gabidulin code $\mathcal{G}_{k,s}$. Also, the authors in [17, Corollary 5.2] determined the left and right idealisers: if $\eta \neq 0$, then

$$L(\mathcal{H}_{k,s}(\eta, h)) \simeq \mathbb{F}_{q^{\gcd(n,h)}} \text{ and } R(\mathcal{H}_{k,s}(\eta, h)) \simeq \mathbb{F}_{q^{\gcd(n, sk-h)}}. \tag{1}$$

The class of generalized twisted Gabidulin codes is closed by Delsarte duality and by the adjoint operation, more precisely $\mathcal{H}_{k,s}(\eta, h)^{\perp}$ is equivalent to $\mathcal{H}_{n-k,s}(-\eta, n-h)$ and $\mathcal{H}_{k,s}(\eta, h)^{\top}$ is equivalent to $\mathcal{H}_{k,s}(1/\eta, sk-h)$, [23, Theorem 6] and [17, Propositions 4.2 & 4.3]. We are interested to the case in which $h = 0$, i.e.

$$\mathcal{H}_{k,s}(\eta) := \mathcal{H}_{k,s}(\eta, 0) = \langle x + \eta x^{q^{sk}}, x^{q^s}, \ldots, x^{q^{s(k-1)}} \rangle_{\mathbb{F}_{q^n}},$$

which is $\mathbb{F}_{q^n}$-linear (more precisely it is an $\mathbb{F}_q$-linear MRD-codes $\mathbb{F}_{q^n}$-linear on the left). Apart from the two infinite families of $\mathbb{F}_q$-linear MRD-codes $\mathbb{F}_{q^n}$-linear on the left ($\mathcal{G}_{k,s}$ and $\mathcal{H}_{k,s}(\eta)$), there are a few other examples known for $n \in \{6, 7, 8\}$.

- In [3], Csajbók, Marino, Polverino and Zanella prove the following results
  - for $q > 4$ it is always possible to find $\delta \in \mathbb{F}_{q^2}$ such that the set

    $$\mathcal{C}_1 = \langle x, \delta x^q + x^{q^4} \rangle_{\mathbb{F}_{q^6}}$$

    is an MRD-code with parameters $(6, 6, q; 5)$, [3, Theorem 7.1]. Its Delsarte dual code is equivalent to

    $$\mathcal{D}_1 = \langle x^q, x^{q^2}, x^{q^4}, x - \delta^q x^{q^3} \rangle_{\mathbb{F}_{q^6}},$$

    whose parameters are $(6, 6, q; 3)$;
  - for q odd and $\delta \in \mathbb{F}_{q^8}$ such that $\delta^2 = -1$ the set

    $$\mathcal{C}_2 = \langle x, \delta x^q + x^{q^5} \rangle_{\mathbb{F}_{q^8}}$$

    is an MRD-code with parameters $(8, 8, q; 7)$, [3, Theorem 7.2]. Its Delsarte dual code is is equivalent to

    $$\mathcal{D}_2 = \langle x^q, x^{q^2}, x^{q^3}, x^{q^5}, x^{q^6}, x - \delta x^{q^4} \rangle_{\mathbb{F}_{q^8}},$$

    whose parameters are $(8, 8, q; 3)$.

– In [4], Csajbók, Marino, Polverino and Zhou prove the following results
  - for q odd and $\gcd(s,7) = 1$ the set

$$\mathcal{C}_3 = \langle x, x^{q^s}, x^{q^{3s}} \rangle_{\mathbb{F}_{q^7}}$$

    is an MRD-code with parameters $(7,7,q;5)$, [4, Theorem 3.3]. Its Delsarte dual code is equivalent to

$$\mathcal{D}_3 = \langle x, x^{q^{2s}}, x^{q^{3s}}, x^{q^{4s}} \rangle_{\mathbb{F}_{q^7}},$$

    whose parameters are $(7,7,q;4)$;
  - for $q \equiv 1 \pmod 3$ and $\gcd(s,8) = 1$ the set

$$\mathcal{C}_4 = \langle x, x^{q^s}, x^{q^{3s}} \rangle_{\mathbb{F}_{q^8}}$$

    is an MRD-code with parameters $(8,8,q;6)$, [4, Theorem 3.5]. Its Delsarte dual code is is equivalent to

$$\mathcal{D}_4 = \langle x, x^{q^{2s}}, x^{q^{3s}}, x^{q^{4s}}, x^{q^{5s}} \rangle_{\mathbb{F}_{q^8}}$$

    whose parameters are $(8,8,q;4)$.
– In [5] Csajbók, Marino and Zullo prove that for q odd, $\delta^2 + \delta = 1$ and $q \equiv 0, \pm 1 \pmod 5$

$$\mathcal{C}_5 = \langle x, x^q + x^{q^3} + \delta x^{q^5} \rangle_{\mathbb{F}_{q^6}}$$

is an MRD-code with parameters $(6,6,q;5)$, [5, Theorem 6.1]. Its Delsarte dual code is is equivalent to

$$\mathcal{D}_5 = \langle x^q, x^{q^3}, x - x^{q^2}, x^{q^4} - \delta x \rangle_{\mathbb{F}_{q^6}}$$

and it has parameters $(6,6,q;3)$.

3 Characterization of generalized twisted Gabidulin codes

In this section, we shall deal with $\mathbb{F}_q$-linear MRD-codes $\mathbb{F}_{q^n}$-linear on the left; hence from now on we will refer to them just as $\mathbb{F}_{q^n}$-linear MRD-codes. Also, we may always assume that $\mathcal{C} \subseteq \tilde{\mathcal{L}}_{n,q}$ and that $L(\mathcal{C}) = \{\alpha x \colon \alpha \in \mathbb{F}_{q^n}\}$. So, if k is the dimension of $\mathcal{C}$ over $L(\mathcal{C})$, we have that

$$\mathcal{C} = \langle f_1(x), \ldots, f_k(x) \rangle_{\mathbb{F}_{q^n}},$$

for some $f_1(x), \ldots, f_k(x) \in \tilde{\mathcal{L}}_{n,q}$.

Horlemann-Trautmann and Marshall in [10] prove the following characterization of generalized Gabidulin codes. In the original version, this result was formulated regarding RD-codes as subsets of $\mathbb{F}_{q^m}^n$; here we rewrite it in the context of linearized polynomials with $\mathcal{C} \subseteq \tilde{\mathcal{L}}_{n,q}$.

Theorem 3. *[10, Theorem 4.8] An $\mathbb{F}_{q^n}$-linear MRD-code $\mathcal{C} \subseteq \tilde{\mathcal{L}}_{n,q}$ having dimension k is equivalent to a generalized Gabidulin code $\mathcal{G}_{k,s}$ if and only if there is an integer $s < n$ with $\gcd(s,n) = 1$ and $\dim_{\mathbb{F}_{q^n}}(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 1$, where $\mathcal{C}^{[s]} = \{f(x)^{[s]} \colon f(x) \in \mathcal{C}\}$, denoting by $[s]$ the power q^s.*

Consider the subfamily of $\mathbb{F}_{q^n}$-linear generalized twisted Gabidulin codes

$$\mathcal{H}_{k,s}(\eta) = \mathcal{H}_{k,s}(\eta, 0) = \langle x + \eta x^{[sk]}, x^{[s]}, \ldots, x^{[s(k-1)]} \rangle_{\mathbb{F}_{q^n}},$$

with $\eta \neq 0$. Note that if $\mathcal{C} \subseteq \tilde{\mathcal{L}}_{n,q}$ is an $\mathbb{F}_{q^n}$-linear MRD-code of dimension k equivalent to a generalized twisted Gabidulin code $\mathcal{H}_{k,s}(\eta)$ with $\eta \neq 0$, then $\dim_{\mathbb{F}_{q^n}}(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 2$. This condition, in general, is not enough to characterize MRD-codes equivalent to $\mathcal{H}_{k,s}(\eta)$. In [9], we determine what further conditions are necessary for a characterization in the spirit of Theorem 3, proving the following result.

Theorem 4. *[9, Theorem 3.9] Let $\mathcal{C}$ be a k-dimensional $\mathbb{F}_{q^n}$-linear MRD-code with $k > 2$ contained in $\tilde{\mathcal{L}}_{n,q}$. Then, the code $\mathcal{C}$ is equivalent to a generalized twisted Gabidulin code if and only if there exists an integer s such that $\gcd(s,n) = 1$ and such that the following two conditions hold*

1. *$\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 2$ and $\dim(\mathcal{C} \cap \mathcal{C}^{[s]} \cap \mathcal{C}^{[2s]}) = k - 3$, i.e. there exist $p(x), q(x) \in \tilde{\mathcal{L}}_{n,q}$ such that*

$$\mathcal{C} = \langle p(x)^{[s]}, p(x)^{[2s]}, \ldots, p(x)^{[s(k-1)]} \rangle_{\mathbb{F}_{q^n}} \oplus \langle q(x) \rangle_{\mathbb{F}_{q^n}};$$

2. *$p(x)$ is invertible and there exists $\eta \in \mathbb{F}_{q^n}^*$ such that $p(x) + \eta p(x)^{[sk]} \in \mathcal{C}$.*

4   Distinguishers for RD-codes

A *distinguisher* is an easy to compute function which allows to identify an object in a family of (apparently) similar ones. Existence of distinguishers is of particular interest for cryptographic applications, as it makes possible to identify a candidate encryption from a random text. Here, we shall present some new distinguishers for rank metric codes.

As seen in the previous section, it has been shown in [10] that an MRD-code $\mathcal{C}$ of parameters $[n, k]$, i.e a k-dimensional MRD-code of $\tilde{\mathcal{L}}_{n,q}$, is equivalent to a generalized Gabidulin code if, and only if, there exists a positive integer s such that $\gcd(s,n) = 1$ and $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 1$. Following the approach of [10], we define for any RD-code $\mathcal{C} \subseteq \tilde{\mathcal{L}}_{n,q}$ the number

$$h(\mathcal{C}) := \max\{\dim(\mathcal{C} \cap \mathcal{C}^{[j]}) \colon j = 1, \ldots, n - 1; \gcd(j, n) = 1\}. \tag{2}$$

Theorem 3 states that an MRD-code $\mathcal{C}$ is equivalent to a generalized Gabidulin code if and only if $h(\mathcal{C}) = k - 1$.

We now define also the *Gabidulin index*, $\mathrm{ind}(\mathcal{C})$ of a $[n, k]$ RD-code as the maximum dimension of a subcode $\mathcal{G} \leq \mathcal{C}$ contained in $\mathcal{C}$ with $\mathcal{G}$ equivalent to a

generalized Gabidulin code. Note that the Gabidulin index is an invariant with respect to strong equivalence since $\mathcal{G}_{k,s}^{\top} \simeq \mathcal{G}_{k,s}$.

In [9], we determine these indexes for each known $\mathbb{F}_{q^n}$-linear MRD-code. Our result is contained in Table 1 and it is of interest since it can be used for the equivalence issue. Note that in Table 1, ind, h and R denote, respectively, the Gabidulin index, the value defined in (2) and the right idealiser.

Code	ind	h	R	$[n,k]$		Code	ind	h	R	$[n,k]$
$\mathcal{G}_{k,s}$	k	$k-1$	$\mathbb{F}_{q^n}$	$[n,k]$						
$\mathcal{H}_{k,s}(\eta)$	$k-1$	$k-2$	$\mathbb{F}_q^{\gcd(n,k)}$	$[n,k]$						
$\mathcal{C}_1$	1	0	$\mathbb{F}_{q^3}$	$[6,2]$		$\mathcal{D}_1$	2	2	$\mathbb{F}_{q^3}$	$[6,4]$
$\mathcal{C}_2$	1	0	$\mathbb{F}_{q^4}$	$[8,2]$		$\mathcal{D}_2$	3	4	$\mathbb{F}_{q^4}$	$[8,6]$
$\mathcal{C}_3$	2	1	$\mathbb{F}_{q^7}$	$[7,3]$		$\mathcal{D}_3$	3	2	$\mathbb{F}_{q^7}$	$[7,4]$
$\mathcal{C}_4$	2	1	$\mathbb{F}_{q^8}$	$[8,3]$		$\mathcal{D}_4$	4	3	$\mathbb{F}_{q^8}$	$[8,5]$
$\mathcal{C}_5$	1	0	$\mathbb{F}_{q^2}$	$[6,2]$		$\mathcal{D}_5$	2	2	$\mathbb{F}_{q^2}$	$[6,4]$

Table 1. Known linear MRD-codes and their distinguishers

Clearly, the Gabidulin index may be defined also in the case in which the code considered is not $\mathbb{F}_{q^n}$-linear.

For instance, we get the following.

Theorem 5. *Let n, s be positive integers such that $\gcd(s,n) = 1$. Let $k \leq n-1$ and $\eta \in \mathbb{F}_{q^n}^*$ such that $N_{q^n/q}(\eta) \neq (-1)^{nk}$, then $\mathcal{H}_{k,s}(\eta, h)$ has Gabidulin index equals to $k-1$.*

Proof. As recalled in Section 2,

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 x + a_1 x^{q^s} + \ldots + a_{k-1}x^{q^{s(k-1)}} + a_0^{q^h}\eta x^{q^{sk}} : a_i \in \mathbb{F}_{q^n}\},$$

and since $\eta \neq 0$, it is not equivalent to any generalized Gabidulin code. Hence, $\mathrm{ind}(\mathcal{H}_{k,s}(\eta, h)) < k$. Also, it contains $\mathcal{G}'$, where

$$\mathcal{G}' = \{a_1 x^{q^s} + \ldots + a_{k-1}x^{q^{s(k-1)}} : a_i \in \mathbb{F}_{q^n}\} \simeq \mathcal{G}_{k-1,s}.$$

Hence, $\mathrm{ind}(\mathcal{H}_{k,s}(\eta, h)) = k-1$.

We aim to continue in investigating such kind of results.

References

1. Berger, T.: Isometries for rank distance and permutation group of Gabidulin codes, *IEEE Trans. Inform. Theory* **49**, 3016–3019 (2003).
2. Byrne E., Ravagnani, A.: Partition-balanced families of codes and asymptotic enumeration in coding theory, https://arxiv.org/abs/1805.02049.

3. Csajbók, B., Marino, G., Polverino, O., Zanella, C.: A new family of MRD-codes, *Linear Algebra Appl.* **548**, 203–220 (2018).
4. Csajbók, B., Marino, G., Polverino, O., Zhou, Y.: Maximum Rank-Distance codes with maximum left and right idealisers, https://arxiv.org/abs/1807.08774.
5. Csajbók, B., Marino, G., Zullo, F.: New maximum scattered linear sets of the projective line, *Finite Fields Appl.* **54**, 133–150 (2018).
6. Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25**, 226–241 (1978).
7. Gabidulin, E.: Theory of codes with maximum rank distance, *Problems of information transmission* **21(3)**, 3–16 (1985).
8. Gabidulin, E., Paramonov, A., Tretjakov, O.: Ideals over a Non-Commutative Ring and Their Application in Cryptology, in *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, 482-489 (1991).
9. Giuzzi, L., Zullo, F.: Identifiers for MRD-codes, https://arxiv.org/abs/1807.09476.
10. Horlemann-Trautmann, A., Marshall, K.: New criteria for MRD and Gabidulin codes and some rank-metric code constructions, *Adv. Math. Commun.* **11(3)**, 533–548 (2017).
11. Huppert, B.: Endliche Gruppen, volume **1**, *Springer Berlin-Heidelberg-New York*, 1967.
12. Kshevetskiy, A., Gabidulin, E.: The new construction of rank codes, *International Symposium on Information Theory*, 2005. ISIT 2005. Proceedings, 2105–2108 (2005).
13. Lidl, R., Niederreiter, H.: Finite fields, volume 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition (1997).
14. Liebhold, D., Nebe, G.: Automorphism groups of Gabidulin-like codes, *Arch. Math.* **107(4)**, 355–366 (2016).
15. Loidreau, P.: A Welch-Berlekamp like algorithm for decoding Gabidulin codes, In *Coding and cryptography*, Springer, Berlin, Heidelberg, 36–45 (2006).
16. Lunardon, G., Trombetti, R., Zhou, Y.: On kernels and nuclei of rank metric codes, *J. Algebraic Combin.* **46**, 313–340 (2017).
17. Lunardon, G., Trombetti, R., Zhou, Y.: Generalized Twisted Gabidulin Codes, *J. Combin. Theory Ser. A* **159**, 79–106 (2018).
18. Morrison, K.: Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes, *IEEE Trans. Inform. Theory* **60(11)**, 7035–7046 (2014).
19. Neri, A., Horlemann-Trautmann, A., Randrianarisoa, T., Rosenthal, J.: On the genericity of maximum rank distance and Gabidulin codes, *Des. Codes Cryptogr.* **86(2)** (2018), 1–23.
20. Puchinger, S., Wachter-Zeh, A.: Fast operations on linearized polynomials and their applications in coding theory, *J. Symbolic Comput.* **89** (2018), 194-215.
21. Ravagnani, A.: Rank-metric codes and their duality theory, *Des. Codes Cryptogr.* **80(1)**, 197–216 (2016).
22. Roth, R. M.: Maximum-Rank Array Codes and their Application to Crisscross Error Correction, *IEEE Trans. Inform. Theory* **37(2)**, 328–336 (1991).
23. Sheekey, J.: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10(3)**, 475–488 (2016).
24. Wachter-Zeh, A.: Decoding of Block and Convolutional Codes in Rank Metric, *PhD Thesis*, Ulm University and University of Rennes 1 (2013).
25. Zullo, F.: Linear codes and Galois geometries: between two worlds, *PhD thesis*, Università degli Studi della Campania "Luigi Vanvitelli".