Identifiers for MRD-codes

Luca Giuzzi and Ferdinando Zullo*

July 25, 2018

Abstract

For any admissible value of the parameters n and k there exist $[n,k]$-Maximum Rank distance $\mathbb{F}_q$-linear codes. Indeed, it can be shown that if field extensions large enough are considered, *almost all* rank distance codes are MRD. On the other hand, very few families up to equivalence of such codes are currently known. In the present paper we study some invariants of MRD codes and evaluate their value for the known families, providing a new characterization of generalized twisted Gabidulin codes.

AMS subject classification: 51E22, 05B25, 94B05

Keywords: Gabidulin codes, Rank distance, Distinguisher

1 Introduction

Delsarte [13] introduced in 1978 rank-distance (RD) codes as q-analogs of the usual linear error correcting codes endowed with Hamming distance. In the same paper, he also showed that the parameters of these codes must obey a Singleton-like bound and that for any admissible value of the length n and the dimension k this bound is sharp. A rank distance code attaining this bound is called *maximum rank distance* (MRD). In 1985 Gabidulin [15] independently rediscovered Rank-distance codes and also devised an algebraic decoding algorithm, in close analogy to what happens for Reed-Solomon Hamming codes, for the family of MRD codes described by Delsarte.

*The research was supported by Ministry for Education, University and Research of Italy MIUR (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

More recently MRD-codes have been intensively investigated both for their applications to network coding and for their links with remarkable geometric and algebraic objects such as linear sets and semifields [1, 4, 5, 7, 9, 10, 11, 12, 24, 26, 32, 34].

It has been shown in [19] (see also [2]) that a generic rank-distance code, provided that the field involved with the construction is large enough, is MRD. The authors of [19] make extensive use of algebraic geometry methods and they are also able to offer an estimate on the probability that a random rank distance code is MRD as well as to show that the probability of obtaining a Gabidulin code goes to 0.

In [2] Byrne and Ravagnani obtain an approximation of the fraction of RD-codes of given length and dimension which are MRD using a mostly combinatorial approach. Their paper show also that some care has to be taken when considering these density results; indeed, the $\mathbb{F}_{q^m}$–linear MRD codes are dense in the family of all $\mathbb{F}_{q^m}$ rank distance codes $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ of dimension k and length n. However, this is not the case for $\mathbb{F}_q$–linear MRD-codes in the family of $\mathbb{F}_q$–linear rank distance codes $\mathcal{C} \leq \mathbb{F}_q^{m\times n}$ with $\dim \mathcal{C} = k$; see [2].

In spite of the aforementioned density results, very few families of MRD codes are currently known up to equivalence; basically, apart from Gabidulin [15] and twisted Gabidulin [32] codes, the state of the art is given by the codes presented in Table 1 and their Delsarte duals.

It is interesting and of much importance for applications to determine some algebraic *distinguishers* in order to describe and or characterize these codes. The case of (generalized) Gabidulin codes is investigated in [19], whose result we recall in Theorem 3.1; see also [27], where such codes are characterized in terms of their generator matrices.

Indeed, a well known public key cryptosystem based on error correcting codes is due to McEliece. The basic idea of this encryption scheme is to hide the generating matrix G of a t-error correcting code by means of an invertible matrix S and a permutation matrix P, so that $\hat{G} = SGP$ and to define the encryption of a message m as the codeword $c = \hat{G}m + e$ where e is a noise vector of weight at most t. In order to discuss the security of this cryptosystem we recall the model of *indistinguishability under chosen plaintext attack* (IND-CPA), that is to say we shall require that an adversary which does not know the key is unable to distinguish between the encodings c_1 and c_2 of any two different messages m_1 and m_2 she has suitably chosen.

In the case of McEliece cryptosystem, given two distinct messages m_1, m_2 with encodings respectively c_1 and c_2, the word $c_1 - c_2$ has distance at most $2t$ from $\hat{G}(m_1 - m_2)$. So, if we consider codes under Hamming distance and t is "small" we see that $\hat{G}(m_1 - m_2)$ has almost everywhere the same components as $c_1 - c_2$.

This makes IND-CPA easier to thwart. Using rank distance instead of Hamming distance codes solves this inconvenience. So a primary application of MRD codes is for McEliece–like cryptosystems.

Unfortunately, even if "almost all $\mathbb{F}_{q^m}$–linear codes are MRD", very few of them are known and even less are amenable to efficient decoding. The possibility of using Gabidulin codes has been considered in [18, 19]. The authors in [18] however proved that there is a very efficient distinguisher for them, i.e. it is possible to easily recognize a Gabidulin code from a generic MRD code of the same parameters chosen uniformly at random. As a consequence, the cryptosystems based on them turn out not to be semantically secure, as it is possible to distinguish a ciphertext from a random vector; see also [30, 31].

In the present paper we investigate the existence of algebraic distinguishers (akin to those of [18]) for the currently known families of $\mathbb{F}_{q^n}$-linear MRD codes and provide some invariants up to equivalence.

Our main results concern the list of dimensions of the intersections of an $\mathbb{F}_{q^n}$-linear MRD-code with its conjugates and a description of a maximum dimension Gabidulin codes contained in a fixed MRD-code. We shall see, in particular, that this can be used as to provide distinguishers for the generalized twisted Gabidulin codes and how it can also be applied to the other 5 known families (and their duals), see Tables 1 and 2.

1.1 Structure of the paper

In Section 2 we recall the definitions of rank distance (RD) codes and their basic properties. We also fix our notation and discuss in Section 2.1 the representation of RD-codes by means of subspaces of q-polynomials; a representation which shall be used in the rest of the paper. Section 2.2 deals with an alternative convenient representation of RD-codes. In Section 3 we prove one of our main results, namely the characterization of generalized twisted Gabidulin codes in terms of the intersection with their conjugates and the Gabidulin subcode they contain; see Theorem 3.5. This leads to the introduction in Section 4 of two indexes

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

and

$$\operatorname{ind}(\mathcal{C}) := \max\{\dim \mathcal{G} \leq \mathcal{C} : \mathcal{G} \text{ is equivalent to a generalized Gabidulin code}\}$$

for MRD-codes. These indexes are then evaluated for the known families of codes. We conclude the paper with some open problems.

2 Preliminaries

Denote by $\mathbb{F}_q$ a finite field and let V_m and V_n be two vector spaces over $\mathbb{F}_q$ of dimension respectively m and n. The vector space $\mathfrak{H} := \mathrm{Hom}_q(V_n, V_m)$ of all $\mathbb{F}_q$–linear transformations $V_n \to V_m$ is naturally endowed with a *rank distance* $d_R : \mathfrak{H} \times \mathfrak{H} \to \mathbb{N}$ where $d_R(\varphi, \psi) := \dim \mathrm{Im}(\varphi - \psi)$. If we fix bases in V_m and V_n we have that $\mathfrak{H}$ is isometric to the vector space $\mathbb{F}_q^{m\times n}$ of all $m \times n$ matrices over $\mathbb{F}_q$ endowed with the distance $d(A, B) := rk\,(A - B)$ for all $A, B \in \mathbb{F}_q^{m\times n}$.

A *rank distance code* (in brief RD-code) $\mathcal{C}$ of parameters $(m, n, q; d)$ is a subset $\mathcal{C}$ of $\mathbb{F}_q^{m\times n}$ with minimum rank distance $d := \min_{A,B\in\mathcal{C},\ A\neq B}\{d(A, B)\}$. An RD-code $\mathcal{C}$ is $\mathbb{F}_q$-linear if it is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^{m\times n}$ (or, equivalently, of $\mathfrak{H}$). When $\mathcal{C}$ is an $\mathbb{F}_q$-linear RD-code of dimension k contained in $\mathbb{F}_q^{n\times n}$, we shall also write, in brief, that $\mathcal{C}$ has parameters $[n, k]$.

As mentioned in Section 1, it has been shown in [13] that an analogue of the Singleton bound holds for RD-codes; namely, if $\mathcal{C}$ is an $(m, n, q; d)$ RD-code, then

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

When this bound is achieved, then $\mathcal{C}$ is an *MRD-code*.

The *Delsarte dual* code of a linear RD-code $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is defined as

$$\mathcal{C}^\perp = \{M \in \mathbb{F}_q^{m\times n} \colon \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}.$$

Lemma 2.1. *[13, 15] 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 $mn - k$.*

The weight of a codeword $c \in \mathcal{C}$ is just the rank of the matrix corresponding to c. The spectrum of weights of a MRD-code is "complete" in the following sense. Denote by A_i the number of codewords of weight i of an RD-code $\mathcal{C}$, then, the following (which is a weaker form of [15, Theorem 5]) holds.

Corollary 2.2. *[26, Lemma 2.1] Let $\mathcal{C}$ be an MRD-code in $\mathbb{F}_q^{m\times n}$ with minimum distance d and suppose $m \leq n$. Assume that the null matrix O is in $\mathcal{C}$. Then, for any $0 \leq l \leq m - d$, we have $A_{d+l} > 0$, i.e. there exists at least one matrix $C \in \mathcal{C}$ such that $\mathrm{rk}(C) = d + l$.*

Existence of MRD-codes for all possible values $(m, n, q; d)$ of the parameters has been originally settled in [13] where *Singleton systems* are constructed and, independently by Gabidulin in [15]; this has also been generalized in [20].

More recently Sheekey [32] discovered a new family of linear maximum rank distance codes for all possible parameters which are inequivalent to those above; see also [25]. Other examples of MRD-codes can be found in [3, 14, 28, 29, 33, 35].

For some chosen values of parameters there are a few other families of $\mathbb{F}_{q^n}$-linear MRD-codes of $\mathbb{F}_q^{n\times n}$ which are currently known; see [5, 6, 9].

The interpretation of linear RD-codes as homomorphisms of vector spaces prompts the following definition of *equivalence*. Two RD-codes $\mathcal{C}$ and $\mathcal{C}'$ of $\mathbb{F}_q^{m\times n}$ are *equivalent* if and only if there exist two invertible matrices $A \in \mathbb{F}_q^{m\times m}$, $B \in \mathbb{F}_q^{n\times n}$ and a field automorphism σ such that $\{AC^\sigma B \colon C \in \mathcal{C}\} = \mathcal{C}'$.

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

$$L(\mathcal{C}) = \{Y \in \mathbb{F}_q^{m\times m} \colon YC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$
$$R(\mathcal{C}) = \{Z \in \mathbb{F}_q^{n\times n} \colon CZ \in \mathcal{C} \text{ for all } C \in \mathcal{C}\},$$

see [22, Definition 3.1]. These sets appear also in [26], where they are respectively called middle nucleus and right nucleus; therein the authors prove the following result.

Proposition 2.3. *[26, Proposition 4.1] If $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent linear RD-codes, then their left (resp. right) idealisers are also equivalent.*

Right idealisers are usually effective as distinguishers for RD-codes, i.e. non-equivalent RD-codes often have non-isomorphic idealisers. This is in sharp contrast with the role played by left idealisers which, for the codes we consider in the present paper, are always isomorphic to $\mathbb{F}_{q^n}$.

2.1 Representation of RD-codes as q-polynomials

Any RD-code over $\mathbb{F}_q$ can be equivalently defined 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 in terms of linearized polynomials which we shall use in the rest of the paper.

Consider two vector spaces V_n and V_m over $\mathbb{F}_q$. 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 a $\mathbb{F}_q$-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 $\mathrm{Hom}_q(\mathbb{F}_{q^n})$ can be represented in a unique way as a q–polynomial over $\mathbb{F}_{q^n}$; see [21]. In other words, for any $\varphi \in \mathrm{Hom}_q(\mathbb{F}_{q^n})$ there is an unique polynomial $f(x)$ of the form

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

with $a_i \in \mathbb{F}_{q^n}$ and $[i] := q^i$ 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 $\mathcal{L}_{n,q}$ of the q-polynomials over $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_{q^n}$ with respect to the usual sum and scalar multiplication of dimension n. When it is regarded as a vector space over $\mathbb{F}_q$, its dimension is n^2 and it is isomorphic to $\mathbb{F}_q^{n\times n}$. We shall use this point of view in the present paper. Actually, $\mathcal{L}_{n,q}$ endowed with the product $\circ$ induced by the functional composition in $\mathrm{Hom}_q(\mathbb{F}_{q^n})$ is an algebra over $\mathbb{F}_q$. In particular, given any two q-polynomials $f(x) = \sum_{i=0}^{n-1} f_i x^{[i]}$ and $g(x) = \sum_{j=0}^{n-1} g_j x^{[j]}$, we can write

$$(f \circ g)(x) := \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f_i g_j^{[i]} x^{[(i+j) \bmod n]}.$$

Take now $\varphi \in \mathrm{Hom}_q(\mathbb{F}_{q^n})$ and let $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathcal{L}_{n,q}$ be the associated q-polynomial. The *Dickson (circulant) matrix* associated to f is

$$D_f := \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & a_0^q & \dots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_0^{q^{n-1}} \end{pmatrix}.$$

It can be seen that the rank of the matrix D_f equals the rank of the $\mathbb{F}_q$-linear map φ, see for example [36].

By 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 $\mathcal{L}_{n,q}$. This approach shall be extensively used in the present paper. In order to fix the notation and ease the reader, we shall reformulate some of the notions recalled before in terms of q-polynomials.

A q-polynomial is called *invertible* if it admits inverse with respect to $\circ$ or, in other words, if its Dickson matrix has non-zero determinant. In the remainder of this paper we shall always silently identify the elements of $\mathcal{L}_{n,q}$ with the morphisms of $\mathrm{Hom}_q(\mathbb{F}_{q^n})$ they represent and, as such, speak also of *kernel* and *rank* of a polynomial.

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 $\{h \circ f^\sigma \circ g \colon f \in \mathcal{C}\} = \mathcal{C}'$.

The notion of Delsarte dual code can be written in terms of q-polynomials as follows, see for example [25, Section 2]. Let $b : \mathcal{L}_{n,q} \times \mathcal{L}_{n,q} \to \mathbb{F}_q$ be the bilinear form given by

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

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

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

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

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

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

Definition 1. Suppose $\gcd(n,s) = 1$ and let $\mathcal{G}_{k,s} := \langle x^{[0]}, x^{[s]}, \ldots, x^{[s(k-1)]} \rangle \leq \mathcal{L}_{n,k}$. Any code equivalent to $\mathcal{G}_{k,s}$ is called a *generalized Gabidulin code*. Any code equivalent to $\mathcal{G}_k := \mathcal{G}_{k,1}$ is called a *Gabidulin code*.

Proposition 2.4 (Theorem 5,[32])**.** *Suppose* $\gcd(s,n) = 1$ *and let* $\mathcal{H}_{k,s}(\eta) := \langle x + \eta x^{[sk]}, x^{[s]}, \ldots, x^{[s(k-1)]} \rangle$. *If* $\mathrm{N}(\eta) := \prod_{i=0}^{n} \eta^{[i]} \neq (-1)^{nk}$, *then* $\mathcal{H}_{k,s}(\eta)$ *is a MRD-code with the same parameters as* $\mathcal{G}_{k,s}$.

Definition 2. Any code equivalent to $\mathcal{H}_{k,s}(\eta)$ with $\mathrm{N}(\eta) \neq (-1)^{nk}$ and $\eta \neq 0$ is called a *(generalized) twisted Gabidulin code*.

Remark 2.5. In [32, Remark 8], it is shown that an RD-code of the form

$$\mathcal{C} = \{\alpha x + a_1 x^{[1]} + \cdots + a_{k-1} x^{[k-1]} + \eta \alpha x^{[k]} \colon \alpha, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

with some $\eta \in \mathbb{F}_{q^n}$, is an $\mathbb{F}_{q^n}$-linear MRD-code of dimension k if and only if it is $\mathcal{H}_{k,1}(\eta)$ and $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$. The same holds for generalized twisted Gabidulin codes, i.e.

$$\mathcal{C} = \{\alpha x + a_1 x^{[s]} + \cdots + a_{k-1} x^{[s(k-1)]} + \eta \alpha x^{[sk]} \colon \alpha, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

is an $\mathbb{F}_{q^n}$-linear MRD-code of dimension k if and only if it is $\mathcal{H}_{k,s}(\eta)$ with $\mathrm{N}_{q^{sn}/q^s}(\eta) = \mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$. This is a consequence of [16, Theorem 10], see also [32, Lemma 3], [8] and [17]; indeed if $\mathcal{C}$ is an MRD-code then $\mathrm{N}_{q^n/q}(\alpha\eta) \neq (-1)^{kn} \mathrm{N}_{q^n/q}(\alpha)$ for each $\alpha \in \mathbb{F}_{q^n}^*$, i.e. $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{kn}$.

Remark 2.6. Clearly, if $1 < k < n-1$

$$\mathcal{H}_{k,s}(\eta) \cap \mathcal{H}_{k,s}(\eta)^{[s]} = \langle x^{[2s]}, \ldots, x^{[s(k-1)]} \rangle$$

and so $\dim(\mathcal{H}_{k,s}(\eta) \cap \mathcal{H}_{k,s}(\eta)^{[s]}) = k-2$ if $\eta \neq 0$. Indeed, $a_0(x + \eta x^{[sk]}) + a_1 x^{[s]} + \ldots + a_{k-1} x^{[s(k-1)]} \in \langle x^{[s]} + \eta^{[s]} x^{[s(k+1)]}, x^{[2s]}, \ldots, x^{[sk]} \rangle$ if and only if $a_0 = a_1 = 0$.

The two families of codes seen above are closed by the Delsarte duality.

Lemma 2.7. *[15, 20, 25, 32] The Delsarte dual $\mathcal{C}^\perp$ of an $\mathbb{F}_{q^n}$-linear MRD-code $\mathcal{C}$ of dimension k is an $\mathbb{F}_{q^n}$-linear MRD-code of dimension $n-k$. Also, $\mathcal{G}_{k,s}^\perp$ is equivalent to $\mathcal{G}_{n-k,s}$ and $\mathcal{H}_{k,s}(\eta)^\perp$ is equivalent to $\mathcal{H}_{n-k,s}(-\eta^{[n-ks]})$.*

Apart from the two infinite families of $\mathbb{F}_{q^n}$-linear MRD-codes $\mathcal{G}_{k,s}$ and $\mathcal{H}_{k,s}(\eta)$, there are a few other examples known for $n \in \{6,7,8\}$. Such examples are listed in Table 1 and their Delsarte duals in Table 2.

$\mathcal{C}$	parameters	conditions	reference
$\mathcal{C}_1 = \langle x, \delta x^{[1]} + x^{[4]} \rangle_{\mathbb{F}_{q^6}}$	$(6,6,q;5)$	$q > 4$ certain choices of δ	[5, Theorem 7.1]
$\mathcal{C}_2 = \langle x, x^{[1]} + x^{[3]} + \delta x^{[5]} \rangle_{\mathbb{F}_{q^6}}$	$(6,6,q;5)$	q odd $q \equiv 0, \pm 1 \pmod 5$ $\delta^2 + \delta = 1$ $(\delta \in \mathbb{F}_q)$	[7, Theorem 5.1]
$\mathcal{C}_3 = \langle x, x^{[s]}, x^{[3s]} \rangle_{\mathbb{F}_{q^7}}$	$(7,7,q;5)$	q odd $\gcd(s,7) = 1$	[6]
$\mathcal{C}_4 = \langle x, \delta x^{[1]} + x^{[5]} \rangle_{\mathbb{F}_{q^8}}$	$(8,8,q;7)$	q odd $\delta^2 = -1$	[5, Theorem 7.2]
$\mathcal{C}_5 = \langle x, x^{[s]}, x^{[3s]} \rangle_{\mathbb{F}_{q^8}}$	$(8,8,q;6)$	$q \equiv 1 \pmod 3$ $\gcd(s,8) = 1$	[6]

Table 1: Linear MRD-codes in low dimension

2.2 Linear RD-codes as subspaces of $\mathbb{F}_{q^n}^n$

In [15], Gabidulin studied RD-codes as subsets of $\mathbb{F}_{q^n}^n$. This view is still used in [2, 18, 19, 27]. As noted before, $\mathcal{L}_{n,q}$ equipped with the classical sum and the scalar multiplication by elements in $\mathbb{F}_{q^n}$ is an $\mathbb{F}_{q^n}$-vector space. Let $\mathcal{B} = (g_1, \ldots, g_n)$ an ordered $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$. The evaluation mapping

$$\Phi_{\mathcal{B}} : f(x) \in \mathcal{L}_{n,q} \mapsto (f(g_1), \ldots, f(g_n)) \in \mathbb{F}_{q^n}^n$$

is an isomorphism between the $\mathbb{F}_{q^n}$-vector spaces $\mathcal{L}_{n,q}$ and $\mathbb{F}_{q^n}^n$. Therefore, if W is an $\mathbb{F}_{q^n}$-subspace of $\mathcal{L}_{n,q}$, a generator matrix G of $\Phi_{\mathcal{B}}(W)$ can be constructed using the images of a basis of W under the action of $\Phi_{\mathcal{B}}$. Also, if G is a generator matrix of $\Phi_{\mathcal{B}}(W)$ of maximum rank, then an $\mathbb{F}_{q^n}$-basis for W can be defined by using the application $\Phi_{\mathcal{B}}^{-1}$ on the rows of G.

$\mathcal{D}_i = \mathcal{C}_i^{\perp}$	parameters	conditions
$\mathcal{D}_1 = \langle x^{[1]}, x^{[2]}, x^{[4]}, x - \delta^{[5]}x^{[3]} \rangle_{\mathbb{F}_{q^6}}$	$(6, 6, q; 3)$	$q > 4$ certain choices of δ
$\mathcal{D}_2 = \langle x^{[1]}, x^{[3]}, x - x^{[2]}, x^{[4]} - \delta x \rangle_{\mathbb{F}_{q^6}}$	$(6, 6, q; 3)$	q odd $q \equiv 0, \pm 1 \pmod 5$ $\delta^2 + \delta = 1$ $(\delta \in \mathbb{F}_q)$
$\mathcal{D}_3 = \langle x, x^{[2s]}, x^{[3s]}, x^{[4s]} \rangle_{\mathbb{F}_{q^7}}$	$(7, 7, q; 4)$	q odd $\gcd(s, 7) = 1$
$\mathcal{D}_4 = \langle x^{[1]}, x^{[2]}, x^{[3]}, x^{[5]}, x^{[6]}, x - \delta x^{[4]} \rangle_{\mathbb{F}_{q^8}}$	$(8, 8, q; 3)$	q odd $\delta^2 = -1$
$\mathcal{D}_5 = \langle x, x^{[2s]}, x^{[3s]}, x^{[4s]}, x^{[5s]} \rangle_{\mathbb{F}_{q^8}}$	$(8, 8, q; 4)$	$q \equiv 1 \pmod 3$ $\gcd(s, 8) = 1$

Table 2: Delsarte duals of the codes $\mathcal{C}_i$ for $i = 1, \ldots, 5$

3 Characterization of generalized twisted Gabidulin codes

A. Horlemann-Trautmann et al. in [18] proved the following characterization of generalized Gabidulin codes.

Theorem 3.1 ([18]). *A MRD-code $\mathcal{C}$ over $\mathbb{F}_q$ of length n and 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 $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k-1$, where $\mathcal{C}^{[s]} = \{f(x)^{[s]} \colon f(x) \in \mathcal{C}\}$.*

If $\mathcal{C}$ is equivalent to a generalized twisted Gabidulin code $\mathcal{H}_{k,s}(\eta)$, then $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 2$. This condition, in general, is not enough to characterize MRD-codes equivalent to $\mathcal{H}_{k,s}(\eta)$. The present section is devoted to determine what further conditions are necessary for a characterization.

Denote by τ_α the linear application defined by $\tau_\alpha(x) = \alpha x$ and denote by $U_1 = \{\mathrm{Tr} \circ \tau_\alpha \colon \alpha \in \mathbb{F}_{q^n}\} = \{\alpha x + \alpha^{[1]}x^{[1]} + \cdots + \alpha^{[n-1]}x^{[n-1]} \colon \alpha \in \mathbb{F}_{q^n}\}$. The set U_1 is an $\mathbb{F}_q$-subspace of $\mathcal{L}_{n,q}$ whose elements have rank at most one. It can be proven that the set $\mathcal{U}_1$ of all linearized polynomials with rank at most one is

$$\mathcal{U}_1 = \bigcup_{\beta \in \mathbb{F}_{q^n}^*} \tau_\beta \circ U_1 = \{\tau_\beta \circ \mathrm{Tr} \circ \tau_\alpha \colon \alpha, \beta \in \mathbb{F}_{q^n}\}.$$

Lemma 3.2. *Let n and s be two integers such that $\gcd(s, n) = 1$, if $p(x) \in \mathcal{L}_{n,q}$ and $p(x) = \lambda p(x)^{[s]}$ for some $\lambda \in \mathbb{F}_{q^n}^*$, then $p(x)$ is in $\mathcal{U}_1$.*

Proof. Under the assumptions, the map $x \to x^{[s]}$ is a generator of the Galois group of $\mathbb{F}_{q^n} : \mathbb{F}_q$. In particular, for all $0 \leq i \leq n-1$ there are λ_i such that $p(x) = \lambda_i p(x)^{[i]}$. It follows that the Dickson matrix of $p(x)$ has rank at most 1 and this proves the thesis. □

For the sake of completeness we prove the following lemma.

Lemma 3.3. *[23, Lemma 3] Let n and s be two integers such that $\gcd(s,n) = 1$, if $W \neq \{0\}$ is an $\mathbb{F}_{q^n}$-subspace of $\mathcal{L}_{n,q}$ such that $W = W^{[s]}$, then $W \cap \mathcal{U}_1 \neq \{0\}$.*

Proof. Note that U_1 is the set of the fixed elements of the semilinear transformation $\vartheta : p(x) \in \mathcal{L}_{n,q} \to p(x)^q \in \mathcal{L}_{n,q}$; see [23]. Since $\gcd(s,n) = 1$, if $W = W^{[s]}$, then also $W = W^{[1]}$, i.e. ϑ fixes W. Take $p(x) = \sum_{i=0}^{n-1} p_i x^{[i]} \in W$ with $p(x) \not\equiv 0$. Then the polynomial

$$p^{\psi}(x) := \sum_{i=0}^{n-1} p(x)^{[i]} = \sum_{i=0}^{n-1} c_p^{[i]} x^{[i]}$$

where

$$c_p := p_1^{[n-1]} + p_2^{[n-2]} + \ldots + p_{n-1}^{[1]} + p_0$$

is in $W \cap U_1$. If $c_p \neq 0$ for at least one polynomial $p(x) \in W$, then we are done. Otherwise, suppose $c_p = 0$ for all $p(x) \in W$. Let $p(x) \in W$ and let $\{\lambda_1, \ldots, \lambda_n\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Clearly, $\lambda_i p(x) \in W$ and $(\lambda_i p)^{\psi}(x) \in W \cap U_1$ for all i. Suppose $c_{\lambda_i p} = \lambda_i^{[n-1]} p_1^{[n-1]} + \lambda_i^{[n-2]} p_2^{[n-2]} + \ldots + \lambda_i^{[1]} p_{n-1}^{[1]} + \lambda_i p_0 = 0$ for all $i = 1, \ldots, n$. Then, the coefficients $p_1^{[n-1]}, \ldots, p_{n-1}^{[1]}, p_0$ must satisfy a homogeneous linear system of n equations with matrix

$$A := \begin{pmatrix} \lambda_1^{[n-1]} & \lambda_1^{[n-2]} & \cdots & \lambda_1 \\ \lambda_2^{[n-1]} & \lambda_2^{[n-2]} & \cdots & \lambda_2 \\ \vdots & & & \vdots \\ \lambda_n^{[n-1]} & \lambda_n^{[n-2]} & \cdots & \lambda_n \end{pmatrix}.$$

The matrix A is non-singular, see e.g. [21, Lemma 3.51]; so $p_0 = p_1 = \cdots = p_{n-1} = 0$, a contradiction. It follows that there is at least one non-zero polynomial in $U_1 \cap W$. □

The following Lemma rephrases the requirements of Theorem 3.1 in a more suitable way for the arguments to follow.

Lemma 3.4. *Let n and s be two integers such that $\gcd(s,n) = 1$ and let $\mathcal{C}$ be an $\mathbb{F}_{q^n}$-subspace of dimension $k > 1$ of $\mathcal{L}_{n,q}$. If $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k-1$ and $\mathcal{C} \cap U_1 = \{0\}$, then there exists $p(x)$ such that*

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

If $\mathcal{C}$ contains at least one invertible linearized polynomial, then $p(x)$ is invertible and $\mathcal{C} \cong \mathcal{G}_{k,s}$.

Proof. Note that, since $\mathcal{C}$ is an $\mathbb{F}_{q^n}$-subspace and $\mathcal{C} \cap U_1 = \{0\}$, then $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$. We argue by induction. We first prove the case $k = 2$. By hypothesis, $\mathcal{C} \cap \mathcal{C}^{[s]} = \langle h(x) \rangle$ and so $h(x)^{[s]} \in \mathcal{C}^{[s]}$. Since $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$, by Lemma 3.2 the polynomials $h(x)$ and $h(x)^{[s]}$ are linearly independent over $\mathbb{F}_{q^n}$ and $\mathcal{C} = \langle h(x)^{[s(n-1)]}, h(x) \rangle_{\mathbb{F}_{q^n}} = \langle p(x), p(x)^{[s]} \rangle_{\mathbb{F}_{q^n}}$, with $p(x) = h(x)^{[s(n-1)]}$.

Suppose now that the assert holds true for $k-1$ and take $k > 2$. Let $V := \mathcal{C} \cap \mathcal{C}^{[s]}$, V is an $\mathbb{F}_{q^n}$-subspace of $\mathcal{C}$ of dimension $k-1$ such that $V \cap \mathcal{U}_1 = \{0\}$, hence by Lemma 3.3 $V \neq V^{[s]}$. Then, since V and $V^{[s]}$ are both contained in $\mathcal{C}^{[s]}$, by Grassmann's formula

$$\dim(V \cap V^{[s]}) = k - 2.$$

So, $\dim V = k-1$, $V \cap \mathcal{U}_1 = \{0\}$ and $\dim(V \cap V^{[s]}) = k-2$. By induction, there is $h(x) \in V$ such that

$$V = \langle h(x), h(x)^{[s]}, \ldots, h(x)^{[s(k-2)]} \rangle_{\mathbb{F}_{q^n}}.$$

Also,

$$h(x)^{[s(n-1)]} \in V^{[s(n-1)]} = \mathcal{C}^{[s(n-1)]} \cap \mathcal{C} \subset \mathcal{C}.$$

If it were $h(x)^{[s(n-1)]} \in V$, then $V = V^{[s]}$, which has already been excluded. So,

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

where $p(x) = h(x)^{[s(n-1)]}$.

Suppose now there is $x_0 \in \mathbb{F}_{q^n}^*$ such that $p(x_0) = 0$. Then, $\alpha_1 p(x_0) + \cdots + \alpha_k p(x_0)^{[s(k-1)]} = 0$ for any choice of $\alpha_i \in \mathbb{F}_{q^n}$, $i = 1, \ldots, k$. In particular, if $\mathcal{C}$ contains at least one invertible linearized polynomial, then $p(x)$ must also be invertible. In such a case

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

so $\mathcal{C}$ is equivalent to $\mathcal{G}_{k,s}$. □

We now focus on the case $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k-2$.

- If $\dim \mathcal{C} = 2$ we just have $\mathcal{C} = \langle p(x), q(x) \rangle_{\mathbb{F}_{q^n}}$ with $q(x) \notin \langle p(x)^{[s]} \rangle_{\mathbb{F}_{q^n}}$ and $p(x) \notin \langle q(x)^{[s]} \rangle_{\mathbb{F}_{q^n}}$.
- Suppose $\dim \mathcal{C} = 3$, $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = 1$ and $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$. As before, write $V := \mathcal{C} \cap \mathcal{C}^{[s]}$. Since V and $V^{[s]}$ are contained in $\mathcal{C}^{[s]}$, by Grassmann's formula,

$$0 \leq \dim(V \cap V^{[s]}) \leq 1.$$

So, either $V = V^{[s]}$ or $\dim(V \cap V^{[s]}) = 0$. The former case is ruled out by Lemma 3.3. So $\dim(V \cap V^{[s]}) = 0$ and $V = \langle h(x) \rangle_{\mathbb{F}_{q^n}}$. It follows that

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

with $p(x) = h(x)^{[s(n-1)]}$.

- Suppose that $\dim \mathcal{C} = 4$, $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = 2$ and $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$. Write $V := \mathcal{C} \cap \mathcal{C}^{[s]}$. Clearly, since $V \neq V^{[s]}$,

$$0 \leq \dim(V \cap V^{[s]}) \leq 1.$$

Suppose $\dim(V \cap V^{[s]}) = 1$. Then, the subspace V fulfills all of the assumptions of Lemma 3.4, so there is $h(x) \in V$ such that

$$V = \langle h(x), h(x)^{[s]} \rangle_{\mathbb{F}_{q^n}}$$

and $h(x)^{[s(n-1)]} \in \mathcal{C} \setminus V$, since, otherwise, $V = V^{[s]}$. So,

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

with $p(x) = h(x)^{[s(n-1)]}$.

Suppose now that $\dim(V \cap V^{[s]}) = 0$; then $\mathcal{C} = V \oplus V^{[s(n-1)]}$. If $V = \langle h(x), g(x) \rangle_{\mathbb{F}_{q^n}}$ then $V^{[s(n-1)]} = \langle h(x)^{[s(n-1)]}, g(x)^{[s(n-1)]} \rangle_{\mathbb{F}_{q^n}}$, and so

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

with $p(x) = h(x)^{[s(n-1)]}$ and $q(x) = g(x)^{[s(n-1)]}$.

More general, we can prove the following result.

Theorem 3.5. *Let n and s be two integers such that $\gcd(s, n) = 1$ and let $\mathcal{C}$ be an $\mathbb{F}_{q^n}$-subspace of dimension $k > 2$ of $\mathcal{L}_{n,q}$. Let $V := \mathcal{C} \cap \mathcal{C}^{[s]}$. Suppose $\dim V = k - 2$ and $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$, then $\mathcal{C}$ has one of the following forms*

1. *if $\dim(V \cap V^{[s]}) = k - 3$, then there exist $p(x)$ and $q(x)$ in $\mathcal{C}$ such that*

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

2. *if $\dim(V \cap V^{[s]}) = k - 4$, then there exist $p(x)$ and $q(x)$ in $\mathcal{C}$ such that*

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

where

$$(i, j) = \begin{cases} (\frac{k}{2}, \frac{k}{2}) & \text{if } k \text{ is even} \\ (\frac{k-1}{2}, \frac{k+1}{2}) & \text{if } k \text{ is odd.} \end{cases}$$

Proof. We have already proved the assert for $k \leq 4$. Assume by induction that the assert holds for each $t < k$ with $k \geq 4$. Since V and $V^{[s]}$ are contained in $\mathcal{C}^{[s]}$, it follows that

$$\dim(V \cap V^{[s]}) \geq k - 4,$$

that is $\dim(V \cap V^{[s]}) \in \{k-4, k-3\}$, since $V \neq V^{[s]}$. If $\dim(V \cap V^{[s]}) = k-3$, then, by Lemma 3.4, there exists $h(x) \in V$ such that

$$V = \langle h(x), h(x)^{[s]}, \ldots, h(x)^{[s(k-3)]} \rangle_{\mathbb{F}_{q^n}}.$$

Since $h(x)^{[s(n-1)]} \in \mathcal{C} \setminus V$ (otherwise $V = V^{[s]}$), we get

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

where $p(x) = h(x)^{[s(n-1)]}$. If $\dim(V \cap V^{[s]}) = k-4$, since V has dimension $k-2$ and $V \cap \mathcal{U}_1 = \{0\}$, by induction there exist $h(x)$ and $g(x)$ such that

$$V = \langle h(x), \ldots, h(x)^{[s(l-1)]} \rangle_{\mathbb{F}_{q^n}} \oplus \langle g(x), \ldots, g(x)^{[s(m-1)]} \rangle_{\mathbb{F}_{q^n}},$$

with

$$(l, m) = \begin{cases} (\frac{k-2}{2}, \frac{k-2}{2}) & \text{if } k \text{ is even} \\ (\frac{k-3}{2}, \frac{k-1}{2}) & \text{if } k \text{ is odd.} \end{cases}$$

Since $V, V^{[s(n-1)]} \subset \mathcal{C}$ and $\dim V \cap V^{[s]} = k-4$ we get $\mathcal{C} = V + V^{[s(n-1)]}$. So,

$$\mathcal{C} = \langle h(x)^{[s(n-1)]}, h(x), \ldots, h(x)^{[s(l-1)]} \rangle_{\mathbb{F}_{q^n}} \oplus \langle g(x)^{[s(n-1)]}, g(x), \ldots, g(x)^{[s(m-1)]} \rangle_{\mathbb{F}_{q^n}}.$$

If we now put $p(x) = h(x)^{[s(n-1)]}$ and $q(x) = g(x)^{[s(n-1)]}$, then we get the assert. □

Examples of k-dimensional MRD-codes $\mathcal{C}$ with $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k-2$ and $\dim(V \cap V^{[s]}) = k-3$, where $V = \mathcal{C} \cap \mathcal{C}^{[s]}$, are the generalized twisted Gabidulin codes; see Remark 2.6. An example where $\dim V \cap V^{[s]} = k-4$ is given by the code $\mathcal{D}_2$ (see Table 2), which can be written as

$$\mathcal{D}_2 = \langle -x + x^{[2]}, -x^{[1]} + x^{[3]} \rangle_{\mathbb{F}_{q^6}} \oplus \langle -\delta x^{[1]} + x^{[3]}, -\delta x^{[2]} + x^{[4]} \rangle_{\mathbb{F}_{q^6}}.$$

Lemma 3.6. *Let $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ be an $\mathbb{F}_{q^n}$-linear RD-code with dimension k containing a MRD-code $\mathcal{G}$ equivalent to a generalized Gabidulin code $\mathcal{G}_{l,s}$ of dimension $l \leq k$, then there exists a permutation q-polynomial $p(x)$ and $(k-l)$ q-polynomials $q_1(x), \ldots, q_{k-l}(x)$ such that*

$$\mathcal{C} = \langle q_1(x), \ldots, q_{k-l}(x), p(x), p(x)^{[s]}, \ldots p(x)^{[s(l-1)]} \rangle. \tag{1}$$

We call the polynomials $q_i(x)$ of Lemma 3.6 *polynomials of extra type.*

Proof. By Lemma 3.4, there exists a permutation q-polynomial $p(x)$ such that

$$\mathcal{G} = \langle p(x), p(x)^{[s]}, \ldots, p(x)^{[s(l-1)]} \rangle_{\mathbb{F}_{q^n}}$$

and $p(x)$,...,$p(x)^{[s(l-1)]}$ are linearly independent. Now, we can extend the list of polynomials $\{p(x), p(x)^{[s]}, \ldots, p(x)^{[s(l-1)]}\}$ to a basis of $\mathcal{C}$ with suitable polynomials q_i as to get the form (1). □

Lemma 3.7. *If $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ is an $\mathbb{F}_{q^n}$-linear MRD-code of dimension k containing a code $\mathcal{G}$ equivalent to $\mathcal{G}_{k-1,s}$, i.e. $\mathcal{G} = \langle p(x), p(x)^{[s]}, \ldots, p(x)^{[s(k-2)]} \rangle_{\mathbb{F}_{q^n}}$ with $p(x)$ a permutation q-polynomial, and for which there exists an extra polynomial $q(x)$ in $\langle p(x)^{[-s]}, p(x)^{[s(k-1)]} \rangle_{\mathbb{F}_{q^n}}$, then $\mathcal{C}$ is equivalent to $\mathcal{H}_{k,s}(\eta)$.*

Proof. By the previous lemma,

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

with $p(x)$ permutation q-polynomial and $g(x) \in \langle p(x)^{[-s]}, p(x)^{[s(k-1)]} \rangle_{\mathbb{F}_{q^n}}$. Since $\mathcal{C}$ and $\mathcal{C}^{[s]}$ are equivalent, we can suppose that

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

with $q(x) \in \langle p(x), p(x)^{[sk]} \rangle_{\mathbb{F}_{q^n}}$, i.e. there exist $\alpha, \beta \in \mathbb{F}_{q^n}$ such that $q(x) = \alpha p(x) + \beta p(x)^{[sk]}$. So,

$$\mathcal{C} = \langle x^{[s]}, \ldots, x^{[s(k-1)]}, \alpha x + \beta x^{[sk]} \rangle_{\mathbb{F}_{q^n}} \circ p(x).$$

Since $\mathcal{C}$ is a MRD-code, then $\mathcal{H} := \mathcal{C} \circ p^{-1}(x) = \langle x^{[s]}, \ldots, x^{[s(k-1)]}, \alpha x + \beta x^{[sk]} \rangle_{\mathbb{F}_{q^n}}$ is also a MRD-code. On the other hand, by Remark 2.5, $\mathcal{H}$ is MRD if and only if $\mathcal{H} = \mathcal{H}_{k,s}(\eta)$ for some $\eta \in \mathbb{F}_{q^n}$ such that $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$. □

Theorem 3.5 prompts the following characterization of generalized twisted Gabidulin codes.

Theorem 3.8. *Let $\mathcal{C}$ be an $\mathbb{F}_{q^n}$-linear MRD-code of dimension $k > 2$ contained in $\mathcal{L}_{n,q}$. 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 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 $p(x), q(x) \in \mathcal{C}$ 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 $p(x) + \eta p(x)^{[sk]} \in \mathcal{C}$.*

Proof. The proof follows directly from Theorem 3.5 and Lemma 3.7. □

As a consequence we get the following.

Theorem 3.9. *Let $\mathcal{C}$ be an $\mathbb{F}_{q^n}$-linear RD-code of dimension $k > 2$ of $\mathcal{L}_{n,q}$, with $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$. If there exists an integer s such that $\gcd(s, n) = 1$ and*

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 $p(x), q(x) \in \mathcal{C}$ 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 $p(x) + \eta p(x)^{[sk]} \in \mathcal{C}$ and $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{kn}$,*

then $\mathcal{C}$ is a MRD-code equivalent to $\mathcal{H}_{k,s}(\eta)$.

Note that if such invertible q-polynomial $p(x)$ exists, then $\mathcal{C} \cap \mathcal{C}^{[s]} \cap \cdots \cap \mathcal{C}^{[s(k-2)]} = \langle p(x)^{[s(k-2)]} \rangle_{\mathbb{F}_{q^n}}$.

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.

As seen in the previous section, it has been shown in [18] that an MRD-code $\mathcal{C}$ of parameters $[n, k]$ 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 [18], we define for any RD-code $\mathcal{C}$ the number

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

Theorem 3.1 states that an MRD-code $\mathcal{C}$ is equivalent to a generalized Gabidulin code if and only if $h(\mathcal{C}) = k - 1$.

Also, for any given $\mathbb{F}_{q^n}$-linear code $\mathcal{C}$, the following proposition is immediate.

Proposition 4.1. *For any k-dimensional $\mathbb{F}_{q^n}$-linear code $\mathcal{C}$,*

$$\mathcal{C}^{[i]\perp} = \mathcal{C}^{\perp[i]},$$

for each $i \in \{0, \ldots, n-1\}$. So, we have

$$h(\mathcal{C}^\perp) = n - 2k + h(\mathcal{C}).$$

We now define also the *Gabidulin index*, $\operatorname{ind}(\mathcal{C})$ 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.

Clearly, $1 \leq \operatorname{ind}(\mathcal{C}) \leq k$ and $\operatorname{ind}(\mathcal{C}) = k$ if and only if $\mathcal{C}$ is a Gabidulin code. It can be readily seen that if $\mathcal{C}$ and $\mathcal{C}'$ are two equivalent codes, then they have the same indexes $\operatorname{ind}(\mathcal{C}) = \operatorname{ind}(\mathcal{C}')$ and $h(\mathcal{C}) = h(\mathcal{C}')$. Also, $h(\mathcal{C}) \geq \operatorname{ind}(\mathcal{C}) - 1$ for RD-codes.

We shall now prove that for the known codes the Gabidulin index can be effectively computed. More in detail, in the next theorem we determine these indexes for each known $\mathbb{F}_{q^n}$-linear MRD-code. Our result is contained in Table 3. Also in the table we recall the right idealisers (up to equivalence) for these codes.

Theorem 4.2. *The Gabidulin indexes* $\operatorname{ind}(\mathcal{C})$ *and the values of* $h(\mathcal{C})$ *for the known MRD-codes* $\mathcal{C}$ *of parameters* $[n,k]$ *are as given in Table 3.*

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	$\mathbb{F}_{q^3}$	$[6,2]$
$\mathcal{C}_2$	1	0	$\mathbb{F}_{q^2}$	$[6,2]$
$\mathcal{C}_3$	2	1	$\mathbb{F}_{q^n}$	$[7,3]$
$\mathcal{C}_4$	1	0	$\mathbb{F}_{q^4}$	$[8,2]$
$\mathcal{C}_5$	2	1	$\mathbb{F}_{q^n}$	$[8,3]$

Code	ind	h	R	$[n,k]$
$\mathcal{D}_1$	2	2	$\mathbb{F}_{q^3}$	$[6,4]$
$\mathcal{D}_2$	2	2	$\mathbb{F}_{q^2}$	$[6,4]$
$\mathcal{D}_3$	3	2	$\mathbb{F}_{q^n}$	$[7,4]$
$\mathcal{D}_4$	3	4	$\mathbb{F}_{q^4}$	$[8,6]$
$\mathcal{D}_5$	4	3	$\mathbb{F}_{q^n}$	$[8,5]$

Table 3: Known linear MRD-codes and their Gabidulin index

Proof. Clearly, the Gabidulin index of a generalized Gabidulin code is k; any twisted generalized Gabidulin code of dimension k contains a generalized Gabidulin code of dimension $k-1$; so, its index is $k-1$.

We now consider the case of the codes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_5, \mathcal{D}_3$ and $\mathcal{D}_5$. By construction, it is immediate to see that they all contain a generalized Gabidulin code of codimension 1; so, they also have Gabidulin index $k-1$, where k is the dimension of the code. Also for all of them $k-2 \leq h(\mathcal{C}) < k-1$, so $h(\mathcal{C}) = k-2$.

The cases of the dual codes $\mathcal{D}_i$ with $i = 1, 2, 4$ must be studied in more detail. First we prove that the codes $\mathcal{D}_1, \mathcal{D}_2$ and $\mathcal{D}_4$ do not contain any code equivalent to $\mathcal{G}_{k-1,s}$, for any s, i.e. that their Gabidulin index is less than $k-1$ and then determine the exact value.

The code $\mathcal{D}_1$

By Table 2, we have that

$$\mathcal{D}_1 = \langle x^{[1]}, x^{[2]}, x^{[4]}, x - \delta^{[5]}x^{[3]} \rangle_{\mathbb{F}_{q^6}}.$$

Suppose that there is a code $\overline{\mathcal{D}}$ contained in $\mathcal{D}_1$ equivalent to a generalized Gabidulin code of dimension 3, i.e. either $\overline{\mathcal{D}} \simeq \mathcal{G}_{3,1}$ or $\overline{\mathcal{D}} \simeq \mathcal{G}_{3,5}$. Since $\mathcal{G}_{3,1}$ and $\mathcal{G}_{3,5}$ are equivalent, then $\overline{\mathcal{D}}$ is equivalent to $\mathcal{G}_{3,1}$. By Theorem 3.1, $h(\overline{\mathcal{D}}) = 2$; on the other hand, since $\mathcal{D}_1$ is not equivalent to a Gabidulin code it must be $h(\mathcal{D}) < 3$. So, $\mathcal{D}_1 \cap \mathcal{D}_1^{[1]} = \overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[1]}$ and hence $\mathcal{D}_1 \cap \mathcal{D}_1^{[5]} = \overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[5]}$. From these equalities we get

$$\overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[1]} = \langle x^{[2]}, x^{[1]} - \delta x^{[4]} \rangle_{\mathbb{F}_{q^6}}$$

and

$$\overline{\mathcal{D}}^{[5]} \cap \overline{\mathcal{D}} = \langle x^{[1]}, x - \delta^{[5]}x^{[3]} \rangle_{\mathbb{F}_{q^6}}.$$

Since $\dim \overline{\mathcal{D}} = 3$ we obtain

$$\overline{\mathcal{D}} = \langle x^{[1]}, x^{[2]}, x^{[1]} - \delta x^{[4]} \rangle_{\mathbb{F}_{q^6}} = \langle x^{[1]}, x^{[2]}, x^{[4]} \rangle_{\mathbb{F}_{q^6}}.$$

The code $\overline{\mathcal{D}}$ is not MRD, since it contains the polynomial $x^{[1]} - x^{[4]}$ which has kernel of dimension 3, in particular it cannot be equivalent to $\mathcal{G}_{3,1}$. It follows that $\operatorname{ind}(\mathcal{D}_1) = 2$ since $\langle x^{[1]}, x^{[2]} \rangle_{\mathbb{F}_{q^6}} \simeq \mathcal{G}_{2,1}$.

The code $\mathcal{D}_2$

By Table 2 the code $\mathcal{D}_2$ is

$$\mathcal{D}_2 = \langle x^{[1]}, x^{[3]}, x - x^{[2]}, x^{[4]} - \delta x \rangle_{\mathbb{F}_{q^6}},$$

with q odd, $\delta^2 + \delta = 1$ and $q \equiv 0, \pm 1 \pmod 5$, hence $\delta \in \mathbb{F}_q$. Suppose $\operatorname{ind}(\mathcal{D}_2) = 3$, as before $\mathcal{D}_2$ contains a code $\overline{\mathcal{D}}$ equivalent to $\mathcal{G}_{3,1}$. Arguing as the previous case, we get

$$\overline{\mathcal{D}} = \langle -x + x^{[2]}, x^{[3]} - \delta x^{[1]}, -x^{[1]} + x^{[3]} \rangle_{\mathbb{F}_{q^6}} = \langle x^{[1]}, x^{[3]}, -x + x^{[2]} \rangle_{\mathbb{F}_{q^6}}.$$

To show that $\overline{\mathcal{D}}$ is not equivalent to any $\mathcal{G}_{3,s}$ we compute its right idealiser $R(\overline{\mathcal{D}})$. Write $\varphi(x) = \sum_{i=0}^{5} a_i x^{[i]} \in R(\overline{\mathcal{D}})$; then $x^{[1]} \circ \varphi(x), x^{[3]} \circ \varphi(x) \in \overline{\mathcal{D}}$, so $\varphi(x) = \eta x$, for some $\eta \in \mathbb{F}_{q^6}$. Furthermore, $(x - x^{[2]}) \circ \varphi(x) \in \overline{\mathcal{D}}$; so $\eta = \eta^{[2]}$ and $\eta \in \mathbb{F}_{q^2}$. So, we get $R(\overline{\mathcal{D}}) \simeq \mathbb{F}_{q^2}$. If $\overline{\mathcal{D}}$ were to be equivalent to $\mathcal{G}_{3,1}$, by Proposition 2.3 and by [26, Corollary 5.2], it would follow that $R(\overline{\mathcal{D}})$ is equivalent to $R(\mathcal{G}_{3,1}) \simeq \mathbb{F}_{q^6}$, which is not possible. Suppose now $\mathcal{D}_2$ to contain a code $\overline{\mathcal{D}}$ equivalent to $\mathcal{G}_{2,1}$.

Then by Theorem 3.1 and by Lemma 3.4 we easily get $\overline{\mathcal{D}} = \langle f(x), f(x)^{[1]} \rangle_{\mathbb{F}_{q^6}}$ with $f(x)$ an invertible linearized polynomial. Also, $\overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[1]} = \langle f(x)^{[1]} \rangle \subset \mathcal{D}_2 \cap \mathcal{D}_2^{[1]} = \langle -x^{[1]} + x^{[3]}, x^{[4]} - \delta x^{[2]} \rangle_{\mathbb{F}_{q^6}}$, so $f(x)^{[1]} = a(-x^{[1]} + x^{[3]}) + b(x^{[4]} - \delta x^{[2]})$, since $f(x)$ is invertible we may assume $b = 1$. In particular, $\mathcal{D}_2$ contains a code equivalent to $\mathcal{G}_{2,1}$ if and only if there exists $a \in \mathbb{F}_{q^6}$ such that $f(x)^{[1]}$ is invertible. Let $D_{f^{[1]}}$ be the Dickson matrix associated to the polynomial $f(x)^{[1]}$ considered above. Then, for $a = 1$ we have $\det D_{f^{[1]}} = 16(2 - 3\delta) \neq 0$. So, $\mathcal{D}_2$ contains $\langle -x - \delta x^{[1]} + x^{[2]} + x^{[3]}, -x^{[1]} + x^{[3]} + x^{[4]} - \delta x^{[2]} \rangle_{\mathbb{F}_{q^6}} \simeq \mathcal{G}_{2,1}$ and, consequently, $\operatorname{ind}(\mathcal{D}_2) = 2$.

The code $\mathcal{D}_4$

The code $\mathcal{D}_4$ is

$$\mathcal{D}_4 = \langle x^{[1]}, x^{[2]}, x^{[3]}, x^{[5]}, x^{[6]}, x - \delta x^{[4]} \rangle_{\mathbb{F}_{q^8}},$$

with q odd and $\delta^2 = -1$. Suppose that $\mathcal{D}_4$ contains a code $\overline{\mathcal{D}}$ equivalent to a generalized Gabidulin code of dimension 5. Since $\mathcal{G}_{5,1} \simeq \mathcal{G}_{5,7}$ and $\mathcal{G}_{5,3} \simeq \mathcal{G}_{5,5}$, we get that either $\overline{\mathcal{D}} \simeq \mathcal{G}_{5,1}$ or $\overline{\mathcal{D}} \simeq \mathcal{G}_{5,3}$. By Lemma 3.4, $\dim(\overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[s]}) = 4$, with either $s = 1$ or $s = 3$, and, since $\mathcal{D}_4$ is not equivalent to any generalized Gabidulin code, $\dim(\mathcal{D}_4 \cap \mathcal{D}_4^{[s]}) < 5$, so $\mathcal{D}_4 \cap \mathcal{D}_4^{[s]} = \overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[s]}$. First assume that $\overline{\mathcal{D}} \simeq \mathcal{G}_{5,1}$. It is easy to see that

$$\overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[1]} = \langle x^{[2]}, x^{[3]}, x^{[6]}, x^{[1]} - \delta^{[1]} x^{[5]} \rangle_{\mathbb{F}_{q^8}}.$$

Since the dimension of $\overline{\mathcal{D}}$ is 5 and $x^{[1]} \in \overline{\mathcal{D}} \setminus (\overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[1]})$, it follows that

$$\overline{\mathcal{D}} = \langle x^{[1]}, x^{[2]}, x^{[3]}, x^{[6]}, x^{[1]} - \delta^{[1]} x^{[5]} \rangle_{\mathbb{F}_{q^8}} = \langle x^{[1]}, x^{[2]}, x^{[3]}, x^{[5]}, x^{[6]} \rangle_{\mathbb{F}_{q^8}}.$$

The Delsarte dual of $\overline{\mathcal{D}}$ is

$$\overline{\mathcal{D}}^{\perp} = \langle x, x^{[4]}, x^{[7]} \rangle_{\mathbb{F}_{q^8}},$$

which is not MRD, since of $x - x^{[4]}$ has kernel of dimension 4. By Lemma 2.1, neither $\overline{\mathcal{D}}$ is an MRD-code, a contradiction. Now, assume $\overline{\mathcal{D}} \simeq \mathcal{G}_{5,3}$. As before,

$$\overline{\mathcal{D}} \cap \overline{\mathcal{D}}^{[3]} = \langle x^{[1]}, x^{[5]}, x^{[6]}, x - \delta x^{[4]} \rangle_{\mathbb{F}_{q^8}}$$

and

$$\overline{\mathcal{D}}^{[5]} \cap \overline{\mathcal{D}} = \langle x^{[6]}, x^{[2]}, x^{[3]}, x^{[5]} - \delta^{[5]} x^{[1]} \rangle_{\mathbb{F}_{q^8}}.$$

So,

$$\overline{\mathcal{D}} = \langle x^{[1]}, x^{[6]}, x^{[2]}, x^{[3]}, x^{[5]} - \delta^{[5]} x^{[1]} \rangle_{\mathbb{F}_{q^8}} = \langle x^{[1]}, x^{[2]}, x^{[3]}, x^{[5]}, x^{[6]} \rangle_{\mathbb{F}_{q^8}}.$$

Again we get a contradiction since $\overline{\mathcal{D}}$ is not an MRD-code.

Suppose now that $\mathcal{D}_4$ contains a code $\overline{\mathcal{D}}$ equivalent to $\mathcal{G}_{4,1}$. By Theorem 3.1 and by Lemma 3.4, $\overline{\mathcal{D}} = \langle p(x), p(x)^{[1]}, p(x)^{[2]}, p(x)^{[3]} \rangle_{\mathbb{F}_{q^8}}$ for some invertible q-polynomial $p(x) \in \mathcal{D}_4$. Clearly, $\langle p(x)^{[1]}, p(x)^{[2]}, p(x)^{[3]} \rangle_{\mathbb{F}_{q^8}} \subset \langle x^{[2]}, x^{[3]}, x^{[6]}, x^{[1]} - \delta^{[1]} x^{[5]} \rangle_{\mathbb{F}_{q^8}} = \mathcal{D}_4 \cap \mathcal{D}_4^{[1]}$ and so there exist $a, b, c, d \in \mathbb{F}_{q^8}$ such that

$$p(x)^{[1]} = ax^{[2]} + bx^{[3]} + cx^{[6]} + d(x^{[1]} - \delta^{[1]} x^{[5]}),$$

$$p(x)^{[2]} = a^{[1]} x^{[3]} + b^{[1]} x^{[4]} + c^{[1]} x^{[7]} + d^{[1]} (x^{[2]} - \delta^{[2]} x^{[6]}),$$

$$p(x)^{[3]} = a^{[2]} x^{[4]} + b^{[2]} x^{[5]} + c^{[2]} x + d^{[2]} (x^{[3]} - \delta^{[3]} x^{[7]}).$$

Since these are all elements of $\mathcal{D}_4$, we get $a = b = c = d = 0$, i.e. $\mathcal{D}_4$ cannot contain a code equivalent to $\mathcal{G}_{4,1}$. Finally, suppose that $\overline{\mathcal{D}}$ is equivalent to $\mathcal{G}_{4,3}$. By Theorem 3.1 and by Lemma 3.4, $\overline{\mathcal{D}} = \langle p(x), p(x)^{[3]}, p(x)^{[6]}, p(x)^{[1]} \rangle_{\mathbb{F}_{q^8}}$ for some invertible q-polynomial $p(x) \in \mathcal{D}_4$ and arguing as before we get a contradiction, i.e. $\mathcal{D}_4$ cannot contain a code equivalent to $\mathcal{G}_{4,3}$. So, $\mathcal{D}_4$ cannot contain a code equivalent to a generalized Gabidulin code of dimension 4 and so $\operatorname{ind}(\mathcal{D}_4) < 4$. Since $\langle x^{[1]}, x^{[2]}, x^{[3]} \rangle_{\mathbb{F}_{q^8}} \simeq \mathcal{G}_{3,1}$, it follows $\operatorname{ind}(\mathcal{D}_4) = 3$. □

Thus Theorem 3.5 provides the following structure result on k-dimensional $\mathbb{F}_{q^n}$-linear RD-codes with $h(\mathcal{C}) = k - 2$.

Theorem 4.3. *Let $\mathcal{C}$ be a k-dimensional $\mathbb{F}_{q^n}$-linear RD-code of $\mathcal{L}_{n,q}$ having $h(\mathcal{C}) = k-2$, with $k > 2$. Denote by s an integer such that $\gcd(s, n) = 1$ and $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) = k - 2$. Let $V := \mathcal{C} \cap \mathcal{C}^{[s]}$ and suppose that $\mathcal{C} \cap \mathcal{U}_1 = \{0\}$, then $\mathcal{C}$ has one of the following forms*

1. *if $\dim(V \cap V^{[s]}) = k - 3$, then there exist $p(x)$ and $q(x)$ in $\mathcal{C}$ such that*

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

2. *if $\dim(V \cap V^{[s]}) = k - 4$, then there exist $p(x)$ and $q(x)$ in $\mathcal{C}$ such that*

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

where

$$(i, j) = \begin{cases} (\frac{k}{2}, \frac{k}{2}) & \text{if } k \text{ is even} \\ (\frac{k-1}{2}, \frac{k+1}{2}) & \text{if } k \text{ is odd.} \end{cases}$$

In particular, $\mathcal{C}$ is equivalent to $\mathcal{H}_{k,s}(\eta)$, for some $\eta \in \mathbb{F}_{q^n}$, if and only if $\dim(V \cap V^{[s]}) = k-3$, $p(x)$ is invertible and there exists $\eta \in \mathbb{F}_{q^n}^*$ such that $p(x) + \eta p(x)^{[sk]} \in \mathcal{C}$ and $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{kn}$.

Remark 4.4. Note that, in the hypothesis of Theorem 4.3, if one of the polynomials $p(x)$ or $q(x)$ is invertible, then either $\operatorname{ind}(\mathcal{C}) = \dim \mathcal{C} - 1$ or $\operatorname{ind}(\mathcal{C}) \geq \dfrac{\dim \mathcal{C}}{2}$. This holds for the known MRD-codes listed in the Tables 1 and 2; it is currently an open question whether an $\mathbb{F}_{q^n}$-linear MRD-code $\mathcal{C}$ having $h(\mathcal{C}) = \dim \mathcal{C} - 2$ and $\operatorname{ind}(\mathcal{C}) < \frac{\dim \mathcal{C}}{2}$ might exist or not. We also remark that the known MRD-codes presented in the Tables 1 and 2 which are not equivalent to a generalized Gabidulin code, have $h(\mathcal{C}) = \dim \mathcal{C} - 2$.

Suppose a code $\mathcal{C}$ has generator matrix in standard form $[I_k|X]$. Using the arguments of [19, Lemma 19] it can be seen that $\dim(\mathcal{C} \cap \mathcal{C}^{[s]}) \geq \dim \mathcal{C} - i$ with $i > 0$ if and only if $rk(X - X^{[s]}) \leq i$, and this condition can be expressed by imposing that all minors of $X - X^{[s]}$ of rank $j > i$ have determinant 0. In particular, the set of all codes with $h(\mathcal{C}) \geq \dim(\mathcal{C}) - i$ is contained in the union of a finite number of closed Zariski sets. So, for a generic MRD-code we have $h(\mathcal{C}) = 0$. We leave as an open problem to determine some families of MRD-codes with $h(\mathcal{C}) < \dim(\mathcal{C}) - 2$ and, more in detail, to determine the possible spectrum of the values of $h(\mathcal{C})$ might attain as $\mathcal{C}$ varies among all MRD-codes over a given field.

References

[1] D. Bartoli and Y. Zhou: Exceptional scattered polynomials, *J. Algebra* **509** (2018), 507–534.

[2] E. Byrne and A. Ravagnani: Partition-balanced families of codes and asymptotic enumeration in coding theory, https://arxiv.org/abs/1805.02049.

[3] A. Cossidente, G. Marino and F. Pavese: Non-linear maximum rank distance codes, *Des. Codes Cryptogr.* **79(3)** (2016), 597–609.

[4] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in PG$(1, q^n)$, *J. Combin. Theory Ser. A* **157** (2018), 402–426.

[5] B. Csajbók, G. Marino, O. Polverino and C. Zanella: A new family of MRD-codes, *Linear Algebra Appl.* **548** (2018), 203–220.

[6] B. Csajbók, G. Marino, O. Polverino and Y. Zhou: Maximum Rank-Distance codes with maximum left and right idealisers, https://arxiv.org/abs/1807.08774.

[7] B. Csajbók, G. Marino, O. Polverino and F. Zullo: Maximum scattered linear sets and MRD-codes, *J. Algebraic Combin.* **46.3-4** (2017), 517–531.

[8] B. Csajbók, G. Marino, O. Polverino and F. Zullo: A characterization of linearized polynomials with maximum kernel, https://arxiv.org/abs/1806.05962.

[9] B. Csajbók, G. Marino and F. Zullo: New maximum scattered linear sets of the projective line, https://arxiv.org/abs/1709.00926.

[10] B. Csajbók and C. Zanella: On the equivalence of linear sets, *Des. Codes Cryptogr.* **81(2)** (2016), 269–281.

[11] B. Csajbók and C. Zanella: On scattered linear sets of pseudoregulus type in PG$(1, q^t)$, *Finite Fields Appl.* **41** (2016), 34–54.

[12] J. de la Cruz, M. Kiermaier, A. Wassermann and W. Willems: Algebraic structures of MRD Codes, *Adv. Math. Commun.* **10** (2016), 499–510.

[13] P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25** (1978), 226–241.

[14] N. Durante and A. Siciliano: Non-linear maximum rank distance codes in the cyclic model for the field reduction on finite geometries, *Electron. J. Combin.* **24.2** (2017), 2–33.

[15] E. Gabidulin: Theory of codes with maximum rank distance, *Problems of information transmission*, **21**(3) (1985), 3–16.

[16] R. Gow and R. Quinlan: Galois theory and linear algebra, *Linear Algebra Appl.*, **430** (2009), 1778–1789.

[17] G. McGuire and J. Sheekey, A Characterization of the Number of Roots of Linearized and Projective Polynomials in the Field of Coefficients, https://arxiv.org/abs/1806.05853.

[18] A. Horlemann-Trautmann and K. Marshall: New criteria for MRD and Gabidulin codes and some rank-metric code constructions, *Adv. Math. Commun.* **11(3)** (2017), 533–548.

[19] A. Horlemann-Trautmann, A. Neri, T. Randrianarisoa and J. Rosenthal: On the genericity of maximum rank distance and Gabidulin codes, *Des. Codes Cryptogr.* **86(2)** (2017), 1–23.

[20] A. Kshevetskiy and E. Gabidulin: The new construction of rank codes, International Symposium on Information Theory, 2005. ISIT 2005. Proceedings, pages 2105–2108, Sept. 2005.

[21] R. Lidl and H. Niederreiter: Finite fields, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997.

[22] D. Liebhold and G. Nebe: Automorphism groups of Gabidulin-like codes, *Arch. Math.* **107**(4) (2016), 355–366.

[23] G. Lunardon: Normal spreads, *Geom. Dedicata* **75** (1999), 245–261.

[24] G. Lunardon: MRD-codes and linear sets, *J. Combin. Theory Ser. A* **149** (2017), 1–20.

[25] G. Lunardon, R. Trombetti and Y. Zhou: Generalized Twisted Gabidulin Codes, *J. Combin. Theory Ser. A* **159** (2018), 79–106.

[26] G. Lunardon, R. Trombetti and Y. Zhou: On kernels and nuclei of rank metric codes, *J. Algebraic Combin.* **46** (2017), 313–340.

[27] A. Neri: Systematic encoders for generalized Gabidulin codes and the q-analogue of Cauchy matrices, https://arxiv.org/abs/1805.06706.

[28] K. Otal and F. Ozbudak: Additive rank metric codes, *IEEE Trans. Inform. Theory* **63(1)** (2017), 164–168.

[29] K. Otal and F. Ozbudak: Some new non-additive maximum rank distance codes, *Finite Fields Appl.* **50** (2018), 293–303.

[30] R. Overbeck: Structural Attacks for Public Key Cryptosystems based on Gabidulin Codes, *J. of Cryptology* **21** (2008), 208-301.

[31] S. Puchinger, J. Renner and A. Wachter-Zeh: Twisted Gabidulin Codes in the GPT Cryptosystem, https://arxiv.org/abs/1806.10055

[32] J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10**(3) (2016), 475–488.

[33] J. Sheekey: New Semifields and new MRD Codes from Skew Polynomial Rings, https://arxiv.org/abs/1806.00251.

[34] J. Sheekey and G. Van de Voorde: Rank-metric codes, linear sets and their duality, https://arxiv.org/abs/1806.05929.

[35] R. Trombetti and Y. Zhou: A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$, *IEEE Transactions on Information Theory*, to appear, 2018.

[36] B. Wu and Z. Liu:, Linearized polynomials over finite fields revisited, *Finite Fields Appl.* **22** (2013), 79–100.

Authors' addresses:

Luca Giuzzi
D.I.C.A.T.A.M. (Section of Mathematics)
University of Brescia
Via Branze 43, I-25123, Brescia, Italy
luca.giuzzi@unibs.it

Ferdinando Zullo
Department of Mathematics and Physics
University of Campania "*Luigi Vanvitelli*"
Viale Lincoln 5, I-81100, Caserta, Italy
ferdinando.zullo@unicampania.it