Non-linear MRD codes from cones over exterior sets

Nicola Durante Giovanni Giuseppe Grimaldi Giovanni Longobardi

Abstract

By using the notion of a d-embedding Γ of a (canonical) subgeometry Σ and of exterior sets with respect to the h-secant variety $\Omega_h(\mathcal{A})$ of a subset \mathcal{A} , $0 \leq h \leq n-1$, in the finite projective space $\operatorname{PG}(n-1,q^n)$, $n \geq 3$, in this article we construct a class of non-linear (n,n,q;d)-MRD codes for any $2 \leq d \leq n-1$. A code of this class $\mathcal{C}_{\sigma,T}$, where $1 \in T \subseteq \mathbb{F}_q^*$ and σ is a generator of $\operatorname{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$, arises from a cone of $\operatorname{PG}(n-1,q^n)$ with vertex an (n-d-2)-dimensional subspace over a maximum exterior set \mathcal{E} with respect to $\Omega_{d-2}(\Gamma)$. We prove that the codes introduced in [2, 8, 9] are suitable punctured ones of $\mathcal{C}_{\sigma,T}$ and we solve completely the inequivalence issue for this class showing that $\mathcal{C}_{\sigma,T}$ is neither equivalent nor adjointly equivalent to the non-linear MRD codes $\mathcal{C}_{n,k,\sigma,I}$, $I \subseteq \mathbb{F}_q$, obtained in [27].

2020 MSC: 51E99, 05B25

Keywords: linear set, rank distance code, linearized polynomial, finite field

1 Introduction

From the 1970s to the present day, rank distance codes have been deeply studied as useful tool to correct errors and erasures in networks, and for the increasing applications which they have in storage systems [31], cryptosystems [25], space-time codes [36] and random linear network coding [35]. Moreover, they are linked to many structures studied in finite geometry such as semifields, linear sets, splitting dimensional dual hyperovals and q-polymatroids; for more details see [12, 29, 33] and the references therein. Delsarte [5] and Gabidulin [10] introduced, independently, rank distance codes as sets of matrices over a finite field equipped with the distance d(A, B) = rk(A - B). The most studied ones are codes with the largest possible size. These are called maximum rank distance codes, MRD codes for short. Rank distance codes that are very rich in structure, for instance subgroups or subspaces of matrices, are the most studied in literature. While only few classes of

non-additive and non-linear are known for almost any choices of parameters.

In this paper, we will give a geometric construction of a new family of these objects. These codes will be obtained from a cone of a projective space whose vertex is a proper subspace and whose base is a special pointset skew with the vertex. The base of such a cone is linked to the non-linear MRD codes constructed by Cossidente et al. [2], Durante and Siciliano [9] and Donati and Durante [8]. These latter can be obtained in turn by puncturing codes in the relevant family. Finally, we will show that this class of codes is not equivalent to that one constructed by Otal and Özbudak in [27].

The article is structured as follows: in Section 2, some basic notions on rank distance codes will be recalled and the state of the art of the known MRD codes will be traced. In Section 3 and 4, the geometric setting will be introduced and the codes exhibited in [8] by Donati and Durante recalled. In Section 5, a geometrical configuration about cones over some particular subsets of the finite projective space will be investigated and this will give rise to our class of non-linear codes exhibited in Section 6. Finally in Section 7, we will show that this class is effectively new, it contains a class of linear MRD codes, and, in certain sense, a class of non-linear MRD ones already known.

2 Preliminary results and notions

Let \mathbb{F}_q be the finite field of q elements, q a prime power, and let $\mathbb{F}_q^{m \times n}$ be the set of $m \times n$ matrices with entries over \mathbb{F}_q endowed with rank distance

$$d: (A, B) \in \mathbb{F}_q^{m \times n} \times \mathbb{F}_q^{m \times n} \longrightarrow \operatorname{rk}(A - B) \in \{0, 1, \dots, \min\{m, n\}\}.$$

A subset of $\mathbb{F}_q^{m \times n}$, including at least two elements is called a rank distance code. The minimum distance $d(\mathcal{C})$ of a code \mathcal{C} is naturally defined by

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

If $d = d(\mathcal{C})$, we will say that \mathcal{C} is an (m, n, q; d)-rank distance code. An (m, n, q; d)-rank distance code is additive if it is an additive subgroup of $\mathbb{F}_q^{m \times n}$. An additive code is \mathbb{F}_q -linear if it is a subspace of $\mathbb{F}_q^{m \times n}$ seen as a vector space over \mathbb{F}_q . A code that it is not an \mathbb{F}_q -subspace is called a non-linear code.

It is well-known that the size of an (m, n, q; d)-rank distance code C satisfies the *Singleton-like bound*, see e.g. [5, Theorem 5.4]:

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

When this bound is achieved, C is called an (m, n, q; d)-maximum rank distance code, or in short (m, n, q; d)-MRD code. The adjoint code of C is defined as the

code made up by the transpose matrices belonging to C:

$$\mathcal{C}^t = \{C^t : C \in \mathcal{C}\}$$

where the superscript t stands for the matrix transposition. By the classification of rank isometries of $\mathbb{F}_q^{m \times n}$ [38, Theorem 3.5], two rank distance codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{m \times n}$, $m, n \geq 2$, are called *equivalent* if there exist $P \in \mathrm{GL}(m,q), \ Q \in \mathrm{GL}(n,q), \ R \in \mathbb{F}_q^{m \times n}$ and a field automorphism $\rho \in \mathrm{Aut}(\mathbb{F}_q)$ such that

$$C' = PC^{\rho}Q + R = \{PC^{\rho}Q + R : C \in \mathcal{C}\}.$$

When m = n, in addition to being equivalent, two codes are said adjointly equivalent if

$$C' = P(C^t)^{\rho}Q + R = \left\{ P(C^t)^{\rho}Q + R : C \in \mathcal{C} \right\}.$$

If both $\mathcal C$ and $\mathcal C'$ are additive, then we may assume that R is the zero matrix. The code $\mathcal C^{[u]}\subseteq \mathbb F_q^{(m-u)\times n}$ obtained from $\mathcal C\subseteq \mathbb F_q^{m\times n}$ by deleting the last u rows, $1\leq u\leq m-1$, is called a *punctured code* of $\mathcal C$. In [1, Corollary 7.3], it is showed that if $\mathcal C\subseteq \mathbb F_q^{m\times n}$, $m\leq n$, is an MRD code then $\mathcal C^{[u]}$ is MRD as well.

The left and right idealisers of a code $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ are defined as the sets

$$I_L(\mathcal{C}) = \left\{ P \in \mathbb{F}_q^{m \times m} : PC \in \mathcal{C}, \forall C \in \mathcal{C} \right\}$$

and

$$I_R(\mathcal{C}) = \left\{ Q \in \mathbb{F}_q^{n \times n} : CQ \in \mathcal{C}, \forall C \in \mathcal{C} \right\},$$

respectively.

Although the rank distance codes are subsets of matrices, they can be represented in a particular setting, that of σ -linearized polynomials. From now on, suppose m=n and let $\sigma: x \in \mathbb{F}_{q^n} \longrightarrow x^{q^s} \in \mathbb{F}_{q^n}$ be a field automorphism of \mathbb{F}_{q^n} with $\gcd(s,n)=1$.

A σ -linearized polynomial with coefficients over \mathbb{F}_{q^n} is a polynomial of the form $\alpha = \sum_{i=0}^{\ell} \alpha_i X^{\sigma^i} \in \mathbb{F}_{q^n}[X], \ \ell \in \mathbb{N}$. If $\alpha_\ell \neq 0$, the integer ℓ is called the σ -degree of α and it will be denoted $\deg_{\sigma} \alpha$ or $\deg_{q^s} \alpha$. The set $\mathcal{L}_{n,q,\sigma}$ of σ -linearized polynomials with coefficients over \mathbb{F}_{q^n} equipped with the usual sum, the scalar multiplication by an element of \mathbb{F}_{q^n} and the map composition is an algebra over \mathbb{F}_{q^n} . While, the set

$$\tilde{\mathcal{L}}_{n,q,\sigma} = \left\{ \sum_{i=0}^{n-1} \alpha_i X^{\sigma^i} : \alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_{q^n} \right\}$$
 (1)

endowed with the sum as in $\mathcal{L}_{n,q,\sigma}$, the multiplication by an element of \mathbb{F}_q and the composition modulo $X^{q^{ns}} - X$ is an algebra over \mathbb{F}_q isomorphic to the algebra of the endomorphisms of \mathbb{F}_{q^n} seen as vector space over \mathbb{F}_q . Indeed, it is well known that

any \mathbb{F}_q -linear endomorphism of \mathbb{F}_{q^n} can be represented uniquely as a σ -polynomial belonging to $\tilde{\mathcal{L}}_{n,q,\sigma}$, [17, Chapter 3]. Then any rank distance code \mathcal{C} , $|\mathcal{C}| \geq 2$, can be seen as a suitable subset of $\tilde{\mathcal{L}}_{n,q,\sigma}$.

So, the definitions of transpose matrix, adjoint code and equivalence between codes can be naturally reformulated in this environment. Let $\alpha = \sum_{i=0}^{n-1} \alpha_i X^{\sigma^i} \in \tilde{\mathcal{L}}_{n,q,\sigma}$, then the adjoint polynomial of α is defined as

$$\hat{\alpha} = \sum_{i=0}^{n-1} \alpha_i^{\sigma^{n-i}} X^{\sigma^{n-i}}$$

and if $C \subseteq \tilde{\mathcal{L}}_{n,q,\sigma}$ is a rank distance code, $C^t = \{\hat{\alpha} : \alpha \in C\}$. Moreover, two rank codes C and C' are equivalent or adjointly equivalent if there exists (f, ρ, g, h) such that $f, g, h \in \tilde{\mathcal{L}}_{n,q,\sigma}$, with f and g permutation polynomials, and $\rho \in \operatorname{Aut}(\mathbb{F}_q)$ such that

$$\mathcal{C}' = \{ f \circ \alpha^{\rho} \circ g + h \colon \alpha \in \mathcal{C} \} \text{ or } \mathcal{C}' = \{ f \circ \alpha^{\rho} \circ g + h \colon \alpha \in \mathcal{C}^t \},$$

respectively. Here the automophism ρ acts only over the coefficients of a polynomial α in \mathcal{C} or \mathcal{C}^t , respectively. A map

$$(f, \rho, g, h) : \alpha \in \mathcal{C} \longrightarrow f \circ \alpha^{\rho} \circ g + h \in \mathcal{C}'$$

is called an *equivalence* between \mathcal{C} and \mathcal{C}' . If $\mathcal{C} = \mathcal{C}'$, an equivalence is said an *automorphism* of \mathcal{C} . The set $\operatorname{Aut}(\mathcal{C})$ of all automorphisms of \mathcal{C} is a group with respect to the product

$$(f, \rho, g, h) \star (f', \rho', g', h') = (f' \circ f^{\rho'}, \rho \rho', g^{\rho'} \circ g', f' \circ h^{\rho'} \circ g' + h')$$

where the composition is taken modulo $X^{q^{ns}} - X$.

To make this article as self-contained as possible, we shall present the state of the art regarding the known (n, n, q; d)-MRD codes in the linearized polynomials setting. Although, very recently, new constructions of both linear and non-linear rectangular MRD codes have been exhibited by Minjia Shi $et\ al.$ in [24]. We shall start from maximum rank distance code that are \mathbb{F}_q -linear subspaces of $\tilde{\mathcal{L}}_{n,q,\sigma}$.

2.1 Linear MRD codes

The first class of linear MRD codes, discovered by Delsarte [5] and Gabidulin [10], are known in literature as *Delsarte-Gabidulin codes*. Later in [11], Gabidulin and Kshevetskiy provided a generalization of them, called *generalized Gabidulin*

codes that we shall recap in our notations: let $1 \le k \le n$ be an integers, then a generalized Gabidulin code is the set of linearized polynomials

$$\mathcal{G}_{k,\sigma} = \left\{ \sum_{i=0}^{k-1} \alpha_i X^{\sigma^i} \colon \alpha_0, \dots, \alpha_{k-1} \in \mathbb{F}_{q^n} \right\}$$

and it is an (n, n, q; n - k + 1)-MRD code.

In [32], Sheekey exhibited a wider class of linear MRD codes, called twisted Gabidulin codes and later generalized in [23] by Lunardon, Trombetti and Zhou. Let n, k, h be positive integers, $1 \le k < n$ and let η be in \mathbb{F}_{q^n} such that $N_{q^{sn}/q^s}(\eta) \ne (-1)^{nk}$, then a generalized twisted Gabidulin code is the set

$$\mathcal{H}_{k,\sigma}(\eta,h) = \left\{ \sum_{i=0}^{k-1} \alpha_i X^{\sigma^i} + \eta \alpha_0^{q^h} X^{\sigma^k} : \alpha_0, \dots, \alpha_{k-1} \in \mathbb{F}_{q^n} \right\}$$

and it is an (n, n, q; n - k + 1)-MRD code¹.

Puchinger *et al.* provided a further generalization of generalized twisted Gabidulin codes in [30].

Finally, a family of maximum rank distance codes in $\tilde{\mathcal{L}}_{n,q,\sigma}$, $n=2t, 1 \leq k < n$ and q odd was discovered by Trombetti and Zhou in 2019 and described in [37]: let $\xi \in \mathbb{F}_{q^n}$ satisfying that $N_{q^n/q}(\xi)$ is a non-square in \mathbb{F}_q , then

$$\mathcal{D}_{k,\sigma}(\xi) = \left\{ \sum_{i=0}^{k-1} \alpha_i X^{\sigma^i} + \xi \alpha_k X^{\sigma^k} : \alpha_0, \alpha_k \in \mathbb{F}_{q^t}, \alpha_1, \dots, \alpha_{k-1} \in \mathbb{F}_{q^n} \right\}$$

is an (n, n, q; n - k + 1)-MRD code.

2.2 Additive MRD codes

In [26], Otal and Özbudak showed a family of non-linear additive MRD codes as a generalization of generalized twisted Gabidulin codes. Let n, k, u, h be positive integers satisfying $q = q_0^u$ and $1 \le k < n$. Let $\eta \in \mathbb{F}_{q^n}$ such that $N_{q^{sn}/q_0^s}(\eta) \ne (-1)^{nku}$. Then the set

$$\mathcal{A}_{k,\sigma,q_0}(\eta,h) = \left\{ \sum_{i=0}^{k-1} \alpha_i X^{\sigma^i} + \eta \alpha_0^{q_0^h} X^{\sigma^k} : \alpha_0, \dots, \alpha_{k-1} \in \mathbb{F}_{q^n} \right\}$$
 (2)

¹The symbol $N_{q^m/q^\ell}(x) = x^{\frac{q^m-1}{q^\ell-1}}$ denote the *norm* of $x \in \mathbb{F}_{q^m}$ over \mathbb{F}_{q^ℓ} , where m, ℓ are integers with $\ell \mid m$.

is an \mathbb{F}_{q_0} -linear (n, n, q; n - k + 1)-MRD code.

Later, another family of non-linear additive MRD codes appeared in [34]. Let $F \in \mathbb{F}_q[Y]$ be irreducible polynomial of degree r and let consider the ideal $\mathcal{I} = (F(X^{q^{sn}}))$ contained in $\mathcal{L}_{n,q,\sigma}$. Let $\rho \in \operatorname{Aut}(\mathbb{F}_q)$ with $\operatorname{Fix}(\rho) = \mathbb{F}_{q_0}$ and let $\eta \in \mathbb{F}_{q^n}$ such that $\operatorname{N}_{q^n/q_0}(\eta)\operatorname{N}_{q/q_0}((-1)^{kr(n-1)}F_0^k) \neq 1$. Then, the set

$$S_{k,\sigma}(\eta,\rho) = \left\{ \sum_{i=0}^{k-1} \alpha_i X^{\sigma^i} + \eta \alpha_0^{\rho} X^{\sigma^k} + \mathcal{I} : \alpha_0, \dots, \alpha_{k-1} \in \mathbb{F}_{q^n} \right\} \subseteq \mathcal{L}_{n,q,\sigma}/\mathcal{I} \cong \mathbb{F}_{q^r}^{n \times n}$$

is an \mathbb{F}_{q_0} -linear MRD code of $\mathbb{F}_{q^r}^{n \times n}$ of size q^{nrk} , [34, Theorem 7]. Note that for suitable choices of F, ρ and η , the (twisted) generalized Gabidulin codes and the non-linear additive codes in (2) return, see [34, Remark 3].

2.3 Non-linear MRD codes

In finite geometry (n, n, q; n)-MRD codes are known as spread sets (see e.g. [6]) and there are examples for both cases linear and non-linear. These are linked to algebraic and geometric structures such as quasifields, semifields and translation planes coordinatized over them, see [4] and [15]. The first class of non-linear MRD codes whose codewords are not invertible and so different from spread sets, are the (3,3,q;2)-MRD codes constructed by Cossidente et al. [2]. These arise from a geometrical context and have been generalized in two steps: firstly, by Durante and Siciliano [9] obtaining a family of (n,n,q;n-1)-MRD codes, $n \geq 3$, and then by Donati and Durante obtaining a family of (d+1,n,q;d)-MRD codes, $2 \leq d \leq n-1$, see [8]. As we shall extend this family further, we will describe it in detail in Section 4.

The second family of non-additive MRD codes for all n, d has been constructed by Otal and Özbudak in [27]: let I be a subset of \mathbb{F}_q , $1 \le k \le n-1$ and consider

$$C_{n,k,\sigma,I}^{(1)} = \left\{ \sum_{i=0}^{k-1} \alpha_i X^{\sigma^i} : \alpha_0, \dots, \alpha_{k-1} \in \mathbb{F}_{q^n}, N_{q^n/q}(\alpha_0) \in I \right\},$$
 (3)

$$\mathcal{C}_{n,k,\sigma,I}^{(2)} = \left\{ \sum_{i=1}^k \beta_i X^{\sigma^i} : \beta_1, \dots, \beta_k \in \mathbb{F}_{q^n}, N_{q^n/q}(\beta_k) \not\in (-1)^{n(k+1)} I \right\}.$$

Then $C_{n,k,\sigma,I} = C_{n,k,\sigma,I}^{(1)} \cup C_{n,k,\sigma,I}^{(2)} \subseteq \tilde{\mathcal{L}}_{n,q,\sigma}$ is an (n,n,q;n-k+1)-MRD code. In [27, Corollary 2.1], they proved

1. if q = 2 or $I \in \{\emptyset, \{0\}, \mathbb{F}_q^*, \mathbb{F}_q\}$ then $\mathcal{C}_{n,k,\sigma,I}$ is equivalent to a generalized Gabidulin code;

2. if q > 2 and $I \notin \{\emptyset, \{0\}, \mathbb{F}_q^*, \mathbb{F}_q\}$, then $\mathcal{C}_{n,k,\sigma,I}$ is not an affine code (i.e. not a translated version of an additive code).

In the following sections, we provide a geometric construction for a class of non-linear (n, n, q; d)-MRD $\mathcal{C}_{\sigma,T}$, $1 \in T \subseteq \mathbb{F}_q^*$, $2 \leq d \leq n-1$, and puncturing properly a code in this relevant class, we get a code described in [8]. We shall show that this class is effectively new, i.e. any code is not equivalent to a non-linear code constructed by Otal and Özbudak.

3 The geometric setting

Let $\mathbb{E} = \operatorname{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ be the vector space of all endomorphisms of \mathbb{F}_{q^n} seen as a vector space over the field \mathbb{F}_q . As any element of \mathbb{E} corresponds 1-to-1 to a linearized polynomial $\alpha = \sum_{i=0}^{n-1} \alpha_i X^{\sigma^i} \in \tilde{\mathcal{L}}_{n,q,\sigma}$, we will define rank of the polynomial α as the dimension over \mathbb{F}_q of $\operatorname{im} \alpha(x)$, where $\alpha(x)$ is the map $x \in \mathbb{F}_{q^n} \mapsto \sum_{i=0}^{n-1} \alpha_i x^{\sigma^i} \in \mathbb{F}_{q^n}$, in symbol $\operatorname{rk} \alpha = \dim_{\mathbb{F}_q} \operatorname{im} \alpha(x)$. Also, the \mathbb{F}_q -linear map $\alpha(x)$ has rank r if and only if the $\operatorname{Dickson\ matrix}$

$$D_{\alpha} = \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \\ \alpha_{n-1}^{\sigma} & \alpha_0^{\sigma} & \dots & \alpha_{n-2}^{\sigma} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{\sigma^{n-1}} & \alpha_2^{\sigma^{n-1}} & \dots & \alpha_0^{\sigma^{n-1}} \end{pmatrix}$$

has rank r, see for more details [17, Chapter 3].

Let V be a v-dimensional vector space over the field \mathbb{F}_{q^n} and let $\operatorname{PG}(v-1,q^n) = \operatorname{PG}(V,\mathbb{F}_{q^n})$. A set Θ of points of $\operatorname{PG}(v-1,q^n)$ is an \mathbb{F}_q -linear set if each point is defined by a non-zero vector of an \mathbb{F}_q -linear vector space $U \subset V$, in symbol

$$\Theta = \left\{ \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} \colon \mathbf{u} \in U, \mathbf{u} \neq \mathbf{0} \right\}.$$

If $\dim_{\mathbb{F}_q} U = u$, we say that Θ has $rank\ u$. The size of Θ can be at most $\frac{q^u-1}{q-1}$ and if it is attained, Θ is said to be scattered. If u = v and $\langle \Theta \rangle = \operatorname{PG}(v-1,q^n)$, then Θ is a (canonical) subgeometry of $\operatorname{PG}(v-1,q^n)$. It follows that Θ is a canonical subgeometry if and only if any of its frame is also a frame of $\operatorname{PG}(v-1,q^n)$.

Let $\Sigma \cong \operatorname{PG}(n-1,q)$ be a canonical subgeometry of $\operatorname{PG}(n-1,q^n)$ and let $\hat{\sigma}$ be a generator of the subgroup of $\operatorname{PFL}(n,q^n)$ whose elements fixing pointwise Σ . Let $\overline{S} = \operatorname{PG}(W,q^n)$ be a subspace of $\operatorname{PG}(n-1,q^n)$. The integer $\dim_{\mathbb{F}_{q^n}} W = w$ will be called the rank of \overline{S} . Then $S = \overline{S} \cap \Sigma$ is a subspace of Σ of rank at most w. We will say that \overline{S} is a $\operatorname{subspace}$ of Σ if S and \overline{S} have the same rank. In particular, this holds if and only if \overline{S} is fixed by the collineation $\hat{\sigma}$ (see e.g. [19]). Any point

P of $PG(n-1,q^n)$ defines the subspace

$$L_{P,\hat{\sigma}} = \langle P, P^{\hat{\sigma}}, \dots, P^{\hat{\sigma}^{n-1}} \rangle.$$

If the collineation $\hat{\sigma}$ is clear from the context, we will indicate $L_{P,\hat{\sigma}}$ simply by L_P . Note that L_P has rank at most n and it is fixed by $\hat{\sigma}$, and so L_P is a subspace of Σ . Denote by $(X_0, X_1, \ldots, X_{n-1})$ the homogeneous projective coordinates of $\mathrm{PG}(n-1,q^n)$ and let $P(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})$ be a point of $\mathrm{PG}(n-1,q^n)$. It will be of type r with respect to Σ if L_P has rank r. In particular, if $\hat{\sigma}$ is the collineation of $\mathrm{PG}(n-1,q^n)$ defined by

$$(X_0, X_1, \dots, X_{n-1})^{\hat{\sigma}} = (X_{n-1}^{\sigma}, X_0^{\sigma}, \dots, X_{n-2}^{\sigma}).$$

Then, the collineation $\hat{\sigma}$ fixes pointwise the canonical subgeometry

$$\Sigma_{n,n} = \{(x, x^{\sigma}, \dots, x^{\sigma^{n-1}}) : x \in \mathbb{F}_{q^n}^*\} \cong \mathrm{PG}(n-1, q). \tag{4}$$

and the point $P(\alpha_0, \alpha_1, \dots, \alpha_{n-1})$ is of type r with respect to $\Sigma_{n,n}$ if and only $\alpha = \sum_{i=0}^{n-1} \alpha_i X^{\sigma^i}$ has rank r, or also the Dickson matrix D_{α} has rank r.

Let $\operatorname{PG}(\mathbb{F}_q^{m\times n}, \mathbb{F}_q) = \operatorname{PG}(mn-1, q), \ m \leq n$, and let $\mathcal{S}_{m,n}$ be the Segre variety of $\operatorname{PG}(\mathbb{F}_q^{m\times n}, \mathbb{F}_q)$, i.e., $\mathcal{S}_{m,n}$ is the set of all points $\langle A \rangle_{\mathbb{F}_q}$ in $\operatorname{PG}(\mathbb{F}_q^{m\times n}, \mathbb{F}_q)$ such that $\operatorname{rk} A = 1$, see [14, Section 4.5]. This can be seen as the \mathbb{F}_q -field reduction of the set of points

$$\Sigma_{m,n} = \{(x, x^{\sigma}, \dots, x^{\sigma^{m-1}}) \colon x \in \mathbb{F}_{q^n}^*\} \cong \mathrm{PG}(n-1, q)$$

of $PG(m-1,q^n)$ in PG(mn-1,q), see [16, Section 2.2].

Let \mathcal{A} be a subset of $\operatorname{PG}(n-1,q)$ and denote by $\Omega_h(\mathcal{A})$ the h-secant variety of \mathcal{A} , i.e. the union of the ℓ -dimensional projective subspaces spanned by points of \mathcal{A} for any $0 \leq \ell \leq h$, [13]. Note that $\Omega_0(\mathcal{A}) = \mathcal{A}$ and for any $1 \leq h \leq n-1$, $\Omega_{h-1}(\mathcal{A}) \subseteq \Omega_h(\mathcal{A})$. Moreover, if $\mathcal{A} \subset \operatorname{PG}(n-1,q)$ such that $\langle \mathcal{A} \rangle = \operatorname{PG}(t-1,q) \subset \operatorname{PG}(n-1,q)$, then $\Omega_h(\mathcal{A}) = \Omega_{t-1}(\mathcal{A})$ for any $t \leq h \leq n-1$. A set of points $\mathcal{E} \subset \operatorname{PG}(n-1,q)$ is called an exterior set with respect to $\Omega_h(\mathcal{A})$ if any line joining two points of \mathcal{E} is disjoint from $\Omega_h(\mathcal{A})$. The following theorem proves an upper bound for the size of an exterior set.

Theorem 3.1. Let $A \subset PG(n-1,q)$ such that $\langle A \rangle = PG(n-1,q)$. Let $\mathcal{E} \subset PG(n-1,q)$ be an exterior set with respect to $\Omega_h(A)$, $0 \leq h \leq n-1$. Then

$$|\mathcal{E}| \le \frac{q^{n-h-1}-1}{q-1}.$$

Proof. Firstly, we may assume $h \leq n-3$. Indeed, if $h \in \{n-2, n-1\}$ the claim is trivially satisfied: if h = n-1, then $\Omega_{n-1}(\mathcal{A}) = \operatorname{PG}(n-1,q)$ and $\mathcal{E} = \emptyset$; if h = n-2, then $\Omega_{n-2}(\mathcal{A})$ contains hyperplanes and $|\mathcal{E}| \leq 1$.

Now, let $h \leq n-3$ and let S_h be an h-dimensional subspace contained in $\Omega_h(\mathcal{A})$. The number of (h+1)-dimensional projective subspaces of $\operatorname{PG}(n-1,q)$ containing S_h equals the number of points of an (n-h-2)-dimensional projective subspace of $\operatorname{PG}(n-1,q)$. Since \mathcal{E} is an exterior set, then it meets any (h+1)-dimensional projective subspace containing S_h in at most one point. This proves the claim. \square

Given M, N two sets of points of PG(n-1,q), with $M \cap N = \emptyset$, we will denote by $\mathcal{K}(M,N)$ the *cone with vertex* M *and base* N, i.e. $\mathcal{K}(M,N)$ is the set of all points belonging to a line joining a point of M and a point of N.

Let suppose that M, N are two disjoint subsets of $\operatorname{PG}(n-1,q)$ such that $\langle M \rangle$ and $\langle N \rangle$ are disjoint subspaces having rank at least 2. Let P,Q be two distinct points in M and P',Q' be two distinct points in N. It is straightforward to show that the lines PP' and QQ' are disjoint. Indeed, if $PP' \cap QQ' \neq \emptyset$ then the plane spanned by PP' and QQ' meets the subspace $\langle M \rangle$ in the line PQ and the subspace $\langle N \rangle$ in the line P'Q', a contradiction. Then, it follows that

$$|\mathcal{K}(M, N)| = |M| + |N| + (q - 1) \cdot |M| \cdot |N|.$$

If the subspaces $\langle M \rangle$ and $\langle N \rangle$ of PG(n-1,q) are not disjoint, then the lines PP' and QQ' can be incident and, clearly,

$$|\mathcal{K}(M, N)| \le |M| + |N| + (q - 1) \cdot |M| \cdot |N|.$$

Corollary 3.2. Let $A \subset PG(n-1,q)$ such that $\langle A \rangle = PG(t-1,q)$, $1 \leq t < n$, and let $\mathcal{E} \subset PG(n-1,q)$ be an exterior set with respect to $\Omega_h(A)$, $0 \leq h \leq n-1$. Then \mathcal{E} is contained in a cone $K = K(S_{n-t-1}, \bar{\mathcal{E}})$, with base $\bar{\mathcal{E}} = \mathcal{E} \cap \langle A \rangle$ and vertex an (n-t-1)-dimensional subspace S_{n-t-1} complementary with $\langle A \rangle$. Moreover,

$$|\mathcal{E}| \le \begin{cases} \frac{q^{n-h-1}-1}{q-1} & \text{if } 0 \le h \le t-1, \\ \frac{q^{n-t}-1}{q-1} & \text{otherwise.} \end{cases}$$
 (5)

Proof. Let suppose $0 \le h \le t - 1$. Clearly, if $\bar{\mathcal{E}} \subset \langle \mathcal{A} \rangle$ is an exterior set with respect to $\Omega_h(\mathcal{A}) \subseteq \langle \mathcal{A} \rangle$, $0 \le h \le t - 1$, by Theorem 3.1,

$$|\bar{\mathcal{E}}| \le \frac{q^{t-h-1} - 1}{q-1}.$$

Let S_{n-t-1} be an (n-t-1)-dimensional subspace of $\operatorname{PG}(n-1,q)$ complementary

with $\langle \mathcal{A} \rangle$. Then,

$$|\mathcal{K}(S_{n-t-1}, \bar{\mathcal{E}})| = |\bar{\mathcal{E}}| \cdot |S_{n-t-1}| \cdot (q-1) + |\bar{\mathcal{E}}| + |S_{n-t-1}|$$

$$\leq \frac{q^{t-h-1} - 1}{q-1} \cdot \frac{q^{n-t} - 1}{q-1} \cdot (q-1) + \frac{q^{t-h-1} - 1}{q-1} + \frac{q^{n-t} - 1}{q-1}$$

$$= \frac{q^{n-h-1} - 1}{q-1}.$$

If $t \leq h \leq n-1$, since $\Omega_h(\mathcal{A}) = \Omega_{t-1}(\mathcal{A})$ and any exterior set contained in $\langle \mathcal{A} \rangle$ with respect $\Omega_h(\mathcal{A})$ is the empty set, the claim follows.

An exterior set $\mathcal{E} \subset \operatorname{PG}(n-1,q)$ with respect to $\Omega_h(\mathcal{A})$, $\langle \mathcal{A} \rangle = \operatorname{PG}(t-1,q)$, $1 \leq h+1 \leq t \leq n$, is called maximum if its size $|\mathcal{E}| = \frac{q^{n-h-1}-1}{q-1}$. Note that the image of $\Omega_h(\Sigma_{m,n}) \subset \operatorname{PG}(m-1,q^n)$ under the \mathbb{F}_q -field reduction is the h-secant variety $\Omega_h(\mathcal{S}_{m,n})$ of the points whose the representative matrices in $\mathbb{F}_q^{m \times n}$ have rank at most h+1. The (maximum) exterior sets with respect to $\Omega_h(\Sigma_{m,n})$ are related to (maximum) rank distance codes. More precisely,

Theorem 3.3. Let \mathcal{E} be an exterior set with respect to $\Omega_h(\Sigma_{m,n})$ of $PG(m-1,q^n)$ and denote by \mathcal{E}' the image of \mathcal{E} under the \mathbb{F}_q -field reduction. Then, the set

$$C = \{ \rho M : \langle M \rangle_{\mathbb{F}_q} \in \mathcal{E}', \rho \in \mathbb{F}_q \}$$
 (6)

is an (m, n, q; h + 2)-RD code closed under \mathbb{F}_q -multiplication. In addition, if \mathcal{E} is maximum then \mathcal{C} is an MRD.

Note that the (m, n, q; h+2)-RD codes closed under \mathbb{F}_q -multiplication and the exterior sets with respect to $\Omega_h(\mathcal{S}_{m,n})$ of PG(mn-1,q) are in 1-to-1 correspondence. Since the pre-image under the field reduction of one of these sets may not be an exterior set of PG $(m-1,q^n)$ with respect to $\Omega_h(\Sigma_{m,n})$, then there exist rank distance codes that don't arise from exterior sets with respect to $\Omega_h(\Sigma_{m,n})$ of PG $(m-1,q^n)$. See [2, 3, 8] and the references therein for more details on exterior sets.

4 Non-linear MRD codes arising from C_F^{σ} -set

In [8], Donati and Durante exhibited a class of non-linear MRD codes with parameters (d+1, n, q; d) with q > 2, $n \ge 3$ and $0 \le d \le n-1$ by means of a family of maximum exterior sets with respect the (d-1)-secant variety of a subgeometry isomorphic to PG(d, q) in $\Sigma_{d+1,n}$. Now, we recall briefly their construction. So, let $PG(d, q^n)$ be a d-dimensional projective space and consider A and A two distinct points of $PG(d, q^n)$, A and A be the stars of lines (pencils of lines if A = 2)

through A and B, respectively. Let σ be the Frobenius automorphism of \mathbb{F}_{q^n} defined by $x \mapsto x^{q^s}$ with $\gcd(n,s) = 1$ and consider Φ a σ -collineation between \mathcal{S}_A and \mathcal{S}_B which does not map the line AB into itself and such that the subspace spanned by the lines $\Phi^{-1}(AB)$, AB, $\Phi(AB)$ has dimension $\min\{3,d\}$. The set \mathcal{X} of points of intersection of corresponding lines under the collineation Φ is called C_F^{σ} -set of $\mathrm{PG}(d,q^n)$ and the points A and B are called the vertices of \mathcal{X} , see [7, 8]. There, it is proved that every C_F^{σ} -set \mathcal{X} of $\mathrm{PG}(d,q^n)$ with vertices A and B is the union of $\{A,B\}$ and q-1 pairwise disjoint subsets, called the components of \mathcal{X} , each of which is a scattered \mathbb{F}_q -linear set of rank n. For more details on linear sets, see e.g. [28].

Let $N_a = \{y \in \mathbb{F}_{q^n} : N_{q^n/q}(y) = a\}$ for any $a \in \mathbb{F}_q^*$. Without loss of generality, we may assume that $A = (0, \dots, 0, 1)$ and $B = (1, 0, \dots, 0)$ and then the sets

$$\mathcal{X}_a = \left\{ (1, t, t^{\sigma+1}, \dots, t^{\sigma^{d-1} + \dots + \sigma + 1}) : t \in N_a \right\},\,$$

with $a \in \mathbb{F}_q^*$, are the components of \mathcal{X} . Since every \mathcal{X}_a has $(q^n - 1)/(q - 1)$ points, then \mathcal{X} has $q^n + 1$ points. In particular, every \mathcal{X}_a is isomorphic to $\mathrm{PG}(n-1,q)$, see [8, Remark 3.5]. For any $a \in \mathbb{F}_q^*$, the line AB of $\mathrm{PG}(d,q^n)$ is partitioned into $\{A,B\}$ and the q-1 sets

$$J_a = \{(1, 0, \dots, 0, (-1)^{d+1}t) : t \in N_a\},\$$

each of which is a scattered \mathbb{F}_q -linear set (of pseudoregulus type with transversal points A and B), see [7, Remark 2.2] and [21]. Note that $\mathcal{X}_1 = \Sigma_{d+1,n}$ and let Π be a subgeometry of $\Sigma_{d+1,n}$ isomorphic to $\mathrm{PG}(d,q)$. Then for any $T \subseteq \mathbb{F}_q^*$, $1 \in T$, the set

$$\mathcal{E} = \left(\mathcal{X} \setminus \bigcup_{a \in T} \mathcal{X}_a \right) \cup \bigcup_{a \in T} J_a$$

is a maximum exterior set with respect to $\Omega_{d-2}(\Pi)$, see [8, Theorem 5.1]. Hence, the set \mathcal{E} corresponds a (d+1, n, q; d)-MRD code.

5 Embeddings and cones over exterior sets

Let $\Sigma \cong \operatorname{PG}(n-1,q)$ be a canonical subgeometry of $\operatorname{PG}(n-1,q^n)$ and consider a subspace Λ^* of rank k disjoint from Σ and Λ a subspace of $\operatorname{PG}(n-1,q^n)$ of rank n-k disjoint from Λ^* . Let Γ be the projection of Σ from Λ^* to Λ , i.e.,

$$\Gamma = \mathbf{p}_{\Lambda^\star,\Lambda}(\Sigma) = \left\{ \langle \Lambda^\star, P \rangle \cap \Lambda : P \in \Sigma \right\}.$$

We recall the following definition given in [20].

Definition 5.1. Let $\Gamma = p_{\Lambda^*,\Lambda}(\Sigma)$ be an \mathbb{F}_q -linear set of rank n. It is called (n-k-1)-embedding of Σ if any subspace of Σ of rank n-k is disjoint from Λ^* .

Note that $\Gamma = \mathbf{p}_{\Lambda^*,\Lambda}(\Sigma)$ is an (n-k-1)-embedding if and only if for any choice of n-k independent points $R_1, R_2, \ldots, R_{n-k}$ of Σ ,

$$\Lambda = \langle R'_1, R'_2, \dots, R'_{n-k} \rangle$$

where $R'_i = p_{\Lambda^*,\Lambda}(R_i)$, i = 1, 2, ..., n - k, also this is equivalent to say that

$$p_{\Lambda^{\star},\Lambda}: P \in \Sigma \longrightarrow \langle P, \Lambda^{\star} \rangle \cap \Lambda \in \Lambda$$

induces an injective map from the set of all subspaces of Σ of rank $\ell \leq n-k-1$ to the set of all subspaces of Λ of the same rank ℓ and, hence, if $R \in \Omega_{n-k-1}(\Sigma)$ then $\langle R, \Lambda^* \rangle \cap \Lambda \in \Omega_{n-k-1}(\Gamma)$.

Remark 5.2. If $\Gamma = \mathrm{p}_{\Lambda^*,\Lambda}(\Sigma)$ is an (n-k-1)-embedding of Σ , it is not true that $\Omega_{n-k-1}(\Gamma) \not\subseteq \Omega_{n-k-1}(\Sigma) \cap \Lambda$. For instance, let

$$\Sigma_{5,5} = \{(x, x^{\sigma}, x^{\sigma^2}, x^{\sigma^3}, x^{\sigma^4}) : x \in \mathbb{F}_{q^5}^*\}$$

be a fixed canonical subgeometry of PG(4, q^5) and let $\Lambda^{\star}(0,0,0,0,1)$ and $\Lambda: X_4=0$ be a point and a hyperplane of PG(4, q^5), respectively. Clearly, $\Omega_1(\Sigma)$ and $\Omega_1(\Gamma)$ contains lines joining two distinct points of Γ and Σ , respectively. If $\Omega_1(\Sigma) \cap \Lambda$ containes a line then it would contain two points of Σ . Since Λ and Σ are disjoint, we get a contradiction.

Lemma 5.3. [20, Theorem 6] The \mathbb{F}_q -linear set $\Gamma = p_{\Lambda^*,\Lambda}(\Sigma)$ is an (n-k-1)-embedding of Σ if and only if any point $P \in \Lambda^*$ is of type $\geq n-k+1$.

Proof. By definition Γ is an (n-k-1)-embedding if and only if Λ^* is disjoint from any subspace of Σ of rank n-k. This is equivalent to saying that for any point P of Λ^* the subspace L_P has rank at least n-k+1, i.e. the point P is of type at least n-k+1.

In [20], in order to get a linear MRD-code, a geometric property for the cone having vertex Λ^* and base a linear set of rank n has been shown. More precisely,

Theorem 5.4. [20, Theorem 5] Let $\Sigma \cong PG(n-1,q)$ be a canonical subgeometry of $PG(n-1,q^n)$ and let Λ^* and Λ be subspaces of $PG(n-1,q^n)$ of rank k and n-k, respectively, such that $\Lambda^* \cap \Sigma = \emptyset = \Lambda^* \cap \Lambda$.

Let $\Gamma = p_{\Lambda^*,\Lambda}(\Sigma)$ be an (n-k-1)-embedding of Σ and let $\Theta \subset \Lambda$ be an \mathbb{F}_q -linear set of rank n. If no points of Θ belong to a subspace spanned by at most n-k points of Γ , then any point of $K = K(\Lambda^*, \Theta)$ is of type $\geq n-k+1$.

Moreover, if $\Sigma = \Sigma_{n,n}$ as in (4), the set $C = \left\{ \sum_{i=0}^{n-1} \alpha_i X^{\sigma^i} : (\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in \mathcal{K} \right\}$ is a linear MRD-code with minimum distance d = n - k + 1.

Here, we shall adapt the result above to the case of cone such that its base is not necessarily a linear set.

Theorem 5.5. Let $\Sigma \cong \operatorname{PG}(n-1,q)$ be a canonical subgeometry of $\operatorname{PG}(n-1,q^n)$ and let Λ^* and Λ be subspaces of $\operatorname{PG}(n-1,q^n)$ of rank k-2 and n-k+2, respectively, such that $\Lambda^* \cap \Sigma = \emptyset = \Lambda^* \cap \Lambda$. Let $\Gamma = \operatorname{p}_{\Lambda^*,\Lambda}(\Sigma)$ be an (n-k+1)-embedding of Σ and let \mathcal{E} be a (maximum) exterior set with respect to $\Omega_{n-k-1}(\Gamma)$. Then, $\mathcal{K} = \mathcal{K}(\Lambda^*, \mathcal{E})$ is a (maximum) exterior set with respect to $\Omega_{n-k-1}(\Sigma)$.

Proof. Let P,Q be two points in $\mathcal{K}=\mathcal{K}(\Lambda^{\star},\mathcal{E})$. We shall distinguish some cases:

- $P, Q \in \Lambda^*$. Since Γ is an (n k + 1)-embedding the line PQ is disjoint from the subspaces of rank (n k) of Σ and so from $\Omega_{n-k-1}(\Sigma)$.
- $P, Q \in \mathcal{E}$. Suppose that the line PQ meets a subspace S of Σ of rank (n-k) and consider

$$\emptyset \neq \langle \Lambda^*, S \cap PQ \rangle \cap \Lambda \subseteq \langle \Lambda^*, S \rangle \cap \Lambda \cap PQ. \tag{7}$$

This is a contradiction by the hypothesis done over \mathcal{E} and since $\langle \Lambda^*, S \rangle \cap \Lambda$ is a subspace of rank n - k.

- the line $PQ \subseteq \mathcal{K} \setminus (\Lambda^* \cup \mathcal{E})$ and joins a point of Λ^* and a point of \mathcal{E} . Then, without loss of generality, we may suppose that $P \in \Lambda^*$ and $Q \in \mathcal{E}$. If the line PQ meets a subspace S of Σ of rank (n-k), then

$$Q \in \langle \Lambda^*, S \cap PQ \rangle \cap \Lambda \subseteq \langle \Lambda^*, S \rangle \cap \Lambda. \tag{8}$$

Then Q belongs to a space spanned by points of Γ with rank (n-k), a contradiction.

- the line $PQ \subseteq \mathcal{K} \setminus (\Lambda^* \cup \mathcal{E})$ and does not joint a point of Λ^* and a point of \mathcal{E} or $PQ \not\subseteq \mathcal{K}$. If PQ meets a subspace S of Σ of rank (n-k), then

$$\emptyset \neq \langle \Lambda^*, S \cap PQ \rangle \cap \Lambda \subseteq \langle \Lambda^*, S \rangle \cap \langle \Lambda^*, PQ \rangle \cap \Lambda. \tag{9}$$

Since the projection from Λ^* to Λ of the line PQ is a line through two points P', Q' of \mathcal{E} , we get that this line meets the space $\langle \Lambda^*, S \rangle \cap \Lambda$ spanned by (n-k) points of Γ , a contradiction.

Then we have showed that any line through two points of \mathcal{K} is disjoint from $\Omega_{n-k-1}(\Sigma)$. Now, since $\langle \Gamma \rangle = \Lambda$, if \mathcal{E} is a maximum exterior set with respect to

$$\Omega_{n-k-1}(\Gamma)$$
, we get

$$\begin{split} |\mathcal{K}(\Lambda^{\star},\mathcal{E})| &= |\Lambda^{\star}| + |\mathcal{E}| + |\Lambda^{\star}||\mathcal{E}|(q^{n} - 1) \\ &= \frac{q^{n(k-2)} - 1}{q^{n} - 1} + \frac{q^{2n} - 1}{q^{n} - 1} + \frac{q^{n(k-2)} - 1}{q^{n} - 1} \cdot \frac{q^{2n} - 1}{q^{n} - 1} (q^{n} - 1) \\ &= \frac{q^{2n} - 1}{q^{n} - 1} + \frac{q^{n(k-2)} - 1}{q^{n} - 1} q^{2n} \\ &= \frac{q^{nk} - 1}{q^{n} - 1}. \end{split}$$

In the same setting of theorem above, it seems that if $\mathcal{K}(\Lambda^*, \mathcal{E})$ is an exterior set with respect to $\Omega_{n-k-1}(\Sigma)$ where \mathcal{E} is a subset contained in Λ , then \mathcal{E} may not be an exterior set with respect $\Omega_{n-k-1}(\Gamma)$. If $\Omega_{n-k-1}(\Sigma) \cap \Lambda = \Omega_{n-k-1}(\Gamma)$, this turns to be true. Indeed, if $A, B \in \mathcal{E}$ and there exists $P \in AB \cap \Omega_{n-k-1}(\Gamma)$, then $P \in AB \cap \Omega_{n-k-1}(\Sigma)$, a contradiction.

6 The class of non-linear MRD codes $C_{\sigma,T}$

In this section, as application of Theorem 5.5, by a suitable choice of Λ^* , Λ , an (n-k+1)-embedding Γ of $\Sigma = \Sigma_{n,n}$, $2 \le k \le n-1$, and a maximum exterior set with respect to $\Omega_{n-k-1}(\Gamma)$ in $\mathrm{PG}(n-1,q^n)$, we will get a class of non-linear MRD codes in $\tilde{\mathcal{L}}_{n,q,\sigma}$. Precisely, let

$$\Lambda^{\star}: X_0 = X_1 = \ldots = X_{n-k+1} = 0$$

and

$$\Lambda: X_{n-k+2} = X_{n-k+3} = \ldots = X_{n-1} = 0$$

be disjoint subspaces of rank (k-2) and (n-k+2) in $PG(n-1,q^n)$, respectively. Consider the linear set of rank n

$$\Gamma = p_{\Lambda^*, \Lambda}(\Sigma) = \{ (x, x^{\sigma}, \dots, x^{\sigma^{n-k+1}}, 0, \dots, 0) : x \in \mathbb{F}_{q^n}^* \}$$
 (10)

where Σ is the canonical geometry as in (4) and let $P = (0, \ldots, 0, \beta_{n-k+2}, \ldots, \beta_{n-1}) \in \Lambda^*$. This is a point of type at least n - k + 3. Indeed, the linearized polynomial

$$\beta = \beta_{n-k+2} X^{\sigma^{n-k+2}} + \ldots + \beta_{n-1} X^{\sigma^{n-1}}$$

has rank at least n-k+3 because the polynomial $\beta \circ X^{\sigma^{k-2}} = \beta_{n-k}X + \ldots + \beta_{n-1}X^{\sigma^{k-3}}$ has at most q^{k-3} roots and $\operatorname{rk}(\beta \circ X^{\sigma^{k-2}}) = \operatorname{rk}\beta$. So, by Lemma 5.3, we get that Γ is an (n-k+1)-embedding of Σ . Finally, let

$$A = (\underbrace{0, \dots, 0}_{n-k+1}, 1, 0, \dots, 0)$$
 and $B = (1, 0, \dots, 0)$

be points in Λ and consider

$$\mathcal{X} = \bigcup_{a \in \mathbb{F}_q^*} \mathcal{X}_a \cup \{A, B\},\,$$

where

$$\mathcal{X}_a = \left\{ (1, t, t^{\sigma+1}, \dots, t^{\sigma^{n-k} + \dots + \sigma + 1}, 0, \dots, 0) : t \in N_a \right\}.$$

The set \mathcal{X} is the C_F^{σ} -set with vertices A and B generated by a σ -collineation Φ between the star of lines through A and B contained in Λ . Let $T \subseteq \mathbb{F}_q^*$, $1 \in T$, then the set

$$\mathcal{E} = \left(\mathcal{X} \setminus \bigcup_{a \in T} \mathcal{X}_a \right) \cup \bigcup_{a \in T} J_a \tag{11}$$

with

$$J_a = \left\{ (1, \underbrace{0, \dots, 0}_{n-k}, (-1)^{n-k}t, 0, \dots, 0) : t \in N_a \right\}, \quad a \in \mathbb{F}_q^*.$$

is a maximum exterior set with respect to $\Omega_{n-k-1}(\Gamma)$ as proved in [8, Theorem 5.1] of size $q^n + 1$. Therefore, the hypothesis of Theorem 5.5 are satisfied and the cone $\mathcal{K}(\Lambda^*, \mathcal{E})$ is a maximum exterior set with respect to $\Omega_{n-k-1}(\Sigma)$ and by Theorem 3.3, the set $\mathcal{C}_{\sigma,T} \subset \mathbb{F}_q^{n \times n}$, as in (6), is a non-linear MRD code with minimum distance d = n - k + 1 which cannot be a translated version of an additive code.

d = n - k + 1 which cannot be a translated version of an additive code. Note that the punctured code $C_{\sigma,T}^{[k-2]} \subset \mathbb{F}_q^{(n-k+2)\times n}$ obtained from $C_{\sigma,T}$ by deleting the last (k-2) rows is exactly the code constructed in [8, Theorem 5.1], while for k=2 the code appeared in [9] and for n=3, k=2 in [2].

By Theorem 3.3 and Theorem 5.5, the $C_{\sigma,T}$ is a subset of square matrices of order n and so, it can be seen as a subset of $\tilde{\mathcal{L}}_{n,q,\sigma}$. Indeed, fixing $T \subseteq \mathbb{F}_q^*$, $1 \in T$, the homogeneous coordinates of the points belonging to \mathcal{E} have one of the following forms

$$(\alpha, \alpha^{\sigma} \xi, \alpha^{\sigma^{2}} \xi^{\sigma+1}, \dots, \alpha^{\sigma^{n-k+1}} \xi^{\sigma^{n-k} + \dots + 1}, 0, \dots, 0)$$

$$(\alpha, \underbrace{0, \dots, 0}_{n-k}, (-1)^{n-k} \alpha^{\sigma} \eta, 0, \dots, 0)$$

$$A = \underbrace{(0, \dots, 0}_{n-k+1}, \alpha, 0, \dots, 0) \text{ and } B = (\alpha, 0, \dots, 0)$$

$$(12)$$

with $N_{q^n/q}(\xi) \in \mathbb{F}_q^* \setminus T$ and $N_{q^n/q}(\eta) \in T$. So the non-linear (n, n, q; d), d = n - k + 1, MRD code $\mathcal{C}_{\sigma,T}$ is the set of σ -linearized polynomials with σ -degree at most n-1 whose coefficients are the homogeneous coordinates of a point in $\mathcal{K}(\Lambda^*, \mathcal{E})$ together with the zero map, i.e.

$$\mathcal{C}_{\sigma,T} = \left\{ \sum_{i=0}^{n-k+1} \lambda \alpha^{\sigma^{i}} \xi^{\frac{\sigma^{i}-1}{\sigma-1}} X^{\sigma^{i}} + \sum_{i=n-k+2}^{n-1} \beta_{i} X^{\sigma^{i}} : \lambda, \alpha, \beta_{i} \in \mathbb{F}_{q^{n}}, N_{q^{n}/q}(\xi) \in \mathbb{F}_{q}^{*} \setminus T \right\} \\
\cup \left\{ \lambda \alpha X + (-1)^{n-k+2} \lambda \alpha^{\sigma} \eta X^{\sigma^{n-k+1}} + \sum_{i=n-k+2}^{n-1} \beta_{i} X^{\sigma^{i}} : \lambda, \alpha, \beta_{i} \in \mathbb{F}_{q^{n}}, N_{q^{n}/q}(\eta) \in T \right\} \\
\cup \left\{ \alpha X^{\sigma^{n-k+1}} + \sum_{i=n-k+2}^{n-1} \beta_{i} X^{\sigma^{i}} : \alpha, \beta_{i} \in \mathbb{F}_{q^{n}} \right\} \cup \left\{ \alpha X + \sum_{i=n-k+2}^{n-1} \beta_{i} X^{\sigma^{i}} : \alpha, \beta_{i} \in \mathbb{F}_{q^{n}} \right\}. \tag{13}$$

7 The equivalence issue for $C_{\sigma,T}$

Finally, in order to state the novelty of the class of non-linear codes obtained, we have to compare a code of type $\mathcal{C}_{\sigma,T}$, $1 \in T \subseteq \mathbb{F}_q^*$, with the only known non-linear MRD codes made up of square matrices: the codes of type $\mathcal{C}_{n,k,\sigma,I}$ with $I \subseteq \mathbb{F}_q$, cf. (3).

It easy straightforward to see that the code $C_{\sigma,T}$ in (13) is closed under \mathbb{F}_{q^n} -multiplication and hence under \mathbb{F}_q -multiplication. While, the code $C_{n,k,\sigma,I}$ in (3), if q > 2 and $I \notin \{\emptyset, \{0\}, \mathbb{F}_q^*, \mathbb{F}_q\}$ is not closed under \mathbb{F}_q -multiplication. Therefore, by Theorem 3.3, $C_{n,k,\sigma,I}$ cannot arise from an exterior set \mathcal{E}' of $\mathrm{PG}(n^2-1,q)$ with respect to the secant variety $\Omega_{n-k-1}(\mathcal{S}_{n,n})$. Moreover, the property of being closed under \mathbb{F}_q -multiplication is not preserved under equivalence between two non-linear MRD codes, and then it cannot be used as an argument to state that these codes are not equivalent.

So, in this section we will investigate their equivalence issue. Firstly, note that the sets

$$\mathcal{U} = \left\{ \alpha X^{\sigma^{n-k+1}} + \sum_{i=n-k+2}^{n-1} \beta_i X^{\sigma^i} : \alpha, \beta_i \in \mathbb{F}_{q^n} \right\} = \left\{ f \circ X^{\sigma^{n-k+1}} : f \in \mathcal{G}_{k-1,\sigma} \right\}$$

$$\tag{14}$$

and

$$\mathcal{V} = \left\{ \alpha X + \sum_{i=n-k+2}^{n-1} \beta_i X^{\sigma^i} : \alpha, \beta_i \in \mathbb{F}_{q^n} \right\} = \left\{ f \circ X^{\sigma^{n-k+2}} : f \in \mathcal{G}_{k-1,\sigma} \right\}, \quad (15)$$

contained in $C_{\sigma,T}$, are equivalent to a generalized Gabidulin code $G_{k-1,\sigma}$ and their intersection

$$\left\{ \sum_{i=d+1}^{n-1} \beta_i X^{\sigma^i} : \beta_i \in \mathbb{F}_{q^n} \right\} = \left\{ f \circ X^{\sigma^{n-k+2}} : f \in \mathcal{G}_{k-2,\sigma} \right\}$$

is equivalent to a generalized Gabidulin code $\mathcal{G}_{k-2,\sigma}$. While the non-linear (n,n,q;n-1)k+1)-MRD code $C_{n,k,\sigma,I} = C_{n,k,\sigma,I}^{(1)} \cup C_{n,k,\sigma,I}^{(2)}$, introduced in Subsection 2.3., contains the set

$$\left\{ \sum_{i=1}^{k-1} \gamma_i X^{\sigma^i} : \gamma_i \in \mathbb{F}_{q^n} \right\} = \left\{ f \circ X^{\sigma} : f \in \mathcal{G}_{k-1,\sigma} \right\},\,$$

which is equivalent to a generalized Gabidulin code $\mathcal{G}_{k-1,\sigma}$ and it is straightforward to see that $\mathcal{C}_{n,k,\sigma,I}$ is contained in a generalized Gabidulin code $\mathcal{G}_{k+1,\sigma}$.

Clearly, if q=2 or $T=\mathbb{F}_q^*$, $\mathcal{C}_{\sigma,T}$ is equivalent to the generalized Gabidulin code $\mathcal{G}_{k,\sigma}$. Then, by [27, Corollary 2.1], it follows

Theorem 7.1. Let $I \subseteq \mathbb{F}_q$, $1 \in T \subseteq \mathbb{F}_q^*$ and σ be a generator of $Gal(\mathbb{F}_{q^n}|\mathbb{F}_q)$. If $q=2 \text{ or } T=\mathbb{F}_q^* \text{ and } I\in\{\emptyset,\{0\},\mathbb{F}_q^*,\mathbb{F}_q\}^{q}, \text{ then the codes } \mathcal{C}_{n,k,\sigma,I} \text{ and } \mathcal{C}_{\sigma,T} \text{ are both } \mathcal{C}_{\sigma,T} \text{ or } \mathcal{C}_{\sigma,T} \text{ are both } \mathcal{C}_{\sigma,T} \text{ or } \mathcal{C}_{$ equivalent to $\mathcal{G}_{k,\sigma}$.

In the remainder of this section, we shall show that apart from these cases, the codes $\mathcal{C}_{\sigma,T}$ and $\mathcal{C}_{n,k,\sigma,I}$ cannot be equivalent. In order to do this, we recall the following result that holds for the σ -linearized polynomials as well.

Theorem 7.2. [32, Theorem 3] A subspace W of $\mathcal{G}_{k,\sigma}$, $k \leq n-1$, is equivalent to $\mathcal{G}_{r,\sigma}$ if and only if there exist invertible linearized polynomials f,g such that

$$\mathcal{W} = \mathcal{G}_{r,\sigma}^{(f,g)} = \{ f \circ \alpha \circ g : \alpha \in \mathcal{G}_{r,\sigma} \},\,$$

where $f_0 = 1$ and $\deg_{\sigma}(f) + \deg_{\sigma}(g) \leq k - r$.

By a similar argument used in [32, Lemma 4] for the generalized twisted Gabidulin codes, we prove the following

Theorem 7.3. Let $I \notin \{\emptyset, \{0\}, \mathbb{F}_q^*, \mathbb{F}_q\}$, the non-linear (n, n, q; n - k + 1)-MRD code $C_{n,k,\sigma,I}$ contains a unique subspace equivalent to $G_{k-1,\sigma}$.

Proof. We have already noted that $\mathcal{C}_{n,k,\sigma,I}$ is contained in $\mathcal{G}_{k+1,\sigma}$. Now, let \mathcal{W} be a subspace of $\mathcal{C}_{n,k,\sigma,I}$ equivalent to $\mathcal{G}_{k-1,\sigma}$. By Theorem 7.2, there exist invertible σ -linearized polynomials f, g such that

$$\mathcal{W} = \mathcal{G}_{k-1,\sigma}^{(f,g)} = \{ f \circ \alpha \circ g : \alpha \in \mathcal{G}_{k-1,\sigma} \}$$

with $f_0 \neq 0$ and $\deg_{\sigma}(f) + \deg_{\sigma}(g) \leq 2$.

If $\deg_{\sigma}(f) = t$ then $\deg_{\sigma}(g) \leq 2 - t$. Let $\alpha = \sum_{i=0}^{k-2} \alpha_i X^{\sigma^i}$ be an element of $\mathcal{G}_{k-1,\sigma}$. Then the coefficient of X in the polynomial $f \circ \alpha \circ g$ is $f_0 \alpha_0 g_0$, while the coefficient of X^{σ^k} is $f_t \alpha_{k-2}^{\sigma^t} g_{2-t}^{\sigma^{k+t-2}}$. Since $\mathcal{C}_{n,k,\sigma,I}^{(1)}$ and $\mathcal{C}_{n,k,\sigma,I}^{(2)}$ are disjoint, first suppose that $\mathcal{W} \subset \mathcal{C}_{n,k,\sigma,I}^{(1)}$. Then, $N_{q^n/q}(f_0\alpha_0g_0) \in I$ and $f_t\alpha_{k-2}^{\sigma^t}g_{2-t}^{\sigma^{k+t-2}} = 0$ for any $\alpha_0, \alpha_{k-2} \in \mathbb{F}_{q^n}$. So, we distinguish three cases:

- 1. Suppose t = 2, then $\deg_{\sigma}(g) = 0$. Since $f_0, f_2 \neq 0$ this is possible if and only if $0 \in I$ and $g_0 = 0$. This yields g is the zero polynomial, a contradiction.
- 2. Suppose t = 1, then $\deg_{\sigma}(g) \leq 1$. Since $f_0, f_1 \neq 0$ this is possible if and only if $0 \in I$ and $g_1 = 0$. If $g_0 \neq 0$, since the map $x \in \mathbb{F}_{q^n} \mapsto \mathrm{N}_{q^n/q}(f_0xg_0) \in \mathbb{F}_q$ is surjective, $I = \mathbb{F}_q$ a contradiction. This yields g is the zero polynomial, leading to a contradiction again.
- 3. Suppose t = 0, then $\deg_{\sigma}(g) \leq 2$. Since $f_0 \neq 0$ this is possible if and only if $0 \in I$ and $g_2 = 0$ and $g_0 = 0$ as in the previous case. It follows $g = g_1 X^{\sigma}$, implying $\mathcal{W} = \{\alpha \circ X^{\sigma} : \alpha \in \mathcal{G}_{k-1,\sigma}\}$.

A similar argument can be applied when $\mathcal{W} \subset \mathcal{C}^{(2)}_{n,k,s,I}$. The claim follows. \square

Theorem 7.4. Let $I \notin \{\emptyset, \{0\}, \mathbb{F}_q^*, \mathbb{F}_q\}$ and $1 \in T \subset \mathbb{F}_q^*$. Then the codes of type $C_{n,k,\sigma,I}$ and $C_{\sigma,T}$ are neither equivalent nor adjointly equivalent.

Proof. By contradiction, assume that $C_{n,k,\sigma,I}$ and $C_{\sigma,T}$ are equivalent or adjointly equivalent. Then, there exist $f, g, h \in \tilde{\mathcal{L}}_{n,q,\sigma}$ with f, g invertible and $\rho \in \operatorname{Aut}(\mathbb{F}_q)$ such that

$$C_{n,k,\sigma,I} = f \circ C_{\sigma,T}^{\rho} \circ g + h \text{ or } C_{n,k,\sigma,I} = f \circ (C_{\sigma,T}^{t})^{\rho} \circ g + h.$$

Let \mathcal{U}, \mathcal{V} be the subspaces in $\mathcal{C}_{\sigma,T}$ equivalent to $\mathcal{G}_{k-1,\sigma}$ as defined in (14) and (15). If $\mathcal{C}_{n,k,\sigma,I}$ and $\mathcal{C}_{\sigma,T}$ are equivalent, then $f \circ \mathcal{U}^{\rho} \circ g + h$ and $f \circ \mathcal{V}^{\rho} \circ g + h$ are two different subspaces of $\mathcal{C}_{n,k,\sigma,I}$ equivalent to $\mathcal{G}_{k-1,\sigma}$. By Theorem 7.3, it follows a contradiction.

Next, suppose that $C_{n,k,\sigma,I} = f \circ (C_{\sigma,T}^t)^\rho \circ g + h$. Then $f \circ (\mathcal{U}^t)^\rho \circ g + h$ and $f \circ (\mathcal{V}^t)^\rho \circ g + h$ are two different subspaces of $C_{n,k,\sigma,I}$ equivalent to $C_{k-1,\sigma}$, see [32, Lemma 1], a contradiction again.

Actually, Theorem 7.1 and Theorem 7.4 can be stated in a slightly more general form, where the automorphisms of $\operatorname{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ defining the two classes of non-linear MRD codes are not necessarily equal. Indeed, let σ and τ be generators of the group $\operatorname{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$. Recalling that two generalized Gabidulin codes $\mathcal{G}_{k,\sigma}$ and $\mathcal{G}_{k,\tau}$ are equivalent if and only if $\tau \in \{\sigma, \sigma^{-1}\}$ (see [23, Theorem 4.4]), we have the following result

Theorem 7.5. Let σ and τ be generators of the group $Gal(\mathbb{F}_{q^n}|\mathbb{F}_q)$. If q=2 or $T=\mathbb{F}_q^*$ and $I\in\{\emptyset,\{0\},\mathbb{F}_q^*,\mathbb{F}_q\}$, then the codes $\mathcal{C}_{\sigma,T}$ and $\mathcal{C}_{n,k,\tau,I}$ are equivalent if and only if $\tau\in\{\sigma,\sigma^{-1}\}$. Otherwise, they are neither equivalent nor adjointly equivalent.

Remark 7.6. For linear codes, left and right idealisers are invariants under equivalence [22, Proposition 4.1] and they are subalgebras of $\tilde{\mathcal{L}}_{n,q,\sigma}$ isomorphic to subfields of \mathbb{F}_{q^n} in the case of square linear MRD codes, see [18, Theorem 3.1] and [22, Theorem 5.4]. This, as already stated in [22], does not hold for non-linear codes. In the following, we shall show an example of two equivalent codes such that their left idealisers have different size.

Let \mathbb{F}_5 be the field with five elements and let

$$C_1 = \left\{ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 3 & 4 \\ 3 & 4 \end{pmatrix} \right\} \subset \mathbb{F}_5^{2 \times 2}. \tag{16}$$

Consider the matrix $H = \begin{pmatrix} 0 & 0 \\ 2 & 1 \end{pmatrix}$ and the code

$$C_2 = C_1 + H = \left\{ \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 0 & 0 \end{pmatrix} \right\}. \tag{17}$$

It is straightforward to see that $I_L(C_1)$ is not a matrix field because of the unique element belonging to it is identity matrix, whereas any matrix I_2 of the shape

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$$

with $a, b \in \mathbb{F}_5$ is an element of $I_L(\mathcal{C}_2)$.

Acknowledgement

We are grateful to the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM) which have supported this research.

References

- [1] Byrne, E., Ravagnani, A.: Covering radius of matrix codes endowed with the rank metric. SIAM J. Discrete Mathematics **31**, 927–944 (2017).
- [2] Cossidente, A., Marino, G., Pavese, F.: Non-linear maximum rank distance codes. Designs, Codes and Cryptography 79, 597–609 (2016).
- [3] COOPERSTEIN, B.N.: External flats to varieties in $PG(M_{n,n}(GF(q)))$. Linear Algebra and its Applications **267**, 175–186 (1997).

- [4] DE LA CRUZ, J., KIERMAIERM M., WASSERMANN, A., WILLEMS, W.: Algebraic structures of MRD codes. Advances in Mathematics of Communications, 10(3): 499–510 (2016).
- [5] Delsarte, P.: Bilinear forms over a finite field, with applications to coding theory. Journal of Combinatorial Theory, Series A 25, 226–241 (1978).
- [6] Dembowski P.: Finite Geometries. Springer, New York (1968).
- [7] DONATI, G., DURANTE, N.: Scattered linear sets generated by collineations between pencils of lines. Journal of Algebraic Combinatorics 40, 1121–1134 (2014).
- [8] DONATI, G., DURANTE, N.: A generalization of the normal rational curve in $PG(d, q^n)$ and its associated non-linear MRD codes. Designs, Codes and Cryptography 86, 1175–1184 (2018).
- [9] DURANTE, N., SICILIANO, A.: Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries. The Electronic Journal of Combinatorics (2017).
- [10] Gabidulin, E.: The theory with maximal rank metric distance. Problem on Information Transmission 21, 1–12 (1985).
- [11] Gabidulin, E., Kshevetskiy, A.: The new construction of rank codes. Proceedings. ISIT (2005).
- [12] GORLA, E., JURRIUS, R., LÓPEZ, H.H., RAVAGNANI, A.: Rank-metric codes and q-polymatroids. Journal of Algebraic Combinatorics **52**(1), 1–19 (2020).
- [13] Harris, J.: Algebraic Geometry, A First Course. Springer-Verlag, New York. ISBN 0-387-97716-3 (1992).
- [14] HIRSCHFELD, J.W.P., THAS, J.A.: General Galois Geometries, 2nd ed. Springer, New York (1991).
- [15] JOHNSON, N., JHA, V., BILIOTTI, M.: Handbook of Finite Translation Planes, 1st ed. Chapman and Hall/CRC, (2007).
- [16] LAVRAUW, M., VAN DE VOORDE, G.: Field reduction and linear sets in finite geometry. Book chapter, Contemporary Mathematics, **632**, 271–293 (2015).
- [17] LIDL, R., NIEDERREITER, H.: Finite Fields, 2nd edition. Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge (1997).

- [18] LONGOBARDI, G., ZANELLA, C.: A standard form for scattered linearized polynomials and properties of the related translation planes. Journal of Algebraic Combinatorics (2024), to appear.
- [19] LUNARDON, G.: Normal spread. Geometriae Dedicata 75, 245–261 (1999).
- [20] LUNARDON, G.: *MRD-codes and linear sets*. Journal of Combinatorial Theory, Series A **149**, 1–20 (2017).
- [21] LUNARDON, G., MARINO, G., POLVERINO, O., TROMBETTI, R.: Maximum scattered linear sets of pseudoregulus type and the Segre Variety $S_{n,n}$. Journal of Algebraic Combinatorics 39, 807–831 (2014).
- [22] LUNARDON, G., TROMBETTI, R., ZHOU, Y.: On kernels and nuclei of rank metric codes. Journal of Algebraic Combinatorics 46, 313–340 (2017).
- [23] LUNARDON, G., TROMBETTI, R., ZHOU, Y.: Generalized twisted Gabidulin codes. Journal of Combinatorial Theory, Series A 159, 79–106 (2018).
- [24] SHI, M., KROTOV, D.S., ÖZBUDAK, F.: Constructing MRD codes by switching. Journal of Combinatorial Designs, 32(5), 219–237, (2022).
- [25] MCELIECE, R.J.: A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report 42(44): 114–116 (1978).
- [26] Otal, K., Özbudak, F.: Additive rank metric codes. IEEE Transactions on Information Theory 63, 164–168 (2017).
- [27] Otal, K., Özbudak, F.: Some new non-additive maximum rank distance codes. Finite Fields and Their Applications 50, 293–303 (2018).
- [28] POLVERINO, O.: Linear sets in finite projective spaces. Discrete Mathematics 310, 3096–3107 (2010).
- [29] POLVERINO, O., ZULLO, F.: Connections between scattered linear sets and MRD-codes. Bulletin of Institute of Combinatorics and its Applications. 89, 46–74 (2020).
- [30] PUCHINGER, S., ROSENKILDE NÉ NIELSEN, J., SHEEKEY, J.: Further Generalisations of Twisted Gabidulin Codes In Proceedings of International Workshop on Coding and Cryptography (2017).
- [31] RAWAT, A.S., SILBERSTEIN, N., KOYLUOGLU, O.O., VISHWANATH, S.: Optimal locally repairable codes with local minimum storage regeneration via rank-metric codes. 2013 Information Theory and Applications Workshop (ITA), San Diego, CA, USA, 2013, 1–8, doi: 10.1109/ITA.2013.6502983.

- [32] Sheekey, J.: A new family of linear maximum rank distance codes. Advances in Mathematics of Communications 10 (3), 475–488 (2016).
- [33] Sheekey, J.: *MRD codes: constructions and connections*. Combinatorics and finite fields-difference sets, polynomials, pseudorandomness and applications, 255–285, Radon Series on Computational and Applied Mathematics, **23**, De Gruyter, Berlin, (2019).
- [34] SHEEKEY, J.: New semifields and new MRD codes from skew polynomial rings. Journal of the London Mathematical Society **101**(2), 432–456 (2020).
- [35] SILVA, D., KSCHISCHANG, F.R., KOETTER, R.: A rank-metric approach to error control in random network coding. IEEE Transactions on Information Theory 54, 3951–3967 (2008).
- [36] TAROKH, V., SESHADRI, N., CALDERBANK, A.R.: Space-time codes for high data rate wireless communication: performance criterion and code construction. IEEE Transactions on Information Theory 44, pp. 744-765 (1998).
- [37] TROMBETTI, R., ZHOU, Y.: 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 **65**(2), 1054–1062 (2019).
- [38] WAN, Z.: Geometry of Matrices, World Scientific (1996).

Dipartimento di Matematica e Applicazioni "Renato Caccioppoli" Università degli Studi di Napoli Federico II,

Via Cintia, Monte S. Angelo I-80126 Napoli, Italy.

Email addresses:

{ndurante, giovannigiuseppe.grimaldi, giovanni.longobardi}@unina.it