

LINEAR MAXIMUM RANK DISTANCE CODES OF EXCEPTIONAL TYPE

DANIELE BARTOLI, GIOVANNI ZINI, AND FERDINANDO ZULLO

ABSTRACT. Scattered polynomials of a given index over finite fields are intriguing rare objects with many connections within mathematics. Of particular interest are the *exceptional* ones, as defined in 2018 by the first author and Zhou, for which partial classification results are known. In this paper we propose a unified algebraic description of \mathbb{F}_{q^n} -linear maximum rank distance codes, introducing the notion of *exceptional* linear maximum rank distance codes of a given index. Such a connection naturally extends the notion of exceptionality for a scattered polynomial in the rank metric framework and provides a generalization of Moore sets in the monomial MRD context. We move towards the classification of exceptional linear MRD codes, by showing that the ones of index zero are generalized Gabidulin codes and proving that in the positive index case the code contains an exceptional scattered polynomial of the same index.

1. INTRODUCTION

Let q be a prime power, n be a positive integer, and denote by \mathbb{F}_{q^n} the finite field with q^n elements. Rank metric codes can be seen as sets of \mathbb{F}_q -linear endomorphisms of \mathbb{F}_{q^n} equipped with the rank distance, that is the distance between two elements is defined as the (linear algebraic) rank of their difference. Since the \mathbb{F}_q -algebra of the \mathbb{F}_q -linear endomorphisms of \mathbb{F}_{q^n} and the \mathbb{F}_q -algebra $\mathcal{L}_{n,q} = \left\{ \sum_{i=0}^{n-1} a_i x^{q^i} : a_i \in \mathbb{F}_{q^n} \right\}$ of \mathbb{F}_q -linearized polynomials of q -degree smaller than n are isomorphic, each rank metric code can be also seen as a subset of $\mathcal{L}_{n,q}$. For any $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, we define $\deg_q(f(x)) = \max\{i : a_i \neq 0\}$ and $\min\deg_q(f(x)) = \min\{i : a_i \neq 0\}$. In this context, a rank metric code $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ with minimum distance d achieving the equality in the Singleton-like bound

$$(1) \quad |\mathcal{C}| \leq q^{n(n-d+1)}$$

is called *maximum rank distance* (MRD) code. Rank metric codes and in particular MRD codes have been introduced several times [14, 17] and have been widely investigated in the last few years, due to applications in network coding [37] and cryptography [23]. Two rank metric codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{L}_{n,q}$ are said to be *equivalent* if there exist two invertible \mathbb{F}_q -linearized polynomials $g(x), h(x) \in \mathcal{L}_{n,q}$ and a field automorphism $\rho \in \text{Aut}(\mathbb{F}_{q^n})$ such that

$$\mathcal{C}_1 = g \circ \mathcal{C}_2^\rho \circ h = \{g \circ f^\rho \circ h : f \in \mathcal{C}_2\},$$

where $f^\rho(x) := \sum_{i=0}^{n-1} \rho(a_i) x^{q^i}$ if $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ and the composition has to be considered modulo $x^{q^n} - x$. In order to study the equivalence between two rank metric codes, one can make use of the idealisers. They have been introduced in [22], where the *left* and *right idealisers* of a rank metric code $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ are defined respectively as

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

Such objects have also been investigated in [27], where they have been called respectively middle and right nuclei.

2020 *Mathematics Subject Classification*. Primary 14G50; Secondary 11T06, 94B27.

In this paper we are interested in \mathbb{F}_{q^n} -linear MRD codes, that is MRD codes \mathcal{C} such that $L(\mathcal{C})$ is equivalent to $\mathcal{F}_n = \{\alpha x : \alpha \in \mathbb{F}_{q^n}\}$; see [36, Definition 12]. Thus, every \mathbb{F}_{q^n} -linear MRD code is equivalent to an \mathbb{F}_{q^n} -subspace of $\mathcal{L}_{n,q}$ and we will always consider MRD codes which are \mathbb{F}_{q^n} -subspaces of $\mathcal{L}_{n,q}$. The MRD condition for \mathbb{F}_{q^n} -linear rank metric codes reads as follows. By (1), an \mathbb{F}_{q^n} -linear rank metric code $\mathcal{C} \subseteq \mathcal{L}_{n,q}$, with $\dim_{\mathbb{F}_{q^n}}(\mathcal{C}) = k$ and minimum distance d , is an MRD code if and only if $d = n - k + 1$, or equivalently,

$$\dim_{\mathbb{F}_q}(\ker(f)) \leq k - 1, \text{ for all } f \in \mathcal{C} \setminus \{0\}.$$

This paper is devoted to the investigation of \mathbb{F}_{q^n} -linear MRD codes which are *exceptional*. An \mathbb{F}_{q^n} -linear MRD code $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ is an *exceptional MRD code* if the rank metric code

$$\mathcal{C}_m = \langle \mathcal{C} \rangle_{\mathbb{F}_{q^{nm}}} \subseteq \mathcal{L}_{nm,q}$$

is an MRD code for infinitely many m . Only two families of exceptional \mathbb{F}_{q^n} -linear MRD codes are known:

- (G) $\mathcal{G}_{k,s} = \langle x, x^{q^s}, \dots, x^{q^{s(k-1)}} \rangle_{\mathbb{F}_{q^n}}$, with $\gcd(s, n) = 1$, see [14, 17, 20];
- (T) $\mathcal{H}_{k,s}(\delta) = \langle x^{q^s}, \dots, x^{q^{s(k-1)}}, x + \delta x^{q^{sk}} \rangle_{\mathbb{F}_{q^n}}$, with $\gcd(s, n) = 1$ and $N_{q^n/q}(\delta) \neq (-1)^{nk}$, see [28, 35].

The first family is known as *generalized Gabidulin codes* and the second one as *generalized twisted Gabidulin codes*.

Although the definition of exceptional \mathbb{F}_{q^n} -linear MRD codes appears in this paper for the first time, it has been already studied in particular subcases in different contexts.

In the case $k = 2$, exceptional MRD codes have been considered via so-called exceptional scattered polynomials. Let $f(x) \in \mathcal{L}_{n,q}$ and t be a nonnegative integer $t \leq n - 1$. Then f is said to be *scattered of index t* if for every $x, y \in \mathbb{F}_{q^n}^*$

$$\frac{f(x)}{x^{q^t}} = \frac{f(y)}{y^{q^t}} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q,$$

or equivalently,

$$(2) \quad \dim_{\mathbb{F}_q}(\ker(f(x) - mx^{q^t})) \leq 1, \text{ for every } m \in \mathbb{F}_{q^n}.$$

The term *scattered* arises from a geometric framework; see [10]. Indeed, f is scattered of index t if and only the \mathbb{F}_q -subspace

$$U_{t,f} = \{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\}$$

has the property that $\dim_{\mathbb{F}_q}(U_{t,f} \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}) \leq 1$ for every nonzero vector $\mathbf{v} \in \mathbb{F}_{q^n}^2$, that is $U_{t,f}$ is scattered with respect to the Desarguesian spread $\{\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}} : \mathbf{v} \in \mathbb{F}_{q^n}^2 \setminus \{(0,0)\}\}$. Sheekey in [35], taking into account (2), pointed out the following connection between scattered polynomials and \mathbb{F}_{q^n} -linear MRD codes: f is scattered of index t if and only if $\mathcal{C}_{f,t} = \langle x^{q^t}, f(x) \rangle_{\mathbb{F}_{q^n}}$ is an MRD code with $\dim_{\mathbb{F}_{q^n}}(\mathcal{C}) = 2$. The polynomial f is said to be *exceptional scattered* of index t if it is scattered of index t as a polynomial in $\mathcal{L}_{nm,q}$, for infinitely many m ; see [8]. Taking into account (2), a polynomial f is exceptional scattered of index t if and only if the corresponding MRD code $\mathcal{C}_{f,t}$ is exceptional. While several families of scattered polynomials have been constructed in recent years [7, 10, 11, 13, 24–26, 28, 29, 31, 35, 39, 40], only two families of exceptional ones are known:

- (Ps) $f(x) = x^{q^s}$ of index 0, with $\gcd(s, n) = 1$ (polynomials of so-called pseudoregulus type);
- (LP) $f(x) = x + \delta x^{q^{2s}}$ of index s , with $\gcd(s, n) = 1$ and $N_{q^n/q}(\delta) \neq 1$ (so-called LP polynomials).

Such two families correspond to the known exceptional \mathbb{F}_{q^n} -linear MRD codes (G) and (T).

Several tools have already been proposed in the study of exceptional scattered polynomials, related to algebraic curves or Galois extensions of function fields; see [2, 4, 6, 8, 15]. However, their classification is still unknown when the index is greater than 1.

For $k > 2$, the only known families of \mathbb{F}_{q^n} -subspaces of $\mathcal{L}_{q,n}$ corresponding to MRD codes are (G) and (T) as described above and Delsarte dual codes of the MRD codes associated with scattered polynomials. In [9] it has been shown that the only exceptional \mathbb{F}_{q^n} -linear MRD codes spanned by monomials are the codes (G), in connection with so-called *Moore exponent sets*.

It is therefore natural to investigate exceptional \mathbb{F}_{q^n} -linear MRD codes not generated by monomials. To this aim, we generalize the notion of Moore exponent set; see Section 3.

Using a connection between the generators of \mathbb{F}_{q^n} -linear rank metric codes \mathcal{C} and certain algebraic hypersurfaces $\mathcal{X}_{\mathcal{C}}$, we obtain a partial classification of exceptional \mathbb{F}_{q^n} -linear MRD codes. Tools from intersection theory (see Section 2) yield sufficient conditions on the generators for \mathcal{C} to be MRD, via the existence of \mathbb{F}_{q^n} -rational absolutely irreducible components of $\mathcal{X}_{\mathcal{C}}$.

Our main results can be summarized as follows.

Main Theorem. *Let $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ be an exceptional k -dimensional \mathbb{F}_{q^n} -linear MRD code containing at least a separable polynomial $f(x)$ and a monomial. If $k > 3$, assume also that $q > 5$. Let t be the minimum integer such that $x^{q^t} \in \mathcal{C}$.*

- *If $t = 0$ and $\mathcal{C} = \langle x^{q^t}, g_2(x), g_3(x), \dots, g_k(x) \rangle_{\mathbb{F}_{q^n}}$, with $\deg_q(g_2(x)) < \dots < \deg_q(g_k(x))$ and $(q, \deg_q(g_2(x))) \notin \{(2, 2), (2, 4), (3, 2), (4, 2), (5, 2)\}$, then \mathcal{C} is a generalized Gabidulin code.*
- *If $t > 0$ and $\mathcal{C} = \langle x^{q^t}, f(x), g_3(x), \dots, g_k(x) \rangle_{\mathbb{F}_{q^n}}$, with $\deg(g_i(x)) > \max\{q^t, \deg(f(x))\}$ for each $i = 3, \dots, k$, then $f(x)$ is exceptional scattered of index t .*

When \mathcal{C} contains a separable polynomial and a monomial, we call the non-negative integer t of Main Theorem the *index* of \mathcal{C} .

2. PRELIMINARIES ON ALGEBRAIC VARIETIES

An algebraic hypersurface is an algebraic variety that can be defined by a single polynomial equation. An algebraic hypersurface defined over a field \mathbb{K} is *absolutely irreducible* if the associated polynomial is irreducible over every algebraic extension of \mathbb{K} . An absolutely irreducible \mathbb{K} -rational component of a hypersurface \mathcal{V} , defined by the polynomial F , is simply an absolutely irreducible hypersurface which is associated to a factor of F defined over \mathbb{K} . For a finite field \mathbb{F}_q , let $\overline{\mathbb{F}}_q$ denote its algebraic closure. Also, $\mathbb{P}^m(\mathbb{K})$ (resp. $\mathbb{A}^m(\mathbb{K})$) denotes the m -dimensional projective (resp. affine) space over the field \mathbb{K} .

We recall some known results on algebraic hypersurfaces of which our approach will make use.

Lemma 2.1. *[1, Lemma 2.1] Let \mathcal{H} be an absolutely irreducible hypersurface and \mathcal{X} be an \mathbb{F}_q -rational hypersurface of $\mathbb{P}^m(\overline{\mathbb{F}}_q)$. If $\mathcal{X} \cap \mathcal{H}$ has a non-repeated \mathbb{F}_q -rational absolutely irreducible component, then \mathcal{X} has a non-repeated \mathbb{F}_q -rational absolutely irreducible component.*

With the symbol $I(P, \mathcal{A} \cap \mathcal{B})$ we denote the intersection multiplicity of two plane curves in $\mathbb{A}^2(\mathbb{K})$ at a point $P \in \mathbb{A}^2(\mathbb{K})$. Classical results on such an integer can be found in most of the textbooks on algebraic curves. For other concepts related to algebraic varieties we refer to [18]. For the special case of curves, a good reference is [16].

Lemma 2.2. *[19, Proposition 2] Let $F \in \mathbb{F}_q[X, Y]$ be such that $F = AB$ for some $A, B \in \overline{\mathbb{F}}_q[X, Y]$. Let $P = (u, v)$ be a point in the affine plane $\mathbb{A}^2(\overline{\mathbb{F}}_q)$ and write*

$$F(X + u, Y + v) = F_m(X, Y) + F_{m+1}(X, Y) + \dots,$$

where F_i is zero or homogeneous of degree i and $F_m \neq 0$. Suppose that $F_m = L^m$ for some linear polynomial $L \in \overline{\mathbb{F}}_q[X, Y]$ such that $L \nmid F_{m+1}$. Then $I(P, \mathcal{A} \cap \mathcal{B}) = 0$, where \mathcal{A} and \mathcal{B} are the curves defined by A and B respectively.

Lemma 2.3. [34, Lemma 4.3], [9, Lemma 2.5] Let $F \in \mathbb{F}_q[X, Y]$ be such that $F = AB$ for some $A, B \in \overline{\mathbb{F}}_q[X, Y]$. Let $P = (u, v)$ be a point in the affine plane $\mathbb{A}^2(\overline{\mathbb{F}}_q)$ and write

$$F(X + u, Y + v) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots,$$

where F_i is zero or homogeneous of degree i and $F_m \neq 0$. Suppose that $F_m = L^m$ for some linear polynomial $L \in \overline{\mathbb{F}}_q[X, Y]$ such that $L \mid F_{m+1}$ and $L^2 \nmid F_{m+1}$. Then $I(P, \mathcal{A} \cap \mathcal{B}) = 0$ or m , where \mathcal{A} and \mathcal{B} are the curves defined by A and B respectively.

Lemma 2.4. [16, Section 3.3] Let $F \in \mathbb{F}_q[X, Y]$ be such that $F = AB$ for some $A, B \in \overline{\mathbb{F}}_q[X, Y]$. Let $P = (u, v)$ be a point in the affine plane $\mathbb{A}^2(\overline{\mathbb{F}}_q)$ and write

$$F(X + u, Y + v) = F_m(X, Y) + F_{m+1}(X, Y) + \cdots,$$

where F_i is zero or homogeneous of degree i and $F_m \neq 0$. Suppose that F_m factors into m distinct linear factors in $\overline{\mathbb{F}}_q[X, Y]$. Then $I(P, \mathcal{A} \cap \mathcal{B}) \leq \lfloor m^2/2 \rfloor$.

Lemma 2.5. Let $F(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n]$ with

$$F(X_1, \dots, X_n) = F_m(X_1, \dots, X_n) + F_{m+1}(X_1, \dots, X_n) + \cdots + F_M(X_1, \dots, X_n),$$

where F_i is zero or homogeneous of degree i and $F_m F_M \neq 0$. If F_m or F_M contains a non-repeated absolutely irreducible \mathbb{F}_q -rational factor, then $F(X_1, \dots, X_n)$ contains a non-repeated absolutely irreducible \mathbb{F}_q -rational factor.

Proof. Let G be the non-repeated absolutely irreducible \mathbb{F}_q -rational factor in F_m (resp. F_M). Consider the unique absolutely irreducible factor F' of F such that $G \mid F'_m$ (resp. $G \mid F'_M$). If F' were not defined over \mathbb{F}_q , then there would exist another absolutely irreducible factor $F'' = \sigma(F') \neq F'$ of F satisfying $G \mid F''_m$ (resp. $G \mid F''_M$), where σ is the q -Frobenius automorphism of $\overline{\mathbb{F}}_q[X_1, \dots, X_n]$, whence $G^2 \mid F_m$ (resp. $G^2 \mid F_M$), a contradiction. \square

In the sequel we will investigate hypersurfaces connected with Moore polynomial sets; see Definition 3.3. In particular, we are interested in getting information on the existence of \mathbb{F}_q -rational absolutely irreducible components of curves contained in such hypersurfaces.

The approach that we follow has been used for the first time by Janwa, McGuire and Wilson [19] to classify functions on \mathbb{F}_{p^n} that are almost perfect nonlinear for infinitely many n , in particular for monomial functions. It can be summarized by the following theorem.

Theorem 2.6. [21, Lemma 2] Let $\mathcal{C} \subset \mathbb{P}^2(\mathbb{F}_q)$ be a curve of degree d and let \mathcal{S} be the set of its singular points. Also, let $i(P)$ denote the maximum possible intersection multiplicity of two putative components of \mathcal{C} at $P \in \mathcal{C}$. If

$$\sum_{P \in \mathcal{S}} i(P) < \frac{2d^2}{9},$$

then \mathcal{C} possesses at least one absolutely irreducible component defined over \mathbb{F}_q .

3. MOORE POLYNOMIAL SETS AND MRD CODES

Let q be a prime power and n be a positive integer. Consider k \mathbb{F}_{q^n} -linearly independent polynomials $f_1(x), f_2(x), \dots, f_k(x) \in \mathcal{L}_{n,q}$ and denote by \underline{f} the k -tuple $(f_1(x), \dots, f_k(x))$. Define

$$M_{\underline{f}}(x_1, \dots, x_k) = \begin{pmatrix} f_1(x_1) & f_2(x_1) & \cdots & f_k(x_1) \\ f_1(x_2) & f_2(x_2) & \cdots & f_k(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(x_k) & f_2(x_k) & \cdots & f_k(x_k) \end{pmatrix}.$$

For any $A = \{\alpha_1, \dots, \alpha_k\} \subseteq \mathbb{F}_{q^n}$, define $M_{\underline{f}, A} = M_{\underline{f}}(\alpha_1, \dots, \alpha_k)$.

Lemma 3.1. *If $\alpha_1, \dots, \alpha_k$ are \mathbb{F}_q -linearly dependent, then $\det(M_{\underline{f}, A}) = 0$.*

Proof. Without loss of generality, suppose that $k \geq 2$ and $\alpha_1 = \sum_{i=2}^k b_i \alpha_i$ with $a_i \in \mathbb{F}_q$. Then

$$M_{\underline{f}, A} = \begin{pmatrix} \sum_{i=2}^k b_i f_1(\alpha_i) & \sum_{i=2}^k b_i f_2(\alpha_i) & \cdots & \sum_{i=2}^k b_i f_k(\alpha_i) \\ f_1(\alpha_2) & f_2(\alpha_2) & \cdots & f_k(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(\alpha_k) & f_2(\alpha_k) & \cdots & f_k(\alpha_k) \end{pmatrix},$$

so that the first row of $M_{\underline{f}, A}$ is a linear combination of the remaining rows. Then $\det(M_{\underline{f}, A}) = 0$. \square

The converse of Lemma 3.1 is not true in general, the following being a counterexample.

Example 3.2. *Let k and n be positive integers with n even and $k \leq n$. Consider $\underline{f} = (x, x^{q^2}, \dots, x^{q^{2(k-1)}})$. Let $A = \{\alpha_1, \dots, \alpha_k\}$ be a subset of \mathbb{F}_{q^n} . Then $M_{\underline{f}, A}$ is the Moore matrix*

$$M_{\underline{f}, A} = \begin{pmatrix} \alpha_1 & \alpha_1^{q^2} & \cdots & \alpha_1^{q^{2(k-1)}} \\ \alpha_2 & \alpha_2^{q^2} & \cdots & \alpha_2^{q^{2(k-1)}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_k & \alpha_k^{q^2} & \cdots & \alpha_k^{q^{2(k-1)}} \end{pmatrix},$$

and $\det(M_{\underline{f}, A}) = 0$ if and only if the elements $\alpha_1, \dots, \alpha_k$ are \mathbb{F}_{q^2} -linearly independent; see [30, Corollary 2.1.95]. Therefore, if $\alpha_1, \dots, \alpha_{k-1}$ are \mathbb{F}_q -linearly independent elements in \mathbb{F}_{q^n} and $\alpha_k \in \langle \alpha_1, \dots, \alpha_{k-1} \rangle_{\mathbb{F}_{q^2}} \setminus \langle \alpha_1, \dots, \alpha_{k-1} \rangle_{\mathbb{F}_q}$, then $\det(M_{\underline{f}, A}) = 0$ even though $\{\alpha_1, \dots, \alpha_k\}$ are \mathbb{F}_q -linearly independent.

The following definition identifies the tuples \underline{f} for which the converse of Lemma 3.1 holds and it will be crucial in our investigation for exceptional MRD codes.

Definition 3.3. *Let $\underline{f} = (f_1(x), \dots, f_k(x))$, where k is a positive integer and $f_1(x), \dots, f_k(x) \in \mathcal{L}_{n,q}$. We say that \underline{f} is a Moore polynomial set for q and n if, for any $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{q^n}$,*

$$\det \begin{pmatrix} f_1(\alpha_1) & f_2(\alpha_1) & \cdots & f_k(\alpha_1) \\ f_1(\alpha_2) & f_2(\alpha_2) & \cdots & f_k(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(\alpha_k) & f_2(\alpha_k) & \cdots & f_k(\alpha_k) \end{pmatrix} = 0 \implies \dim_{\mathbb{F}_q} \langle \alpha_1, \dots, \alpha_k \rangle_{\mathbb{F}_q} < k.$$

If \underline{f} is a Moore polynomial set for q and nm for infinitely many m , we say that \underline{f} is an exceptional Moore polynomial set for q and n .

Moore polynomial sets can be characterized in terms of MRD codes as follows.

Theorem 3.4. *Let k and n be positive integers with $k \leq n$, and denote by \underline{f} the k -tuple $(f_1(x), \dots, f_k(x))$, where $f_1(x), \dots, f_k(x) \in \mathcal{L}_{n,q}$ are \mathbb{F}_{q^n} -linearly independent. The \mathbb{F}_{q^n} -linear rank metric code*

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

is an MRD code if and only if \underline{f} is a Moore polynomial set for q and n .

Proof. Suppose that $M_{\underline{f}, A}$ is singular for some $A = \{\alpha_1, \dots, \alpha_k\} \subseteq \mathbb{F}_{q^n}$, that is, there exist $b_1, \dots, b_k \in \mathbb{F}_{q^n}$ such that $\sum_{i=1}^k b_i f_i(\alpha_j) = 0$, for every $j \in \{1, \dots, k\}$. This means that A is contained in the kernel of $F(x) = \sum_{i=1}^k b_i f_i(x) \in \mathcal{C}_{\underline{f}}$. Since $\mathcal{C}_{\underline{f}}$ is an MRD code, it follows that $\dim_{\mathbb{F}_q}(\ker(F)) \leq k - 1$, and hence $\alpha_1, \dots, \alpha_k$ are \mathbb{F}_q -linearly dependent.

Conversely, suppose that \underline{f} is a Moore polynomial set for q and n . Assume by contradiction that there exists $g(x) \in \mathcal{C}_{\underline{f}}$ with $\dim_{\mathbb{F}_q}(\ker(g(x))) \geq k$ and write $g(x) = \sum_{i=1}^k b_i f_i(x)$ with $b_i \in \mathbb{F}_{q^n}$. Let $A = \{\alpha_1, \dots, \alpha_k\} \subseteq \ker(g(x))$ where $\alpha_1, \dots, \alpha_k$ are \mathbb{F}_q -linearly independent. Then $M_{\underline{f}, A}$ is singular because its columns are \mathbb{F}_{q^n} -linearly dependent through $\sum_{i=1}^k b_i f_i(\alpha_j) = 0$ for all $j = 1, \dots, k$. Therefore, \underline{f} is not a Moore polynomial set for q and n . \square

As a natural consequence, a characterization of the exceptionality property is obtained.

Corollary 3.5. *Let $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ be an \mathbb{F}_{q^n} -linear rank metric code. The following are equivalent:*

- \mathcal{C} is an exceptional MRD code.
- Every \mathbb{F}_{q^n} -basis $\{f_1(x), \dots, f_k(x)\}$ of \mathcal{C} defines an exceptional Moore polynomial set $\underline{f} = (f_1(x), \dots, f_k(x))$ for q and n .
- There exists an \mathbb{F}_{q^n} -basis $\{f_1(x), \dots, f_k(x)\}$ of \mathcal{C} for which $\underline{f} = (f_1(x), \dots, f_k(x))$ is an exceptional Moore polynomial set for q and n .

We will investigate exceptional MRD codes by means of exceptional Moore polynomial sets.

4. MOORE POLYNOMIAL SETS AND VARIETIES OVER FINITE FIELDS

In this section we study exceptional \mathbb{F}_{q^n} -linear MRD codes $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ of dimension k under the assumption that \mathcal{C} contains a monomial. Up to equivalence, we can assume that \mathcal{C} contains a separable polynomial. We denote by t the smallest non-negative integer such that $x^{q^t} \in \mathcal{C}$.

Remark 4.1. *If \mathcal{C} is an \mathbb{F}_{q^n} -linear MRD code in $\mathcal{L}_{n,q}$, then \mathcal{C} contains an invertible map $f(x)$ (see [27, Lemma 2.1] and [33, Lemma 52]), and hence $f^{-1} \circ \mathcal{C}$ contains the identity x . If \mathcal{C} is exceptional, then $\max\{\deg_q(g(x)) : g(x) \in \langle \mathcal{C} \rangle_{\mathbb{F}_{q^{nm}}}\}$ does not depend on the infinitely many m 's for which $\langle \mathcal{C} \rangle_{\mathbb{F}_{q^{nm}}}$ is MRD. On the contrary, $\max\{\deg_q(g(x)) : g(x) \in \langle f^{-1} \circ \mathcal{C} \rangle_{\mathbb{F}_{q^{nm}}}\}$ may depend on m , so that $f^{-1} \circ \mathcal{C}$ may not be exceptional.*

On the other hand, the assumption that \mathcal{C} contains a separable polynomial does not affect the exceptionality of \mathcal{C} , since $\max\{\deg_q(g(x)) : g(x) \in \mathcal{C}\}$ decreases by $\min\{\text{mindeg}_q(g(x)) : g(x) \in \mathcal{C}\}$.

Assumptions 4.2. *Note that there exist $f_1(x), \dots, f_k(x) \in \mathcal{C}$ such that the following hold:*

- (1) $f_1(x), \dots, f_k(x)$ are monic and \mathbb{F}_{q^n} -linearly independent;
- (2) $M_1 := \deg_q(f_1(x)), \dots, M_k := \deg_q(f_k(x))$ are all distinct;
- (3) $m_1 := \text{mindeg}_q(f_1(x)), \dots, m_k := \text{mindeg}_q(f_k(x))$ are all distinct, and $m_i = 0$ for some i ;
- (4) $f_1(x) = x^{q^t}$;
- (5) for any i , if $f_i(x)$ is a monomial then $m_i = M_i \geq t$.

Therefore, by Corollary 3.5, we investigate Moore polynomial sets as in the following definition.

Definition 4.3. *A Moore polynomial set $\underline{f} = (f_1(x), \dots, f_k(x)) \subseteq \mathcal{L}_{n,q}^k$ satisfying Assumptions 4.2 is said to be a Moore polynomial set for q and n of index t .*

A key tool in our approach is a link between Moore polynomial sets and algebraic hypersurface. To this aim, we introduce the following \mathbb{F}_{q^n} -rational hypersurfaces: $\mathcal{U} := \mathcal{U}_{\underline{f}} \subset \mathbb{P}^k(\overline{\mathbb{F}_{q^n}})$ is the hypersurface defined by the affine equation

$$F_{\underline{f}}(X_1, \dots, X_k) := \det(M_{\underline{f}}(X_1, \dots, X_k)) = 0,$$

and $\mathcal{V} \subset \mathbb{P}^k(\overline{\mathbb{F}_{q^n}})$ is the hypersurface $\mathcal{U}_{(x, x^q, \dots, x^{q^{k-1}})}$. Note that

$$F_{(x, x^q, \dots, x^{q^{k-1}})}(X_1, \dots, X_k) = \prod_{(a_1, \dots, a_k) \in \mathbb{P}^{k-1}(\mathbb{F}_q)} (a_1 X_1 + \dots + a_k X_k),$$

with a suitable choice of the representative for the points $(a_1 : \dots : a_k)$. Since $f_1(x), \dots, f_k(x)$ are \mathbb{F}_q -linearized, the polynomial $F_{(x, x^q, \dots, x^{q^{k-1}})}(X_1, \dots, X_k)$ divides $F_{\underline{f}}(X_1, \dots, X_k)$, so that \mathcal{V} is a component of \mathcal{U} . Therefore we can define the \mathbb{F}_{q^n} -rational variety $\mathcal{W} \subset \mathbb{P}^k(\overline{\mathbb{F}}_q^n)$ with affine equation

$$\mathcal{W}: F_{\underline{f}}(X_1, \dots, X_k) / F_{(x, x^q, \dots, x^{q^{k-1}})}(X_1, \dots, X_k) = 0.$$

The link between Moore polynomial sets and algebraic hypersurfaces \mathcal{W} is straightforward.

Theorem 4.4. *The k -tuple \underline{f} is a Moore polynomial set for q and n if and only if all the affine \mathbb{F}_{q^n} -rational points of \mathcal{W} lie on \mathcal{V} .*

Proof. For any $A = \{\alpha_1, \dots, \alpha_k\} \subseteq \mathbb{F}_{q^n}$, the condition $\det(M_{\underline{f}, A}) = 0$ is equivalent to $(\alpha_1, \dots, \alpha_k)$ being an affine \mathbb{F}_{q^n} -rational point of \mathcal{W} , while the condition $\dim_{\mathbb{F}_q}(\langle \alpha_1, \dots, \alpha_k \rangle_{\mathbb{F}_q}) < k$ is equivalent to $(\alpha_1, \dots, \alpha_k)$ being a point of \mathcal{V} . The claim follows. \square

In the case when $f_1(x), \dots, f_k(x)$ are monomials, Theorem 4.4 was already noticed (using a slightly different terminology) and used in [9] to prove the following result.

Theorem 4.5. [9, Theorems 1.1, 3.2, 4.1] *Let $I = \{i_1 = 0, i_2, \dots, i_k\}$ be a set of non-negative integers with $0 < i_2 < \dots < i_k$ such that I is not in arithmetic progression. Suppose that one of the following holds:*

- $|I| = 3$ and $n > 4i_k + 2$;
- $|I| > 3$, $q > 5$ and $n > \frac{13}{3}i_k + \log_q(13 \cdot 2^{10/3})$.

Then $(x, x^{q^{i_2}}, \dots, x^{q^{i_k}})$ is not a Moore polynomial set for q and n .

In the sequel, we will use the following notation: for any $i = 1, \dots, k$, write $f_i(x) = \sum_{j=m_i}^{M_i} a_{ij}x^{q^j}$ and $f_i(x, z) := \sum_{j=m_i}^{M_i} a_{ij}x^{q^j}z^{M_j - q^j}$.

4.1. Moore polynomial sets of index 0. In this section we investigate Moore polynomial sets of index 0, so that $f_1(x) = x$. Without loss of restriction, we assume $M_1 = 0 < M_2 < \dots < M_k$.

Theorem 4.6. *Suppose that one of the following holds:*

- $k = 3$ and $n > 4M_3 + 2$;
- $k > 3$, $q > 5$ and $n > \frac{13}{3}M_k + \log_q(13 \cdot 2^{10/3})$.

If \underline{f} is a Moore polynomial set for q and n of index 0, then $(M_1 = 0, M_2, \dots, M_k)$ is in arithmetic progression and $(m_{\sigma(1)} = 0, m_{\sigma(2)}, \dots, m_{\sigma(k)})$ is in arithmetic progression for some $\sigma \in S_k$ with $\sigma(1) = 1$.

Proof. In order to prove the claim on the M_i 's, consider the intersection $\mathcal{W}_\infty = \mathcal{W} \cap \mathcal{H}_\infty$ between \mathcal{W} and the hyperplane at infinity $\mathcal{H}_\infty \subset \mathbb{P}^k(\overline{\mathbb{F}}_q^n)$. Note that $\mathcal{W}_\infty \subset \mathbb{P}^{k-1}(\overline{\mathbb{F}}_q^n)$ is defined by

$$\mathcal{W}_\infty: F_{(x, x^{q^{M_2}}, \dots, x^{q^{M_k}})}(X_1, \dots, X_k) / F_{(x, x^q, \dots, x^{q^{k-1}})}(X_1, \dots, X_k) = 0.$$

Suppose that (M_1, \dots, M_k) is not in arithmetic progression. Then it has been shown in [9, Theorems 3.1 and 4.2] that \mathcal{U}_∞ contains an \mathbb{F}_{q^n} -rational non-repeated absolutely irreducible component \mathcal{X} . It follows by Lemma 2.5 that \mathcal{W} has an \mathbb{F}_{q^n} -rational non-repeated absolutely irreducible component. Then, as shown in [9] (in page 9 for $k = 3$, and in page 17 for $k > 3$), there exists an affine \mathbb{F}_{q^n} -rational point in $\mathcal{W} \setminus \mathcal{V}$. Thus, \underline{f} is not a Moore polynomial set for q and n by Theorem 4.4.

Now suppose that $(m_{\sigma(1)}, \dots, m_{\sigma(k)})$ is not in arithmetic progression for any $\sigma \in S_k$. Consider the tangent variety \mathcal{T} of \mathcal{W} at the origin O . Then

$$\mathcal{T}: F_{(x^{q^{m_{\sigma(1)}}}, x^{q^{m_{\sigma(2)}}}, \dots, x^{q^{m_{\sigma(k)}}})}(X_1, \dots, X_k) / F_{(x, x^q, \dots, x^{q^{k-1}})}(X_1, \dots, X_k) = 0.$$

Now the same arguments as above show that \mathcal{T} has an \mathbb{F}_{q^n} -rational non-repeated absolutely irreducible component. Then \mathcal{W} has an \mathbb{F}_{q^n} -rational non-repeated absolutely irreducible component by Lemma 2.5. Therefore, as in [9], \mathcal{W} has an affine \mathbb{F}_{q^n} -rational point not in \mathcal{V} , so that \underline{f} is not a Moore polynomial set for q and n . \square

In the rest of this subsection, \underline{f} is a Moore polynomial set for q and n of index 0, satisfying the assumptions of Theorem 4.6, so that $M_1 = 0, M_2 = M, \dots, M_k = (k-1)M$.

Let $\lambda_3, \dots, \lambda_k$ be \mathbb{F}_q -linearly independent elements of \mathbb{F}_{q^n} and define $H_{\underline{f}}(X_1, X_2) = F_{\underline{f}}(X_1, X_2, \lambda_3, \dots, \lambda_k) \in \mathbb{F}_{q^n}[X_1, X_2]$. Since \underline{f} is a Moore polynomial set, $H_{\underline{f}}(X_1, X_2) \neq 0$. Let $\mathcal{D}_{\underline{f}} \subset \mathbb{P}^2(\overline{\mathbb{F}_{q^n}})$ be the curve defined by $H_{\underline{f}}(X_1, X_2) = 0$. We denote by $H_{\underline{f}}(X_1, X_2, T)$ the homogenization of $H_{\underline{f}}(X_1, X_2)$, i.e.

$$H_{\underline{f}}(X_1, X_2, T) := \det \begin{pmatrix} X_1 & f_2(X_1, T) & \cdots & f_k(X_1, T) \\ X_2 & f_2(X_2, T) & \cdots & f_k(X_2, T) \\ \lambda_3 T & f_2(\lambda_3)T^{q^M} & \cdots & f_k(\lambda_3)T^{q^{(k-1)M}} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_k T & f_2(\lambda_k)T^{q^M} & \cdots & f_k(\lambda_k)T^{q^{(k-1)M}} \end{pmatrix} \Big/ T^{\frac{q^{(k-2)M}-1}{q^M-1}}.$$

Lemma 4.7. *If $\mathcal{D}_{\underline{f}}$ has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component not contained in $\mathcal{D}_{x, x^q, \dots, x^{q^{k-1}}}$, then \mathcal{W} has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component not contained in \mathcal{V} .*

Proof. Consider the variety $\mathcal{W}_3 \subset \mathbb{P}^3(\overline{\mathbb{F}_{q^n}})$ defined by

$$\mathcal{W}_3: F_{\underline{f}}(X_1, X_2, X_3, \lambda_4, \dots, \lambda_k) / F_{(x, x^q, \dots, x^{q^{k-1}})}(X_1, X_2, X_3, \lambda_4, \dots, \lambda_k) = 0.$$

Let $\Pi_3 \subset \mathbb{P}^3(\overline{\mathbb{F}_{q^n}})$ be the hyperplane with affine equation $X_3 = \lambda_3$. By the assumptions, $\mathcal{W}_3 \cap \Pi_3$ has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component. Hence, by Lemma 2.1, \mathcal{W}_3 has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component. The claim follows by repeatedly applying this argument to $\mathcal{W}_3, \dots, \mathcal{W}_k = \mathcal{W}$. \square

Remark 4.8. *It is readily seen that $(x, f(x))$ is a Moore polynomial set for q and n if and only if $f(x)$ is scattered of index 0 over \mathbb{F}_{q^n} . By the results in [6, 8], if $n > 4 \deg_q(f(x))$ and $(x, f(x))$ is a Moore polynomial set for q and n , then $f(x)$ is a monomial with $\gcd(n, \deg_q(f(x))) = 1$. Next results deal with the case $k > 2$.*

Theorem 4.9. *Let $\underline{f} = (f_1(x) = x, f_2(x), f_3(x))$ be a Moore polynomial set for q and n of index 0 with $0 < M_2 < M_3$. If $n > 4M_3 + 2$, then $f_2(x) \in \mathcal{L}_{n,q}$ is scattered of index 0.*

Proof. By Theorem 4.6, $M_3 = 2M$ where $M = M_2$. Suppose that $f_2(x) \in \mathcal{L}_{n,q}$ is not scattered of index 0, so that there exist $\lambda, \mu \in \mathbb{F}_{q^n}^*$ such that $\lambda/\mu \notin \mathbb{F}_q$ and $f_2(\lambda)/\lambda = f_2(\mu)/\mu$. By [5, Corollary 3.4], we can assume that $\mu \notin \mathbb{F}_q$ and $f_2(\lambda) \neq 0$.

Let $\lambda_3 = \lambda$ and define $\mathcal{D}_{\underline{f}}$ as above. Let $\mathcal{D}'_{\underline{f}}$ be the image of $\mathcal{D}_{\underline{f}}$ under the \mathbb{F}_{q^n} -rational projectivity $\varphi : (X_1 : X_2 : T) \mapsto (T : X_2 - X_1 : X_1)$. Note that the point $P = (1 : 1 : 0) \in \mathcal{D}_{\underline{f}}$ is mapped by φ to $O = (0 : 0 : 1)$. The curve $\mathcal{D}'_{\underline{f}}$ has affine equation $H'_{\underline{f}}(X_1, X_2) = 0$, where

$$\begin{aligned} H'_{\underline{f}}(X_1, X_2) &= H_{\underline{f}}(1, X_2+1, X_1) = \det \begin{pmatrix} 1 & f_2(1, X_1) & f_3(1, X_1) \\ X_2+1 & f_2(1, X_1) + f_2(X_2, X_1) & f_3(1, X_1) + f_3(X_2, X_1) \\ \lambda & f_2(\lambda)X_1^{q^M-1} & f_3(\lambda)X_1^{q^{2M}-1} \end{pmatrix} \\ &= \det \begin{pmatrix} 1 & f_2(1, X_1) & f_3(1, X_1) \\ X_2 & f_2(X_2, X_1) & f_3(X_2, X_1) \\ \lambda & f_2(\lambda)X_1^{q^M-1} & f_3(\lambda)X_1^{q^{2M}-1} \end{pmatrix} = -\lambda f_2(X_2, X_1) + f_2(\lambda)X_2X_1^{q^M-1} + G(X_1, X_2), \end{aligned}$$

for some $G(X_1, X_2) \in \mathbb{F}_{q^n}[X_1, X_2]$ of degree bigger than q^M .

The homogeneous polynomial $L(X_1, X_2) = -\lambda f_2(X_2, X_1) + f_2(\lambda)X_2X_1^{q^M-1}$ has $X_2 - \mu X_1$ as a non-repeated factor in $\mathbb{F}_{q^n}[X_1, X_2]$, since μ is a root of the separable polynomial $L(1, X_2) \in \mathbb{F}_{q^n}[X_2]$. Therefore $\mathcal{D}'_{\underline{f}}$ has a non repeated \mathbb{F}_{q^n} -rational absolutely irreducible component, and the same holds for $\mathcal{D}_{\underline{f}}$. Since $\mu \notin \mathbb{F}_q$, such a component of $\mathcal{D}_{\underline{f}}$ is not contained in $\mathcal{D}_{(x, x^q, x^{q^2})}$.

By Lemma 4.7, \mathcal{W} has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component \mathcal{Z} not contained in \mathcal{V} . The degree of \mathcal{V} is $q^2 + q + 1$, and the degree of \mathcal{Z} is at most $q^{2M} + q^M - q^2 - q$. Thus, by [38, Corollary 7], \mathcal{Z} has an affine \mathbb{F}_{q^n} -rational point not on \mathcal{V} , a contradiction to Theorem 4.4. \square

Theorem 4.10. *Let $\underline{f} = (f_1(x) = x, f_2(x), f_3(x))$ be a Moore polynomial set for q and n of index 0 such that $0 < M_2 < M_3$, and $(q, M) \notin \{(2, 2), (2, 4), (3, 2), (4, 2), (5, 2)\}$. If $n > 4M_3 + 2$, then $\underline{f} = (x, x^{q^M}, x^{q^{2M}})$ with $\gcd(M, n) = 1$.*

Proof. By Theorem 4.6, $M_3 = 2M$ and $\max\{m_2, m_3\} = 2 \min\{m_2, m_3\}$. By Theorem 4.9, $f_2(x)$ is scattered of index 0 over \mathbb{F}_{q^n} . Thus, by the numerical assumption on n , it follows that $f_2(x) = x^{q^M}$ and $\gcd(M, n) = 1$; see [8, Section 3.1] for $q > 5$ and [6, Section 5] for $q \leq 5$.

From $m_2 = M$ it follows that $m_3 \in \{2M, M/2\}$. Suppose by contradiction that $f_3(x) \neq x^{q^{2M}}$, so that $m_3 = M/2 < M$, and in particular M is even. Choose $\lambda_3 = \lambda \in \mathbb{F}_{q^n}^*$ such that $f_2(\lambda)f_3(\lambda) \neq 0$. Via Theorem 2.6, we will prove that the variety \mathcal{W}_3 with affine equation

$$\mathcal{W}_3: F_{\underline{f}}(X_1, X_2, \lambda)/F_{(x, x^q, x^{q^2})}(X_1, X_2, \lambda) = 0$$

has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component not contained in \mathcal{V} .

Suppose that \mathcal{W}_3 splits into two components \mathcal{A} and \mathcal{B} sharing no common absolutely irreducible component. Let $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ be two components of $\mathcal{D}_{\underline{f}}$ sharing no common absolutely irreducible components and such that $\mathcal{A} \subseteq \tilde{\mathcal{A}}$, $\mathcal{B} \subseteq \tilde{\mathcal{B}}$. Singular points of \mathcal{W}_3 are also singular points of $\mathcal{D}_{\underline{f}}$, and the intersection multiplicity of \mathcal{A} and \mathcal{B} at a point is at most the intersection multiplicity of $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ at that point. We start the inspection of singular points of \mathcal{W}_3 from affine ones. Let $P = (\alpha, \beta) \in \mathbb{P}^2(\mathbb{F}_{q^n})$ be an affine point of $\mathcal{D}_{\underline{f}}$. The point P is singular for $\mathcal{D}_{\underline{f}}$ if and only if $f_3(\lambda)f_2(\alpha) - f_2(\lambda)f_3(\alpha) = 0$ and $f_3(\lambda)f_2(\beta) - f_2(\lambda)f_3(\beta) = 0$, that is

$$f_3(\lambda)\alpha^{q^M} - \lambda^{q^M}f_3(\alpha) = f_3(\lambda)\beta^{q^M} - \lambda^{q^M}f_3(\beta) = 0.$$

Also, the intersection multiplicity of $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ at P equals the intersection multiplicity of $\tau(\tilde{\mathcal{A}})$ and $\tau(\tilde{\mathcal{B}})$ at $\tau(P) = O = (0, 0)$, where τ is the translation $(X_1, X_2) \mapsto (X_1 - \alpha, X_2 - \alpha)$. The image $\mathcal{D}'_{\underline{f}}$ of $\mathcal{D}_{\underline{f}}$ under τ has affine equation $H'_{\underline{f}}(X_1, X_2) = 0$, with

$$\begin{aligned} H'_{\underline{f}}(X_1, X_2) &= H_{\underline{f}}(X_1 + \alpha, X_2 + \beta) = \det \begin{pmatrix} X_1 + \alpha & X_1^{q^M} + \alpha^{q^M} & f_3(X_1) + f_3(\alpha) \\ X_2 + \beta & X_2^{q^M} + \beta^{q^M} & f_3(X_2) + g(\beta) \\ \lambda & \lambda^{q^M} & f_3(\lambda) \end{pmatrix} \\ &= a \left((\lambda\alpha^{q^M} - \alpha\lambda^{q^M})X_2^{q^{m_3}} - (\lambda\beta^{q^M} - \beta\lambda^{q^M})X_1^{q^{m_3}} - \lambda^{q^M}(X_1X_2^{q^{m_3}} - X_2X_1^{q^{m_3}}) \right) + G(X_1, X_2), \end{aligned}$$

where $a \neq 0$ is the coefficient of $x^{q^{m_3}}$ in $f_3(x)$, and $G(X_1, X_2) \in \mathbb{F}_{q^n}[X_1, X_2]$ has degree bigger than $q^{m_3} + 1$. We denote respectively by $(H'_{\underline{f}})_{q^{m_3}}$ and $(H'_{\underline{f}})_{q^{m_3+1}}$ the homogeneous polynomials $(\lambda\alpha^{q^M} - \alpha\lambda^{q^M})X_2^{q^{m_3}} - (\lambda\beta^{q^M} - \beta\lambda^{q^M})X_1^{q^{m_3}}$ and $X_1X_2^{q^{m_3}} - X_2X_1^{q^{m_3}}$. If non-vanishing, they are, up to a scalar multiple, the homogeneous parts of smallest degrees in $H'_{\underline{f}}(X_1, X_2)$. Note that the $q^{m_3} + 1$ linear factors of $(H'_{\underline{f}})_{q^{m_3+1}}$ are all distinct.

- There are at most q^{2M} singular points (α, β) of $\mathcal{D}_{\underline{f}}$ which satisfy $\lambda\alpha^{q^M} - \alpha\lambda^{q^M} = \lambda\beta^{q^M} - \beta\lambda^{q^M} = 0$. In this case, $(H'_{\underline{f}})_{q^{m_3+1}}$ is the non-zero homogeneous part of smallest degree in $H'_{\underline{f}}(X_1, X_2)$. Thus O is an ordinary $(q^{m_3} + 1)$ -fold point for $\mathcal{D}'_{\underline{f}}$, and by Lemma 2.4 the intersection multiplicity of $\tau(\tilde{\mathcal{A}})$ and $\tau(\tilde{\mathcal{B}})$ at O is at most $(q^{m_3} + 1)^2/4$.
- There are at most $2(q^{2M-m_3} - 1) \cdot q^M$ singular points (α, β) of $\mathcal{D}_{\underline{f}}$ which satisfy either $\lambda\alpha^{q^M} - \alpha\lambda^{q^M} \neq 0 = \lambda\beta^{q^M} - \beta\lambda^{q^M}$ or $\lambda\alpha^{q^M} - \alpha\lambda^{q^M} = 0 \neq \lambda\beta^{q^M} - \beta\lambda^{q^M}$.
In this case, $(H'_{\underline{f}})_{q^{m_3}} = X_2^{q^{m_3}}$ or $(H'_{\underline{f}})_{q^{m_3}} = X_1^{q^{m_3}}$ up to a non-zero scalar multiple, and hence $\gcd(H'_{\underline{f}})_{q^{m_3}}, (H'_{\underline{f}})_{q^{m_3+1}} = X_2$ or X_1 . By Lemma 2.3, the intersection multiplicity of $\tau(\tilde{\mathcal{A}})$ and $\tau(\tilde{\mathcal{B}})$ at O is at most q^{m_3} .
- There are at most $(q^{2M-m_3} - 1) \cdot (q^{m_3} - 1) \cdot q^M$ singular points (α, β) of $\mathcal{D}_{\underline{f}}$ which satisfy $\lambda\alpha^{q^M} - \alpha\lambda^{q^M} \neq 0$, $\lambda\beta^{q^M} - \beta\lambda^{q^M} \neq 0$, and $\eta(\lambda\alpha^{q^M} - \alpha\lambda^{q^M}) = \xi(\lambda\beta^{q^M} - \beta\lambda^{q^M})$ for some $(\xi : \eta) \in \mathbb{P}^1(\mathbb{F}_{q^{m_3}}) \setminus \{(1 : 0), (0 : 1)\}$. In this case, $(H'_{\underline{f}})_{q^{m_3}} = (\xi X_2 - \eta X_1)^{q^{m_3}}$ up to a non-zero scalar multiple, and hence $(H'_{\underline{f}})_{q^{m_3}}$ and $(H'_{\underline{f}})_{q^{m_3+1}}$ are not coprime. By Lemma 2.3, the intersection multiplicity of $\tau(\tilde{\mathcal{A}})$ and $\tau(\tilde{\mathcal{B}})$ at O is at most q^{m_3} .
- If a singular point (α, β) of $\mathcal{D}_{\underline{f}}$ satisfies $\eta(\lambda\alpha^{q^M} - \alpha\lambda^{q^M}) = \xi(\lambda\beta^{q^M} - \beta\lambda^{q^M})$ for some $(\xi : \eta) \notin \mathbb{P}^1(\mathbb{F}_{q^{m_3}})$, then $(H'_{\underline{f}})_{q^{m_3}}$ and $(H'_{\underline{f}})_{q^{m_3+1}}$ are coprime. In this case, by Lemma 2.2, the intersection multiplicity of $\tau(\tilde{\mathcal{A}})$ and $\tau(\tilde{\mathcal{B}})$ at O is 0.

Since the homogeneous part of largest degree in $H_{\underline{f}}(X_1, X_2)$ is

$$\lambda \cdot X_1^{q^M} \cdot \prod_{\gamma \in \mathbb{F}_{q^M}} (X_2 - \gamma X_1)^{q^M},$$

the points at infinity of $\mathcal{D}_{\underline{f}}$ are $(0 : 1 : 0)$ and $(1 : \gamma : 0)$ with $\gamma \in \mathbb{F}_{q^M}$. As the map $(X_1 : X_2 : T) \mapsto (X_2 : X_1 : T)$ maps $(0 : 1 : 0)$ to $(1 : 0 : 0)$ and leaves invariant the curves $\mathcal{D}_{\underline{f}}$ and $\mathcal{D}_{(x, x^q, x^{q^2})}$, it is enough to consider the points $P_{\gamma} = (1 : \gamma : 0)$ with $\gamma \in \mathbb{F}_{q^M}$. The intersection multiplicity of $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ at P_{γ} equals the intersection multiplicity of $\sigma(\tilde{\mathcal{A}})$ and $\sigma_{\gamma}(\tilde{\mathcal{B}})$ at $\sigma_{\gamma}(P) = O = (0, 0)$, where $\sigma_{\gamma} : (X_1 : X_2 : T) \mapsto (T : X_2 - \gamma T : X_1)$. The image $\mathcal{D}'_{\underline{f}}$ of $\mathcal{D}_{\underline{f}}$ under σ_{γ} has affine equation $H''_{\underline{f}}(X_1, X_2) = 0$, where

$$H''_{\underline{f}}(X_1, X_2) = H_{\underline{f}}(1, X_2 + \alpha, X_1) = \det \begin{pmatrix} 1 & f_2(1, X_1) & f_3(1, X_1) \\ X_2 + \gamma & f_2(X_2 + \gamma, X_1) & f_3(X_2 + \gamma, X_1) \\ \lambda & f_2(\lambda)X_1^{q^M-1} & f_3(\lambda)X_1^{q^{2M}-1} \end{pmatrix} =$$

$$\det \begin{pmatrix} 1 & 1 & f_3(1, X_1) \\ X_2 & X_2^{q^M} & f_3(X_2, X_1) + f_3(\gamma, X_1) - \gamma f_3(1, X_1) \\ \lambda & \lambda^{q^M} X_1^{q^M-1} & f_3(\lambda)X_1^{q^{2M}-1} \end{pmatrix} = \lambda^{q^M} X_2 X_1^{q^M-1} - \lambda X_2^{q^M} + G(X_1, X_2),$$

for some $G(X_1, X_2)$ of degree greater than q^M (here, we used that the constant term in $f_3(\gamma, X_1)$ is the same as in $\gamma f_3(1, X_1)$). Since $\lambda^{q^M} X_2 X_1^{q^M-1} - \lambda X_2^{q^M}$ is homogeneous and separable in each variable, 0 is an ordinary q^M -fold point for $\mathcal{D}'_{\underline{f}}$, and by Lemma 2.4 the intersection multiplicity of $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ at P_{α} is at most $q^{2M}/4$. The same holds at $(0 : 1 : 0)$.

Summing up, the number of intersection points of two components of $H_{\underline{f}}(X_1, X_2, T) = 0$, counted with multiplicity, satisfies

$$\sum_P I(P, \mathcal{A} \cap \mathcal{B}) \leq q^{2M} \frac{(q^{m_3} + 1)^2}{4} + 2(q^{2M-m_3} - 1)q^{M+m_3} + (q^{2M-m_3} - 1)(q^{m_3} - 1)q^{M+m_3} + (q^M + 1) \frac{q^{2M}}{4}.$$

Since $(q, M) \notin \{(2, 2), (2, 4), (3, 2), (4, 2), (5, 2)\}$, the above quantity is less than

$$\frac{2}{9} \deg(\mathcal{W}_3)^2 = \frac{2}{9}(q^{2M} + q^M - q^2 - q)^2.$$

By Theorem 2.6, \mathcal{W}_3 contains an \mathbb{F}_{q^n} -rational absolutely irreducible component \mathcal{X} . Note that $\mathcal{D}_{\underline{f}}$ has only finitely many singular points, and hence \mathcal{X} is non-repeated and not contained in \mathcal{V} . Arguing as in the last paragraph of the proof of Theorem 4.9, a contradiction arises. This shows $m_3 = 2M$, i.e. $f_3(x) = x^{q^{2M}}$. \square

By means of an induction argument, we are able to extend the result of Theorem 4.10 to any Moore polynomial set of index 0, as follows.

Theorem 4.11. *Let $\underline{f} = (f_1(x) = x, f_2(x), \dots, f_k(x))$, with $k > 3$, be a Moore polynomial set for q and n of index 0 such that $0 < M_2 < \dots < M_k$. Suppose also that $q > 5$ and $n > \frac{13}{3}M_k + \log_q(13 \cdot 2^{10/3})$. Then $\underline{f} = (x, x^{q^M}, \dots, x^{q^{(k-1)M}})$ with $\gcd(M, n) = 1$.*

Proof. By Theorem 4.6, $M_i = (i-1)M$ for every i , with $\gcd(M, n) = 1$. Also, $\{0, m_2, \dots, m_k\}$ can be ordered so that they are in arithmetic progression.

We prove by finite induction on $i \in \{3, \dots, k\}$ the following fact: if $\underline{h} = (x, f_2(x), \dots, f_i(x))$ satisfies $\underline{h} \neq (x, x^{q^M}, \dots, x^{q^{(i-1)M}})$, then the hypersurface $\mathcal{U}_{\underline{h}}$ has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component not contained in \mathcal{V} . The base $i = 3$ has been worked out in the proof of Theorem 4.10. For $i > 3$, define the map $\varphi: (X_1: \dots: X_i: T) \mapsto (T: X_2 - X_1: X_3: \dots: X_i: X_1)$, which maps $(1: 1: 0: \dots: 0) \in \mathcal{U}_{\underline{f}}$ to $O = (0: \dots: 0: \dots: 1)$, and consider the image $\mathcal{U}'_{\underline{f}}$ of $\mathcal{U}_{\underline{f}}$ under φ , which has affine equation $F'_{\underline{f}}(X_1, \dots, X_i) = 0$, where $F'_{\underline{f}}(X_1, X_2, \dots, X_i)$ equals

$$\det \begin{pmatrix} 1 & f_2(1, X_1) & \dots & f_i(1, X_1) \\ X_2 + 1 & f_2(1, X_1) + f_2(X_2, X_1) & \dots & f_i(1, X_1) + f_i(X_2, X_1) \\ X_3 & f_2(X_3, X_1) & \dots & f_i(X_3, X_1) \\ \vdots & \vdots & \ddots & \vdots \\ X_i & f_2(X_i, X_1) & \dots & f_i(X_i, X_1) \end{pmatrix} = \det \begin{pmatrix} 1 & f_2(1, X_1) & \dots & f_i(1, X_1) \\ X_2 & f_2(X_2, X_1) & \dots & f_i(X_2, X_1) \\ X_3 & f_2(X_3, X_1) & \dots & f_i(X_3, X_1) \\ \vdots & \vdots & \ddots & \vdots \\ X_i & f_2(X_i, X_1) & \dots & f_i(X_i, X_1) \end{pmatrix}.$$

The tangent cone to $\mathcal{U}'_{\underline{f}}$ at O has equation

$$F_{\underline{g}}^*(X_2, \dots, X_i, X_1) = \det \begin{pmatrix} X_2 & f_2(X_2, X_1) & \dots & f_{i-1}(X_2, X_1) \\ X_3 & f_2(X_3, X_1) & \dots & f_{i-1}(X_3, X_1) \\ \vdots & \vdots & \ddots & \vdots \\ X_i & f_2(X_i, X_1) & \dots & f_{i-1}(X_i, X_1) \end{pmatrix} = 0,$$

where $\underline{g} = (f_1(x) = x, f_2(x), \dots, f_{i-1}(x))$. Note that $F_{\underline{g}}^*(X_2, \dots, X_i, X_1)$ is homogeneous, and its dehomogenized polynomial with respect to X_1 is $F_{\underline{g}}(X_2, \dots, X_i)$.

If $\underline{g} \neq (x, x^{q^M}, \dots, x^{q^{(i-2)M}})$, then by induction hypothesis $\mathcal{U}_{\underline{g}}$ has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component not contained in \mathcal{V} , and hence by Lemma 2.5 the same holds for $\mathcal{U}_{\underline{h}}$. If $\underline{g} = (x, x^{q^M}, \dots, x^{q^{(i-2)M}})$ then $f_i(x) = x^{q^{(i-1)M}}$, because $i \geq 4$ implies that the arithmetic progressions of the M_j 's and m_j 's both have ratio M .

For $i = k$, if $\underline{f} \neq (x, x^{q^M}, \dots, x^{q^{(k-2)M}})$, then \mathcal{W} has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component \mathcal{Z} not contained in \mathcal{V} . Thus, by [38, Corollary 7], \mathcal{Z} has an affine \mathbb{F}_{q^n} -rational point not on \mathcal{V} , a contradiction to Theorem 4.4. \square

4.2. Moore polynomial sets of positive index. In this section we investigate Moore polynomial sets of index $t > 0$, so that $f_1(x) = x^{q^t}$.

Proposition 4.12. *Suppose that one of the following holds:*

- $k = 3$ and $n > 4M_3 + 2$;
- $k > 3$, $q > 5$ and $n > \frac{13}{3}M_k + \log_q(13 \cdot 2^{10/3})$.

If \underline{f} is a Moore polynomial set for q and n of index t , then $(m_{\sigma(1)}, \dots, m_{\sigma(k)})$ is in arithmetic progression for some $\sigma \in S_n$.

Proof. Since $m_i = 0$ for some i , the proof is the same as in the proof of Theorem 4.6 for $t = 0$. \square

Up to reordering, we can assume that the permutation σ in Proposition 4.12 satisfies $\sigma(1) = 2$, that is, $f_2(x)$ is separable.

Proposition 4.13. *Let $\underline{f} = (f_1(x) = x^{q^t}, f_2(x), f_3(x))$ be a Moore polynomial set for q and n of index $t > 0$ such that $f_2(x)$ is separable. If $\max\{t, M_2\} < M_3$ and $n > 4M_3 + 2$, then $f_2(x) \in \mathcal{L}_{n,q}$ is scattered of index t .*

Proof. The proof is similar to the one of Theorem 4.9. Suppose that $f_2(x) \in \mathcal{L}_{n,q}$ is not scattered of index t . Then there exist $\lambda, \mu \in \mathbb{F}_{q^n}^*$ such that $\mu \notin \mathbb{F}_q$, $\lambda/\mu \notin \mathbb{F}_q$ and $f_2(\lambda)/\lambda^{q^t} = f_2(\mu)/\mu^{q^t} \neq 0$. Let $\lambda_3 = \lambda$ and define $\mathcal{D}_{\underline{f}}$ as above. Then $\mathcal{D}_{\underline{f}}$ is $\text{PGL}(3, q^n)$ -equivalent to the curve $\mathcal{D}'_{\underline{f}}$ with affine equation $H'_{\underline{f}}(X_1, X_2) = 0$, where

$$H'_{\underline{f}}(X_1, X_2) = H_{\underline{f}}(1, X_2 + 1, X_1) = -\lambda^{q^t} f_2(X_2, X_1) X_1^{q^t-1} + f_2(\lambda) X_2^{q^t} X_1^{q^{M_2}-1} + G(X_1, X_2)$$

and $G(X_1, X_2)$ has degree at least $q^t + q^{M_2}$. The tangent cone to $\mathcal{D}'_{\underline{f}}$ at $(0, 0)$ has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component with affine equation $X_2 - \mu X_1 = 0$, which corresponds to a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component of $\mathcal{D}_{\underline{f}}$ which is not contained in $\mathcal{D}_{(x, x^q, x^{q^2})}$. Arguing as in the proof of Theorem 4.9, the claim follows. \square

We now use the known classification results on exceptional scattered polynomials.

Corollary 4.14. *Let $\underline{f} = (f_1(x) = x^{q^t}, f_2(x), f_3(x))$ be a Moore polynomial set for q and n of index t such that $f_2(x)$ is separable, $\max\{t, M_2\} < M_3$, and $n > 4M_3 + 2$. Then:*

- (1) $t > 0$ and $\max\{t, M_2\}$ is not an odd prime;
- (2) if either $t = 1$, or $t = 2$ and q is odd, then $\underline{f} = (x^{q^t}, ax + x^{q^{2t}}, f_3(x))$ and $m_3 = 2t$.

Proof. Since $f_2(x)$ is separable, the case $t = 0$ cannot occur by definition. Then $f_2(x) \in \mathcal{L}_{n,q}$ is exceptional scattered of positive index t .

- (1) If $\max\{t, M_2\}$ is an odd prime, then from [15, Theorem 1.4] it follows $f_2(x) = x$, so that \underline{f} has index 0, a contradiction.
- (2) If either $t = 1$, or $t = 2$ and q is odd, then the results in [8, Page 511] and [6, Theorem 1.4 and Corollary 1.5] imply $f_2(x) = ax + x^{q^{2t}}$ with $a \neq 0$. The claim follows from Proposition 4.12. \square

Proposition 4.13 can be extended as follows.

Theorem 4.15. *Let $\underline{f} = (f_1(x) = x^{q^t}, f_2(x), \dots, f_k(x))$, with $k > 3$, be a Moore polynomial set for q and n of index $t > 0$ such that $f_2(x)$ is separable. Suppose also that $q > 5$, $\max\{t, M_2\} < M_i$ for any $i \geq 3$, and $n > \frac{13}{3} \max\{M_i : i \geq 3\} + \log_q(13 \cdot 2^{10/3})$. Then $f_2(x) \in \mathcal{L}_{n,q}$ is scattered of index t .*

Proof. It can be proved by finite induction on $i \in \{3, \dots, k\}$ that, if $\underline{h} = (x^{q^t}, f_2(x), \dots, f_i(x))$ and $f_2(x) \in \mathcal{L}_{n,q}$ is not scattered of index t , then the hypersurface $\mathcal{U}_{\underline{h}}$ has a non-repeated \mathbb{F}_{q^n} -rational absolutely irreducible component not contained in \mathcal{V} . The base $i = 3$ is in the proof of Proposition 4.13. For $i > 3$, the argument is analogous to the one in the proof of Theorem 4.11. The claim then follows again by using [38, Corollary 7]. \square

Recalling the correspondence between Moore polynomial sets and MRD codes described in Corollary 3.5, we finally obtain Main Theorem as a consequence of Theorem 4.10, Theorem 4.11, Proposition 4.13 and Theorem 4.15.

Note that, if the hypothesis of n being large enough in the aforementioned results are incorporated in the assumptions of Main Theorem, then the exceptionality of the MRD code $\mathcal{C} \subset \mathcal{L}_{n,q}$ can be dropped, as well as the exceptionality of the scattered property for $f_2(x) \in \mathcal{L}_{n,q}$.

5. KNOWN EXAMPLES OF MOORE POLYNOMIAL SETS

This section is devoted to the description of the known examples of Moore polynomial sets corresponding to inequivalent \mathbb{F}_{q^n} -linear MRD codes; see Table 1. The only known examples of exceptional Moore polynomial sets are the first two in Table 1.

Let $b: \mathcal{L}_{n,q} \times \mathcal{L}_{n,q} \rightarrow \mathbb{F}_q$ be the bilinear form given by $b(f, g) = \text{Tr}_{q^n/q} \left(\sum_{i=0}^{n-1} a_i b_i \right)$, where $\text{Tr}_{q^n/q}(x) = \sum_{i=0}^{n-1} x^{q^i}$, $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, $g(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathcal{L}_{n,q}$. The *Delsarte dual code* of a rank metric code $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ is

$$\mathcal{C}^\perp = \{f(x) \in \mathcal{L}_{n,q} : b(f, g) = 0, \text{ for all } g(x) \in \mathcal{C}\}.$$

Recall that the Delsarte dual code of an MRD code, having minimum distance greater than one, is an MRD code; see e.g. [14, 17]. This yields new examples of Moore polynomial sets; see lines 4,6,8,10,12,14 in Table 1.

Table 1: Known examples of Moore polynomial sets

n	k	$f_1(x), \dots, f_k(x)$	conditions	references
		$x, x^{q^s}, \dots, x^{q^{s(k-1)}}$	$\gcd(s, n) = 1$	[14, 17, 20]
		$x^{q^s}, \dots, x^{q^{s(k-1)}}, x + \delta x^{q^{sk}}$	$\gcd(s, n) = 1,$ $N_{q^n/q}(\delta) \neq (-1)^{nk}$	[28, 35]
$2t$	2	$x,$ $x^{q^s} + x^{q^{s(t-1)}} + \delta^{q^t+1} x^{q^{s(t+1)}} + \delta^{1-q^{2t-1}} x^{q^{s(2t-1)}}$	q odd, $N_{q^{2t}/q^t}(\delta) = -1,$ $\gcd(s, n) = 1$	[7, 24, 25, 31, 40]
$2t$	$2t - 2$	$x^{q^{st}} : i \notin \{0, 1, t-1, t+1, 2t-1\},$ $h_1(x) = x^{q^s} - x^{q^{s(t-1)}},$ $h_2(x) = \delta^{q^t+1} x^{q^s} - x^{q^{s(t+1)}},$ $h_3(x) = \delta^{1-q^{2t-1}} x^{q^s} - x^{q^{s(2t-1)}}$	q odd, $N_{q^{2t}/q^t}(\delta) = -1,$ $\gcd(s, n) = 1$	[7, 24, 25, 31, 40]
6	2	$x, x^q + \delta x^{q^4}$	$q > 4,$ certain choices of δ	[3, 11, 32]
6	4	$x^q, x^{q^2}, x^{q^4}, x - \delta^{q^5} x^{q^3}$	$q > 4,$ certain choices of δ	[3, 11, 32]
6	2	$x, x^q + x^{q^3} + \delta x^{q^5}$	q odd, $\delta^2 + \delta = 1$	[13, 29]
6	4	$x^q, x^{q^3}, x - x^{q^2}, x^{q^4} - \delta x$	q odd, $\delta^2 + \delta = 1$	[13, 29]
7	3	$x, x^{q^s}, x^{q^{3s}}$	q odd, $\gcd(s, 7) = 1$	[12]
7	4	$x, x^{q^{2s}}, x^{q^{3s}}, x^{q^{4s}}$	q odd, $\gcd(s, n) = 1$	[12]

n	k	$f_1(x), \dots, f_k(x)$	conditions	references
8	3	$x, x^{q^s}, x^{q^{3s}}$	$q \equiv 1 \pmod{3}$, $\gcd(s, 8) = 1$	[12]
8	5	$x, x^{q^{2s}}, x^{q^{3s}}, x^{q^{4s}}, x^{q^{5s}}$	$q \equiv 1 \pmod{3}$, $\gcd(s, 8) = 1$	[12]
8	2	$x, x^q + \delta x^{q^5}$	q odd, $\delta^2 = -1$	[12]
8	6	$x^q, x^{q^2}, x^{q^3}, x^{q^5}, x^{q^6}, x - \delta x^{q^4}$	q odd, $\delta^2 = -1$	[12]

6. CONCLUSIONS AND OPEN PROBLEMS

In this paper we introduce the notion of *exceptional* linear maximum rank distance codes of a given index, which naturally extends the notion of exceptionality for a scattered polynomial in the rank metric framework. We then classify those of index 0, and prove that those of positive index contain an exceptional scattered polynomial of the same index.

We list a couple of open problems related to the obtained results.

- Under the assumptions of Proposition 4.13 or Theorem 4.15, for n large enough, one may conjecture that Moore polynomial sets of positive index do not exist. Whereas, relaxing the assumption $\max\{t, M_2\} < M_i$ for every $i \geq 3$, one should include also the second example listed in Table 1, that is the one corresponding to generalized twisted Gabidulin codes. However, a new approach seems to be needed.
- A complete classification of exceptional scattered polynomials could yield to more precise results on the asymptotics of Moore polynomial sets of positive index and hence of \mathbb{F}_{q^n} -linear MRD codes in $\mathcal{L}_{n,q}$.

ACKNOWLEDGMENTS

This research was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The second author is funded by the project “Attrazione e Mobilità dei Ricercatori” Italian PON Programme (PON-AIM 2018 num. AIM1878214-2). The second and the third authors are supported by the project “VALERE: VAnviteLli pER la RicERca” of the University of Campania “Luigi Vanvitelli”.

REFERENCES

- [1] AUBRY, Y., MCGUIRE, G., AND RODIER, F. A few more functions that are not APN infinitely often. In *Finite fields: theory and applications*, vol. 518 of *Contemp. Math.* Amer. Math. Soc., Providence, RI, 2010, pp. 23–31.
- [2] BARTOLI, D. Hasse-weil type theorems and relevant classes of polynomial functions. *London Mathematical Society Lecture Note Series, Proceedings of 28th British Combinatorial Conference, Cambridge University Press* (2021), 43–102.
- [3] BARTOLI, D., CSAJBÓK, B., AND MONTANUCCI, M. On a conjecture about maximum scattered subspaces of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$. *arXiv preprint arXiv:2004.13101* (2020).
- [4] BARTOLI, D., GIULIETTI, M., AND ZINI, G. The classification of exceptional scattered polynomials of odd degree. *in preparation* (2021).
- [5] BARTOLI, D., MICHELI, G., ZINI, G., AND ZULLO, F. r -fat linearized polynomials over finite fields. *arXiv preprint arXiv:2012.15357* (2020).
- [6] BARTOLI, D., AND MONTANUCCI, M. On the classification of exceptional scattered polynomials. *J. Combin. Theory Ser. A* 179 (2021), 105386, 28.
- [7] BARTOLI, D., ZANELLA, C., AND ZULLO, F. A new family of maximum scattered linear sets in $\text{PG}(1, q^6)$. *Ars Math. Contemp.* 19, 1 (2020), 125–145.
- [8] BARTOLI, D., AND ZHOU, Y. Exceptional scattered polynomials. *J. Algebra* 509 (2018), 507–534.
- [9] BARTOLI, D., AND ZHOU, Y. Asymptotics of Moore exponent sets. *J. Combin. Theory Ser. A* 175 (2020), 105281, 18.

- [10] BLOKHUIS, A., AND LAVRAUW, M. Scattered spaces with respect to a spread in $\text{PG}(n, q)$. *Geom. Dedicata* 81, 1 (2000), 231–243.
- [11] CSAJBÓK, B., MARINO, G., POLVERINO, O., AND ZANELLA, C. A new family of MRD-codes. *Linear Algebra Appl.* 548 (2018), 203–220.
- [12] CSAJBOK, B., MARINO, G., POLVERINO, O., AND ZHOU, Y. MRD codes with maximum idealizers. *Discrete Math.* 343, 9 (2020), 111985.
- [13] CSAJBÓK, B., MARINO, G., AND ZULLO, F. New maximum scattered linear sets of the projective line. *Finite Fields Appl.* 54 (2018), 133–150.
- [14] DELSARTE, P. Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A* 25, 3 (1978), 226–241.
- [15] FERRAGUTI, A., AND MICHELI, G. Exceptional scatteredness in prime degree. *J. Algebra* 565 (2021), 691–701.
- [16] FULTON, W. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.
- [17] GABIDULIN, E. M. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii* 21, 1 (1985), 3–16.
- [18] HARTSHORNE, R. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.
- [19] JANWA, H., MCGUIRE, G. M., AND WILSON, R. M. Double-error-correcting cyclic codes and absolutely irreducible polynomials over $\text{GF}(2)$. *J. Algebra* 178, 2 (1995), 665–676.
- [20] Kshevetskiy, A., AND GABIDULIN, E. The new construction of rank codes. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005*. (2005), IEEE, pp. 2105–2108.
- [21] LEDUCQ, E. Functions which are PN on infinitely many extensions of \mathbb{F}_p , p odd. *Des. Codes Cryptogr.* 75, 2 (2015), 281–299.
- [22] LIEBHOLD, D., AND NEBE, G. Automorphism groups of Gabidulin-like codes. *Arch. Math.* 107, 4 (2016), 355–366.
- [23] LOIDREAU, P. A new rank metric codes based encryption scheme. In *Post-quantum cryptography*, vol. 10346 of *Lecture Notes in Comput. Sci.* Springer, Cham, 2017, pp. 3–17.
- [24] LONGOBARDI, G., MARINO, G., TROMBETTI, R., AND ZHOU, Y. A large family of maximum scattered linear sets of $\text{PG}(1, q^n)$ and their associated MRD codes. *arXiv preprint arXiv:2102.08287* (2021).
- [25] LONGOBARDI, G., AND ZANELLA, C. Linear sets and MRD-codes arising from a class of scattered linearized polynomials. *J. Algebraic Combin.* (2021), 1–23.
- [26] LUNARDON, G., AND POLVERINO, O. Blocking sets of size $q^t + q^{t-1} + 1$. *J. Combin. Theory Ser. A* 90, 1 (2000), 148–158.
- [27] LUNARDON, G., TROMBETTI, R., AND ZHOU, Y. On kernels and nuclei of rank metric codes. *J. Algebraic Combin.* 46 (2017), 313–340.
- [28] LUNARDON, G., TROMBETTI, R., AND ZHOU, Y. Generalized twisted gabidulin codes. *J. Combin. Theory Ser. A* 159 (2018), 79–106.
- [29] MARINO, G., MONTANUCCI, M., AND ZULLO, F. MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$. *Linear Algebra Appl.* 591 (2020), 99–114.
- [30] MULLEN, G. L., AND PANARIO, D. *Handbook of finite fields*. CRC Press, 2013.
- [31] NERI, A., SANTONASTASO, P., AND ZULLO, F. Extending two families of maximum rank distance codes. *arXiv preprint arXiv:2104.07602* (2021).
- [32] POLVERINO, O., AND ZULLO, F. On the number of roots of some linearized polynomials. *Linear Algebra Appl.* 601 (2020), 189–218.
- [33] RAVAGNANI, A. Rank-metric codes and their duality theory. *Designs, Codes and Cryptography* 80, 1 (2016), 197–216.
- [34] SCHMIDT, K.-U., AND ZHOU, Y. Planar functions over fields of characteristic two. *J. Algebraic Combin.* 40, 2 (2014), 503–526.
- [35] SHEEKEY, J. A new family of linear maximum rank distance codes. *Adv. Math. Commun.* 10, 3 (2016), 475–488.
- [36] SHEEKEY, J. MRD codes: constructions and connections. *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications* 23 (2019).
- [37] SILVA, D., KSCHISCHANG, F. R., AND KÖTTER, R. A rank-metric approach to error control in random network coding. *IEEE Trans. Inform. Theory* 54, 9 (2008), 3951–3967.
- [38] SLAVOV, K. An application of random plane slicing to counting \mathbb{F}_q -points on hypersurfaces. *Finite Fields and Their Applications* 48 (2017), 60–67.
- [39] ZANELLA, C. A condition for scattered linearized polynomials involving Dickson matrices. *J. Geom.* 110, 3 (2019), 1–9.

- [40] ZANELLA, C., AND ZULLO, F. Vertex properties of maximum scattered linear sets of $PG(1, q^n)$. *Discrete Math.* 343, 5 (2020), 111800.

DANIELE BARTOLI, Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia, Italy
Email address: `daniele.bartoli@unipg.it`

GIOVANNI ZINI, FERDINANDO ZULLO, Dipartimento di Matematica e Fisica, Università degli Studi della Campania
"Luigi Vanvitelli", Viale Lincoln, 5, I-81100 Caserta, Italy
Email address: `{giovanni.zini,ferdinando.zullo}@unicampania.it`