MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5}$ $F_{q^6}[x]$

Marino, Giuseppe; Montanucci, Maria; Zullo, Ferdinando

Published in:
Linear Algebra and Its Applications

Link to article, DOI:
[10.1016/j.laa.2020.01.004](https://doi.org/10.1016/j.laa.2020.01.004)

Publication date:
2020

Document Version
Peer reviewed version

[Link back to DTU Orbit](#)

Citation (APA):
Marino, G., Montanucci, M., & Zullo, F. (2020). MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5}$ $F_{q^6}[x]$. *Linear Algebra and Its Applications*, 591, 99-114. <https://doi.org/10.1016/j.laa.2020.01.004>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

MRD-codes arising from the trinomial

$$x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$$

Giuseppe Marino, Maria Montanucci and Ferdinando Zullo

December 16, 2019

Abstract

In [10], the existence of $\mathbb{F}_q$ -linear MRD-codes of $\mathbb{F}_q^{6 \times 6}$, with dimension 12, minimum distance 5 and left idealiser isomorphic to $\mathbb{F}_{q^6}$, defined by a trinomial of $\mathbb{F}_{q^6}[x]$, when q is odd and $q \equiv 0, \pm 1 \pmod{5}$, has been proved. In this paper we show that this family produces $\mathbb{F}_q$ -linear MRD-codes of $\mathbb{F}_q^{6 \times 6}$, with the same properties, also in the remaining q odd cases, but not in the q even case. These MRD-codes are not equivalent to the previously known MRD-codes. We also prove that the corresponding maximum scattered $\mathbb{F}_q$ -linear sets of $\text{PG}(1, q^6)$ are not $\text{PGL}(2, q^6)$ -equivalent to any previously known linear set.

AMS subject classification: 51E20, 05B25, 51E22

Keywords: Scattered subspace, MRD-code, Linear set

1 Introduction and preliminary results

Let $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) := \text{Hom}_q(\mathbb{F}_{q^n}, \mathbb{F}_{q^n})$ be the set of all $\mathbb{F}_q$ -linear maps of $\mathbb{F}_{q^n}$ in itself. It is well-known that each element f of $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ can be represented in a unique way as a q -polynomial over $\mathbb{F}_{q^n}$ of degree less than or equal to $q^n - 1$, that is $f(x) = \sum_{i=0}^{q^n-1} a_i x^{q^i}$, with coefficients in $\mathbb{F}_{q^n}$. Such polynomials are also called *linearized*. The set of q -polynomials over $\mathbb{F}_{q^n}$, say $\mathcal{L}_{n,q}$, considered modulo $(x^{q^n} - x)$, and endowed with the addition and composition of polynomials in $\mathbb{F}_{q^n}$ and scalar multiplication by elements in $\mathbb{F}_q$, forms an

$\mathbb{F}_q$ -subalgebra of the algebra of $\mathbb{F}_q$ -linear transformations of $\mathbb{F}_{q^n}$. Hence, we can define the *kernel* of f as the kernel of the corresponding $\mathbb{F}_q$ -linear transformation of $\mathbb{F}_{q^n}$, which is the same as the set of roots of f in $\mathbb{F}_{q^n}$; and the *rank* of f as the rank of the corresponding $\mathbb{F}_q$ -linear transformation of $\mathbb{F}_{q^n}$. For $f \in \mathcal{L}_{n,q}$ with $\deg f = q^k$, we call k the *q-degree* of f and we denote it by $\deg_q f$. It is clear that in this case the kernel of f has dimension at most k and the rank of f is at least $n - k$.

In [8], the q -polynomials f such that $\dim_{\mathbb{F}_q} \ker f = \deg_q f$ are called *q-polynomials with maximum kernel*. Also in [8, Theorem 1.2], sufficient and necessary conditions for the coefficients of a q -polynomial f over $\mathbb{F}_{q^n}$ ensuring f has maximum kernel are given (see also [28]).

The set $\mathbb{F}_q^{m \times n}$ of all $m \times n$ matrices over $\mathbb{F}_q$ is a rank metric $\mathbb{F}_q$ -space with the *rank metric* or the *rank distance* defined by

$$d(A, B) = \text{rank}(A - B),$$

for any $A, B \in \mathbb{F}_q^{m \times n}$. A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ with respect to the rank metric is usually called a *rank-metric code* or a *rank-distance code* (or *RD-code* for short). When $\mathcal{C}$ contains at least two elements, the *minimum distance* of $\mathcal{C}$ is given by

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

When $\mathcal{C}$ is an $\mathbb{F}_q$ -linear subspace of $\mathbb{F}_q^{m \times n}$, we say that $\mathcal{C}$ is an $\mathbb{F}_q$ -linear code and its dimension $\dim_{\mathbb{F}_q}(\mathcal{C})$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$. For any $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$ with $d(\mathcal{C}) = d$, it is well-known that

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

which is a Singleton like bound for the rank metric ([14]). When equality holds, we call $\mathcal{C}$ a *maximum rank-distance* (MRD for short) code.

In this paper we only consider $\mathbb{F}_q$ -linear RD and MRD-codes with $m = n$.

Two $\mathbb{F}_q$ -linear rank-distance codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{F}_q^{n \times n}$ are *equivalent* if there exist $A, B \in \text{GL}(n, q)$ and $\rho \in \text{Aut}(\mathbb{F}_q)$ such that $\mathcal{C}_2 = \{AM^\rho B : M \in \mathcal{C}_1\}$.

In general, it is a difficult task to tell whether two given rank-distance codes are equivalent or not. The idealizers of an RD-code are useful invariants which may help us to distinguish them (see [23, 27, 17]). Given an $\mathbb{F}_q$ -linear rank-distance code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times n}$, following [23] its *left* and *right idealisers* are defined as

$$L(\mathcal{C}) = \{M \in \mathbb{F}_q^{n \times n} : MC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\},$$

and

$$R(\mathcal{C}) = \{M \in \mathbb{F}_q^{n \times n} : CM \in \mathcal{C} \text{ for all } C \in \mathcal{C}\},$$

respectively.

The *adjoint* of an $\mathbb{F}_q$ -linear RD-code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times n}$ is the $\mathbb{F}_q$ -linear code

$$\mathcal{C}^\top := \{C^T \in \mathbb{F}_q^{n \times n} : C \in \mathcal{C}\},$$

where $(\cdot)^T$ denotes the transpose operation. Note that the adjoint operation also preserves rank distance, implying that an $\mathbb{F}_q$ -linear RD-code and its adjoint have the same minimum distance. Also $L(\mathcal{C}) = R(\mathcal{C}^\top)$ and $R(\mathcal{C}) = L(\mathcal{C})$ ([27, Prop. 4.2]).

The *Delsarte dual code* of an $\mathbb{F}_q$ -linear code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times n}$ is

$$\mathcal{C}^\perp := \{M \in \mathbb{F}_q^{n \times n} : \text{Tr}(MN^T) = 0 \text{ for all } N \in \mathcal{C}\},$$

where $(\cdot)^T$ denotes the transpose operation. If $\mathcal{C}$ is a linear MRD-code then $\mathcal{C}^\perp$ is also a linear MRD-code as it was proved by Delsarte [14]. Also from [14], if $\mathcal{C}$ is an $\mathbb{F}_q$ -linear code $\mathcal{C} \subseteq \mathbb{F}_q^{n \times n}$ with dimension k and minimum distance d , then $\mathcal{C}^\perp$ has dimension $n(n - k)$ and minimum distance $k + 1$.

It is well-known that two linear rank-distance codes are equivalent if and only if their adjoint codes (or their Delsarte duals) are equivalent.

Two MRD-codes in $\mathbb{F}_q^{n \times n}$ with minimum distance n are equivalent if and only if the corresponding semifields are isotopic [22, Theorem 7]. In contrast, it appears to be difficult to obtain inequivalent MRD-codes in $\mathbb{F}_q^{n \times n}$ with minimum distance strictly less than n . So far, the known inequivalent MRD-codes in $\mathbb{F}_q^{n \times n}$ of minimum distance strictly less than n , can be divided into two types.

1. The first type of constructions consists of MRD-codes of minimum distance d for arbitrary $2 \leq d \leq n$.
 - The first construction of MRD-codes was given by Delsarte [14] and rediscovered independently by Gabidulin [16]. This construction was generalized by Kshevetskiy and Gabidulin [20] with the nowadays commonly called (generalized) Gabidulin codes. In 2016, Sheekey [32] found the so-called (generalized) twisted Gabidulin codes. They can be generalized into additive MRD-codes [29]. Very recently, by using skew polynomial rings Sheekey [33] proved that they can be further generalized into a quite large family and all the MRD-codes mentioned above can be obtained in this way.

- The non-additive family constructed by Otal and Özbudak in [30].
 - The family appeared in [35].
2. The second type of constructions provides us MRD-codes of minimum distance $d = n - 1$.
- Non-linear MRD-codes by Cossidente, the second author and Pavese [13] which were later generalized by Durante and Siciliano [15].
 - Linear MRD-codes associated with maximum scattered linear sets of $\text{PG}(1, q^6)$ and $\text{PG}(1, q^8)$ presented in [6] and [10].

Very recently, new MRD-codes of minimum distance $d = n - 2$ and $n \in \{7, 8\}$ have been constructed in [5].

For the relationship between MRD-codes and other geometric objects such as linear sets and Segre varieties, we refer to [24] and also to [34].

Since the metric space $\mathbb{F}_q^{n \times n}$ is isomorphic to the metric space $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ with rank distance defined as $d(f, g) := \text{rk}(f - g)$, taking into account the previous algebra isomorphism between $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$ and $\mathcal{L}_{n,q}$, it is clear that each $\mathbb{F}_q$ -linear RD-code $\mathcal{C}$ can be regarded as an $\mathbb{F}_q$ -vector subspace of $\mathcal{L}_{n,q}$. Hence, in terms of linearized polynomial, an RD-code of $\mathbb{F}_q^{n \times n}$, with minimum distance d , is an $\mathbb{F}_q$ -subspace of $\mathcal{L}_{n,q}$ and $d := \min\{d(f, g) : f, g \in \mathcal{C}, f \neq g\}$. Also two given $\mathbb{F}_q$ -linear MRD-codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if and only if there exist $\varphi_1, \varphi_2 \in \mathcal{L}_{n,q}$ permuting $\mathbb{F}_{q^n}$ and $\rho \in \text{Aut}(\mathbb{F}_q)$ such that

$$\varphi_1 \circ f^\rho \circ \varphi_2 \in \mathcal{C}_2 \text{ for all } f \in \mathcal{C}_1,$$

where $\circ$ stands for the composition of maps and $f^\rho(x) = \sum a_i^\rho x^{q^i}$ for $f(x) = \sum a_i x^{q^i}$. For a rank distance code $\mathcal{C}$ given by a set of linearized polynomials, its left and right idealisers can be written as

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

and

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

respectively.

Consider the non-degenerate symmetric bilinear form of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ defined by $\langle x, y \rangle = \text{Tr}_{q^n/q}(xy)$, for each $x, y \in \mathbb{F}_{q^n}$. Then the *adjoint* $\hat{f}$ of the linearized polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathcal{L}_{n,q}$ with respect to the bilinear

form $\langle, \rangle$ is $\hat{f}(x) = \sum_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}$. We will refer to $\hat{f}$ simply as the adjoint of f , omitting the bilinear form involved. Hence, we may define the adjoint of a rank distance code $\mathcal{C}$ given by a set of linearized polynomials as follows $\mathcal{C}^\top := \{\hat{f} : f \in \mathcal{C}\}$.

In [10], the authors proved that the set $\mathcal{C} = \langle x, x^q + x^{q^3} + cx^{q^5} \rangle_{\mathbb{F}_{q^6}}$, q odd, $c^2 + c = 1$, $q \equiv 0, \pm 1 \pmod{5}$ is an $\mathbb{F}_q$ -linear MRD-code of $\mathcal{L}_{6,q}$ of dimension 12, minimum distance 5 and left idealiser isomorphic to $\mathbb{F}_{q^6}$. The right idealiser of $\mathcal{C}$ is isomorphic to $\mathbb{F}_{q^2}$ ([36, Appendix B]). In this paper we further investigate the set $\mathcal{C}$ with the same assumption $c^2 + c = 1$ and for each value of q (odd and even), obtaining the following result.

Theorem 1.1. *The set of q -polynomials of $\mathcal{L}_{6,q}$*

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

with $c^2 + c = 1$, is an $\mathbb{F}_q$ -linear MRD-code of $\mathcal{L}_{6,q}$ with dimension 12, minimum distance 5, left idealiser isomorphic to $\mathbb{F}_{q^6}$ and right idealiser isomorphic to $\mathbb{F}_{q^2}$, if and only if q is odd. Moreover, when q is odd and $q \equiv \pm 2 \pmod{5}$, $\mathcal{C}$ is not equivalent to the previously known MRD-codes.

Since both the adjoint and the Delsarte dual operations preserve the equivalence of MRD-codes, we have also that the MRD-codes presented in Theorem 1.1 are not equivalent neither to the adjoint nor to the Delsarte dual of any previously known MRD-code.

2 $\mathbb{F}_q$ -linear MRD-codes and maximum scattered $\mathbb{F}_q$ -subspaces

An $\mathbb{F}_q$ -subspace U of rank n of a 2-dimensional $\mathbb{F}_{q^n}$ -space V is *maximum scattered* if it defines a scattered $\mathbb{F}_q$ -linear set of the projective line $\text{PG}(V, \mathbb{F}_{q^n})$, i.e. $\dim_{\mathbb{F}_q}(U \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}) \leq 1$ for each $\mathbf{v} \in V \setminus \{\mathbf{0}\}$. Let $V = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, up to the action of the group $\text{GL}(2, q^n)$, an $\mathbb{F}_q$ -subspace U of V of rank n can be written as $U = U_f = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\}$, for some $f \in \mathcal{L}_{n,q}$.

Sheekey in [32] made a breakthrough in the construction of new linear MRD-codes using linearized polynomials (see also [26]).

In [32], the author proved the following result (which have been generalized in [24, Section 2.7] and [34], see also [9, Result 4.7]).

Result 2.1. $\mathcal{C}$ is an $\mathbb{F}_q$ -linear MRD-code of $\mathcal{L}_{n,q}$ with minimum distance $n-1$ and with left-idealiser isomorphic to $\mathbb{F}_{q^n}$ if and only if up to equivalence

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

for some $f \in \mathcal{L}_{n,q}$ and the $\mathbb{F}_q$ -subspace

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

is a maximum scattered $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$.

Also, two $\mathbb{F}_q$ -linear MRD-codes $\mathcal{C}$ and $\mathcal{C}'$ of $\mathcal{L}_{n,q}$, with minimum distance $n-1$ and with left idealisers isomorphic to $\mathbb{F}_{q^n}$, are equivalent if and only if $U_{\mathcal{C}}$ and $U_{\mathcal{C}'}$ are $\Gamma\mathrm{L}(2, q^n)$ -equivalent.

So far, the known non-equivalent (under $\Gamma\mathrm{L}(2, q^n)$) maximum scattered $\mathbb{F}_q$ -subspaces, yielding to the known non-equivalent $\mathbb{F}_q$ -linear MRD-codes with left idealiser isomorphic to $\mathbb{F}_{q^n}$, are

1. $U_s^{1,n} := \{(x, x^{q^s}) : x \in \mathbb{F}_{q^n}\}$, $1 \leq s \leq n-1$, $\gcd(s, n) = 1$, see [1, 12];
2. $U_{s,\delta}^{2,n} := \{(x, \delta x^{q^s} + x^{q^{n-s}}) : x \in \mathbb{F}_{q^n}\}$, $n \geq 4$, $N_{q^n/q}(\delta) \notin \{0, 1\}$ ¹, $\gcd(s, n) = 1$, see [25] for $s = 1$, [32, 26] for $s \neq 1$;
3. $U_{s,\delta}^{3,n} := \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) : x \in \mathbb{F}_{q^n}\}$, $n \in \{6, 8\}$, $\gcd(s, n/2) = 1$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$, for the precise conditions on δ and q see [6, Theorems 7.1 and 7.2]²;
4. $U_c^4 := \{(x, x^q + x^{q^3} + cx^{q^5}) : x \in \mathbb{F}_{q^6}\}$, q odd, $c^2 + c = 1$, $q \equiv 0, \pm 1 \pmod{5}$, see [10].

In this paper, we further investigate the $\mathbb{F}_q$ -subspaces U_f arising from the trinomial

$$f(x) = x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x],$$

with the same assumption $c^2 + c = 1$ and for each value of q (odd and even), showing that the $\mathbb{F}_q$ -subspace U_f of $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ is maximum scattered also for q odd and $q \equiv \pm 2 \pmod{5}$, whereas it is not scattered for q even.

To do this, as we will see in Section 4, studying the Delsarte dual of the code arising from U_f was successful.

¹This condition implies $q \neq 2$.

²Also here $q > 2$, otherwise $L_{s,\delta}^{3,n}$ is not scattered.

3 The Delsarte dual of an RD-code

In terms of linearized polynomials, the Delsarte dual of a rank distance code $\mathcal{C}$ of $\mathcal{L}_{n,q}$ can be interpreted as follows

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

where $b(f, g) = \text{Tr}_{q^n/q}(\sum_{i=0}^{n-1} a_i b_i)$ for $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, $g(x) = \sum_{i=0}^{n-1} b_i x^{q^i} \in \mathbb{F}_{q^n}[x]$ and $\text{Tr}_{q^n/q}$ denotes the trace function from $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

The following result has been proved in [14].

Result 3.1. *Let $\mathcal{C}$ be an $\mathbb{F}_q$ -linear RD-code of $\mathcal{L}_{n,q}$. Then $\mathcal{C}$ is an $\mathbb{F}_q$ -linear MRD-code if and only if $\mathcal{C}^\perp$ is an $\mathbb{F}_q$ -linear MRD-code.*

Let us consider the set of $\mathcal{L}_{6,q}$

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

with $c^2 + c = 1$. By [10, Theorem 5.1 and Proposition 6.1], $\mathcal{C}$ is an $\mathbb{F}_q$ -linear MRD-code of $\mathcal{L}_{6,q}$ with dimension 12, minimum distance 5, left idealiser isomorphic to $\mathbb{F}_{q^6}$ and right idealiser isomorphic to $\mathbb{F}_{q^2}$ when q is odd and $q \equiv 0, \pm 1 \pmod{5}$.

In order to investigate the remaining cases, by Result 3.1, we can consider the Delsarte dual RD-code of $\mathcal{C}$, which is equivalent to

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

Our aim is now to establish under which conditions the RD-code

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

is an MRD-code³.

The $\mathbb{F}_q$ -linear RD-code $\mathcal{D}$ is an MRD if and only if for each nonzero element $f \in \mathcal{D}$ we get $\dim_{\mathbb{F}_q} \ker f \leq 3$. Since the maximum q -degree of the polynomials in $\mathcal{D}$ is 4 it suffices that do not exist α, β and γ in $\mathbb{F}_{q^6}$ such that the kernel of

$$f(x) = \alpha x^q + \beta x^{q^3} + \gamma(-x + x^{q^2}) + cx - x^{q^4} =$$

³We write c instead of c^q , since c^q satisfies $x^2 + x = 1$.

$$= (-\gamma + c)x + \alpha x^q + \gamma x^{q^2} + \beta x^{q^3} - x^{q^4}$$

has dimension 4. Taking into account the characterization of maximum kernel q -polynomials when $k = 4$ and $n = 6$ (cf. [8, Section 3.4]) we have the following result.

Proposition 3.2. *The set of q -polynomials*

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

with $c^2 + c = 1$ is an $\mathbb{F}_q$ -linear MRD-code of $\mathcal{L}_{6,q}$ with dimension 12, minimum distance 5 and left idealiser isomorphic to $\mathbb{F}_{q^6}$, if and only if the system

$$\begin{cases} \alpha \neq 0 \\ (-\gamma + c)^{\frac{q^6-1}{q-1}} = 1 \\ (-\gamma + c)[(-\gamma + c)^{q^4+q^2} + \beta^{q^5+q^4}(-\gamma + c)^{q^4+q^3+q^2} + \beta^{q^2+q}] = 1 \\ \alpha = -(-\gamma + c)^{q+1}\beta^{q^2} \\ \gamma = -(-\gamma + c)^{q^2+1} + \beta^{q^3+q^2}(-\gamma + c)^{q^2+q+1} \\ \beta = (-\gamma + c)^{q^3+q^2+1}\beta^{q^4} + \beta^{q^2}(-\gamma + c)^{q^3+q+1} - \beta^{q^4+q^3+q^2}(-\gamma + c)^{q^3+q^2+q+1} \end{cases} \quad (1)$$

has no solutions α, β and γ in $\mathbb{F}_{q^6}$.

In the next section we will study System (1) when q is odd, $q \equiv \pm 2 \pmod{5}$ and when q is even separately.

4 Proof of Theorem 1.1

In this section we prove the main theorem of the paper, showing that System (1) has solutions in $\mathbb{F}_{q^6}$ if and only if q is even. By Result 3.1, taking [10, Theorem 5.1 and Proposition 6.1] into account, System (1) has no solutions α, β and γ in $\mathbb{F}_{q^6}$ when $q \equiv 0, \pm 1 \pmod{5}$. Hence, we have to investigate the remaining cases. The resultants presented in this section have been obtained by using the software package MAGMA [2].

4.1 The q odd case, $q \equiv \pm 2 \pmod{5}$

From [19, Section 1.5 (xiv)] it follows that $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, and so c and c^q are the two distinct roots of $x^2 + x - 1$. Also $c^{q+1} = c + c^q = -1$.

Our aim now is to show that the system

$$\begin{cases} (-\gamma + c)[-(-\gamma + c)^{q^4+q^2} + \beta^{q^5+q^4}(-\gamma + c)^{q^4+q^3+q^2} + \beta^{q^2+q}] = 1 \\ \gamma = -(-\gamma + c)^{q^2+1} + \beta^{q^3+q^2}(-\gamma + c)^{q^2+q+1} \end{cases} \quad (2)$$

has no solutions in the variables γ and β over $\mathbb{F}_{q^6}$ and as a consequence System (1) does not have solutions. It is straightforward to see that the previous system admits solutions if and only if the following system

$$\begin{cases} \gamma = -\gamma^{q^3}(-\gamma + c)^{q^2+q+1} \\ \left(\frac{1}{-\gamma+c} - \gamma^{q^2}\right)^{\frac{q^6-1}{q+1}} = 1 \end{cases} \quad (3)$$

admits $\mathbb{F}_{q^6}$ -rational solutions in the variable γ . Clearly, System (2) may be written as

$$\begin{cases} (-\gamma^{q-1}(-\gamma + c))^{q^2+q+1} = 1 \\ \left(\frac{1}{-\gamma+c} - \gamma^{q^2}\right)^{\frac{q^6-1}{q+1}} = 1. \end{cases} \quad (4)$$

The following preliminary result holds.

Proposition 4.1. *If x is a solution of System (4), then*

$$x = \frac{2}{\lambda^{q^2+q}(c+2) - \lambda^{q^2}c + c},$$

for some $\lambda \in \mathbb{F}_{q^3}^*$ such that $\lambda^{q^2+q+1} = 1$.

Proof. By the second equation of (4) it follows that $x \neq 0$ and

$$\frac{1}{-x+c} - x^{q^2}$$

is a $(q+1)$ -th power in $\mathbb{F}_{q^6}^*$. Therefore, there exists $y \in \mathbb{F}_{q^6}^*$ such that

$$y^{q+1} = \frac{1}{-x+c} - x^{q^2}, \quad (5)$$

and hence

$$-x+c = \frac{1}{y^{q+1} + x^{q^2}}.$$

The first equation of (4) reads

$$\left(-\frac{x^{q-1}}{y^{q+1} + x^{q^2}}\right)^{q^2+q+1} = 1.$$

Hence, this is equivalent to the existence of $\lambda \in \mathbb{F}_{q^3}^*$ with $\lambda^{q^2+q+1} = 1$ and

$$-\lambda x^{q-1} = y^{q+1} + x^{q^2}. \quad (6)$$

By Equations (5) and (6) we have

$$-x^{q^2} - \lambda x^{q-1} = \frac{1}{-x + c} - x^{q^2},$$

and hence

$$\frac{1}{\lambda} \left(\frac{1}{x}\right)^q + c \frac{1}{x} - 1 = 0.$$

Denoting $T := \frac{1}{x}$, the above equation becomes

$$T^q + c\lambda T - \lambda = 0. \quad (7)$$

By [19, Theorem 1.22], since

$$(-\lambda c)^{q^5+q^4+q^3+q^2+q+1} = \lambda^{(q^2+q+1)(q^3+1)} c^{3(q+1)} = -1 \neq 1,$$

Equation (7) has one solution and it is

$$\begin{aligned} \bar{T} := & \lambda(-\lambda c)^{q^5+q^4+q^3+q^2+q} + \lambda^q(-\lambda c)^{q^5+q^4+q^3+q^2} + \\ & + \lambda^{q^2}(-\lambda c)^{q^5+q^4+q^3} + \lambda^{q^3}(-\lambda c)^{q^5+q^4} \lambda^{q^4}(-\lambda c)^{q^5} + \lambda^{q^5}. \end{aligned}$$

Since $\lambda \in \mathbb{F}_{q^3}^*$ and $c^2 + c - 1 = 0$ we have

$$\bar{T} = \frac{c + \lambda^{q^2+q}(c+2) - c\lambda^{q^2}}{2}$$

and the assertion follows. $\square$

By way of contradiction, suppose that System (3) admits at least one solution in γ , say x . Hence x is as in Proposition 4.1 and the variables of System (4) are λ and c . In particular the first equation becomes $\lambda^{q^2+q+1} = 1$.

Our aim is to show that a solution λ of the new system obtained in this way does not exist.

Looking at each q -power of λ as a distinct variable, we define

$$L := \lambda, M := \lambda^q, N := \lambda^{q^2}, C := c$$

and consider the Frobenius images λ^{q^i} , with $i = 0, 1, 2$ as variables in System (4). Hence, we have a weaker system, say Σ , in the variables L, M, N, C . We want to show that System Σ has no solutions over $\mathbb{F}_{q^6}$. Denote by $EQ1$ and by $NEQ2$ the first equation and the numerator of the system Σ , respectively. Hence

$$EQ1 := LMN - 1 = 0.$$

We have that

$$\begin{aligned} \text{Resultant}(\text{Resultant}(NEQ2, C^2 + C - 1, C), EQ1, L) = \\ = 2^{14} N^8 \cdot M^{12} \cdot \text{COND1}^2 \cdot \text{COND2}^2 \cdot \text{COND3}^2, \end{aligned}$$

where

$$\text{COND1} := M^2 N^2 - 2MN^2 - 4MN + N^2 + 4N - 1,$$

$$\text{COND2} := M^2 N^2 + 4MN^2 - 4MN - N^2 + 2N - 1,$$

and

$$\text{COND3} := M^2 N^2 + 4MN^2 - 2MN - N^2 - 4N + 1.$$

Hence, three cases occur.

- $\text{COND1} = 0$.

Let $Z := NM - N$, we get

$$Z^2 - 4Z - 1 = 0,$$

which implies $Z \in \mathbb{F}_q$ since $\lambda \in \mathbb{F}_{q^3}$. Therefore $Z - Z^q = 0$ and hence the following two resultants should be zero

$$R1 := \text{Resultant}(Z - Z^q, EQ1, N) = 0$$

and

$$R2 := \text{Resultant}(\text{COND1}, EQ1, N) = 0.$$

Also,

$$\text{Resultant}(R1, R2, M) = 4L^2(L^2 - L - 1) = 0,$$

i.e. $\lambda \in \mathbb{F}_{q^2} \cap \mathbb{F}_{q^3} = \mathbb{F}_q$, which implies $\lambda^3 = 1$. This means that either $\lambda = 1$ or $q \equiv 1 \pmod{3}$ and $\lambda^2 + \lambda + 1 = 0$. But both cases contradict condition $\lambda^2 - \lambda - 1 = 0$.

- COND2 = 0.

In this case the following resultants should be zero

$$Q1 := \text{Resultant}(\text{COND2}, EQ1, N) = 0$$

and

$$Q2 := \text{Resultant}(\text{COND2}^q, EQ1, N) = 0.$$

This implies that

$$\text{Resultant}(Q1, Q2, Lq) = 2^4 L^6 (L^2 + 5L - 5) = 0.$$

Again $\lambda \in \mathbb{F}_q$ and we get a contradiction when $q \equiv \pm 2 \pmod{5}$.

- COND3 = 0.

Then

$$S1 := \text{Resultant}(\text{COND3}, EQ1, N) = 0$$

and

$$S2 := \text{Resultant}(\text{COND3}, EQ1, N) = 0,$$

and then

$$\text{Resultant}(S1, S2, Lq) = 2^4 L^4 (5L^2 - 5L + 1) = 0,$$

again a contradiction.

The proof is now complete.

4.2 The q even case

Differently from what happens in the case q odd, we want to show that, when q is even, System (1) admits at least a solution of type $(\alpha, \beta, 0) \in \mathbb{F}_{q^6}^3$, with α and β not zero. Indeed, substituting the value $\gamma = 0$ in System (1) we get

$$\begin{cases} \alpha \neq 0 \\ c^{\frac{q^6-1}{q-1}} = 1 \\ c[c^{q^4+q^2} + \beta^{q^5+q^4} c^{q^4+q^3+q^2} + \beta^{q^2+q}] = 1 \\ \alpha = c^{q+1} \beta^{q^2} \\ 0 = c^{q^2+1} + \beta^{q^3+q^2} c^{q^2+q+1} \\ \beta = c^{q^3+q^2+1} \beta^{q^4} + \beta^{q^2} c^{q^3+q+1} + \beta^{q^4+q^3+q^2} c^{q^3+q^2+q+1} \end{cases} \quad (8)$$

Note that the conditions on α will be automatically satisfied once we define $\alpha := c^{q+1} \beta^{q^2}$ forcing $\beta \neq 0$. Also, the second equation is trivially satisfied since $c \in \mathbb{F}_4^*$ and $c \in \mathbb{F}_{q^2}$. Hence System (8) has solutions if and only if the following system admits solutions

$$\begin{cases} c[c^{q^4+q^2} + \beta^{q^5+q^4} c^{q^4+q^3+q^2} + \beta^{q^2+q}] = 1 \\ 1 = \beta^{q^3+q^2} c^q \\ \beta = c^{q+2} \beta^{q^4} + \beta^{q^2} c^{2q+1} + \beta^{q^4+q^3+q^2} c^{2(q+1)} \end{cases} \quad (9)$$

Since $c^2 + c + 1 = 0$, then $c \in \mathbb{F}_{q^2}$ and $c^3 = 1$. Then there exists $\beta \in \mathbb{F}_{q^6}$ such that $\beta^{q+1} = 1/c^q$. Hence $\beta^{q^3+q^2} = (1/c^q)^{q^2} = 1/c^q$ and the second equation of (9) is satisfied. Also, the first equation of System (9) reads

$$1 = c \left[c^2 + \frac{1}{c^q} c^{q+2} + \frac{1}{c} \right],$$

and hence it is fulfilled. At this point the third equation of (9) becomes

$$1 = c^{q+2} \beta^{q^4-1} + c^{2q+1} \beta^{q^2-1} + \beta^{q^4+q^3+q^2-1} c^{2(q+1)},$$

and using that $\beta^{q+1} = 1/c^q$ and $c^3 = 1$, we get that it is satisfied.

4.3 The right idealiser of RD-codes of Theorem 1.1

Following the computations in [36, Appendix B]), we show that the right idealiser of the RD-codes presented in Theorem 1.1 is isomorphic to $\mathbb{F}_{q^2}$. Indeed, let $\varphi(x)$ be an element of $R(\mathcal{C})$. Since $\mathcal{C}$ contains the identity map $\varphi(x) \in \mathcal{C}$ and hence there exist $\alpha, \beta \in \mathbb{F}_{q^6}$ such that $\varphi(x) = \alpha x + \beta x^q + \beta x^{q^3} + \beta c x^{q^5}$. Also,

$$(x^q + x^{q^3} + c x^{q^5}) \circ \varphi(x) = \varphi(x)^q + \varphi(x)^{q^3} + c \varphi(x)^{q^5} \in \mathcal{C}$$

implying the existence of $a, b \in \mathbb{F}_{q^6}$ such that

$$\begin{aligned} & \alpha^q x^q + \beta^q (x^{q^2} + x^{q^4} + c^q x) + \alpha^{q^3} x^{q^3} + \beta^{q^3} (x^{q^4} + x + c^{q^3} x^{q^2}) \\ & + c(\alpha^{q^5} x^{q^5} + \beta^{q^5} (x + x^{q^2} + c^{q^5} x^{q^4})) = ax + b(x^q + x^{q^3} + cx^{q^5}), \end{aligned}$$

which is a polynomial identity in x . By comparing the coefficients of terms of degree q and q^3 we get $\alpha \in \mathbb{F}_{q^2}$, and by comparing the coefficients of the terms of degree q^2 and q^4 , taking into account that $c \in \mathbb{F}_{q^2}$, we get

$$\beta^q + c^q \beta^{q^3} + c \beta^{q^5} = 0 \text{ and } \beta^q + \beta^{q^3} + c^{q+1} \beta^{q^5} = 0.$$

Subtracting the second equation to the first one, we get $(c^q - 1)(\beta^{q^3} - c \beta^{q^5}) = 0$. Since $c \neq 1$, then $\beta^{q^4} = c^q \beta$ and this equation admits a nonzero solution $\beta \in \mathbb{F}_{q^6}$ if and only if $c^3 = 1$, contradicting the condition $c^2 + c - 1 = 0$.

4.4 The equivalence issue

We want to finish this part of the paper showing that the $\mathbb{F}_q$ -linear MRD-codes of $\mathcal{L}_{6,q}$ defined in Theorem 1.1 are not equivalent to the previously known MRD-codes.

From [6, Section 6] and [10, Theorem 6.1], the previously known $\mathbb{F}_q$ -linear MRD-codes of $\mathcal{L}_{6,q}$ with dimension 12, minimum distance 5 and left idealiser isomorphic to $\mathbb{F}_{q^6}$, up to equivalence, arise from one of the following maximum scattered subspaces of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$: $U_s^{1,6}$, $U_{s,\delta}^{2,6}$, $U_{s,\delta}^{3,6}$ and U_c^4 . Also, from Result 2.1, two $\mathbb{F}_q$ -linear MRD-codes $\mathcal{C}$ and $\mathcal{C}'$ of $\mathcal{L}_{6,q}$, with minimum distance 5 and with left-idealisers isomorphic to $\mathbb{F}_{q^6}$, are equivalent if and only if $U_{\mathcal{C}}$ and $U_{\mathcal{C}'}$ are $\Gamma\text{L}(2, q^6)$ -equivalent.

The stabilisers of the $\mathbb{F}_q$ -subspaces above in the group $\text{GL}(2, q^6)$ were determined in [6, Sections 5 and 6] and in [10, Proposition 5.2]. They have the following orders:

1. for $U_s^{1,6}$ we have a group of order $q^6 - 1$,
2. for $U_{s,\delta}^{2,6}$ and U_c^4 we have a group of order $q^2 - 1$,
3. for $U_{s,\delta}^{3,6}$ we have a group of order $q^3 - 1$.

Also, since the $\Gamma\text{L}(2, q^6)$ -equivalence preserves the order of such stabilisers and since the results of [10, Propositions 5.2 and 5.3] do not depend on the congruence of q odd, using the same arguments we prove the last part of Theorem 1.1.

5 New maximum scattered $\mathbb{F}_q$ -linear sets of $\text{PG}(1, q^6)$

A point set L of a line $\Lambda = \text{PG}(W, \mathbb{F}_{q^n}) = \text{PG}(1, q^n)$ is said to be an $\mathbb{F}_q$ -linear set of Λ of rank n if it is defined by the non-zero vectors of an n -dimensional $\mathbb{F}_q$ -vector subspace U of the two-dimensional $\mathbb{F}_{q^n}$ -vector space W , i.e.

$$L = L_U := \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\}.$$

One of the most natural questions about linear sets is their equivalence. Two linear sets L_U and L_V of $\text{PG}(1, q^n)$ are said to be *PFL-equivalent* (or simply *equivalent*) if there is an element in $\text{PFL}(2, q^n)$ mapping L_U to L_V . In the applications it is crucial to have methods to decide whether two linear sets are equivalent or not. This can be a difficult problem and some results in this direction can be found in [11, 3].

Linear sets of rank n of $\text{PG}(1, q^n)$ have size at most $(q^n - 1)/(q - 1)$. A linear set L_U of rank n whose size achieves this bound is called *maximum scattered*. For applications of these objects we refer to [31] and [21].

To make notation easier, by $L_s^{i,n}$, $L_{s,\delta}^{i,n}$ and L_c^4 we will denote the $\mathbb{F}_q$ -linear set defined by $U_s^{i,n}$, $U_{s,\delta}^{i,n}$ and U_c^4 , respectively. The $\mathbb{F}_q$ -linear sets $\text{PFL}(2, q^n)$ -equivalent to $L_s^{1,n}$ are called *of pseudoregulus type*. It is easy to see that $L_1^{1,n} = L_s^{1,n}$ for any s with $\gcd(s, n) = 1$ and that $U_{s,\delta}^{2,n}$ is $\text{GL}(2, q^n)$ -equivalent to $U_{n-s,\delta-1}^{2,n}$.

In [25, Theorem 3] Lunardon and Polverino proved that $L_{1,\delta}^{2,n}$ and $L_1^{1,n}$ are not $\text{PFL}(2, q^n)$ -equivalent when $q > 3$, $n \geq 4$. For $n = 5$, in [4] it is proved that $L_{2,\delta}^{2,5}$ is $\text{PFL}(2, q^5)$ -equivalent neither to $L_{1,\delta'}^{2,5}$ nor to $L_1^{1,5}$.

In [10, Theorem 4.4], the authors proved that for $n = 6, 8$ the linear sets $L_1^{1,n}$, $L_{s,\delta}^{2,n}$ and $L_{s',\delta'}^{3,n}$ are pairwise non-equivalent for any choice of s, s', δ, δ' . Also in [10, Theorem 5.4] it has been proved that the linear set L_c^4 for q odd and $q \equiv 0, \pm 1 \pmod{5}$ is not equivalent to the aforementioned maximum scattered linear sets of $\text{PG}(1, q^6)$. This result has been obtained by [10, Proposition 5.3], where the congruences of q odd plays no role. Hence, using the same arguments, we have the following result.

Theorem 5.1. *The $\mathbb{F}_q$ -linear set L_c of rank 6 of $\text{PG}(1, q^6)$ defined by the $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$*

$$U_c = \{(x, x^q + x^{q^3} + cx^{q^5}) : x \in \mathbb{F}_{q^6}\},$$

with $c^2 + c = 1$, is scattered if and only if q is odd. Also, when $q \equiv \pm 2 \pmod{5}$ L_c is not $\text{P}\Gamma\text{L}(2, q^6)$ -equivalent to the previously known maximum scattered $\mathbb{F}_q$ -linear sets of $\text{PG}(1, q^6)$.

Final remark

In this paper we have proved that the RD-code $\mathcal{C} = \langle x, f(x) \rangle_{\mathbb{F}_{q^{2n}}}$ of $\mathcal{L}_{2n,q}$, with $f(x) = x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}$ ($n = 3$) and $c^2 + c + 1 = 0$, is an MRD-code with dimension 12, minimum distance 5 and left idealiser isomorphic to $\mathbb{F}_{q^6}$ if and only if q is odd. Computational results show that, for suitable choices of $c \in \mathbb{F}_{q^6} \setminus (\mathbb{F}_{q^2} \cup \mathbb{F}_{q^3})$ the previous trinomial produces MRD-codes also when $q \leq 64$ is even.

We strongly believe that the previous MRD-codes belong to a larger class of MRD-codes, arising from polynomials of type $f(x) = x^q + \sum_{i=1}^{n-1} a_{2i+1} x^{q^{2i+1}} \in \mathbb{F}_{q^{2n}}[x]$, under suitable assumptions on the coefficients a_j 's. In Table 1 we provide some explicit examples. They are the results of our successful searches using the software package MAGMA [2] for small values of n and q . When a parameter a_i appears in a row of the table it means that there exist explicit values of $a_i \in \mathbb{F}_{q^{2n}}$ for which the polynomial $f(x)$ gives rise to an MRD-code. Certainly, a careful study of the corresponding $\mathbb{F}_q$ -subspaces of $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ should be undertaken in order to establish whether the MRD-codes are equivalent to the previously known ones. The authors are currently beginning work on these two projects.

n	q	f(x)
3	$q \leq 64$, even	$x^q + x^{q^3} + a_5 x^{q^5}$
3	3, 5	$x^q - x^{q^3} + a_5 x^{q^5}$
3	3, 5, 7	$x^q + a_3 x^{q^3} + a_3^2 x^{q^5}$
4	3, 5	$x^q + x^{q^3} + x^{q^5} - x^{q^7}$
4	4	$x^q + a_3^2 x^{q^3} + a_3 x^{q^5} + x^{q^7}$
5	3	$x^q + a_3 x^{q^3} + a_5 x^{q^5} + a_7 x^{q^7} + a_9 x^{q^9}$

Table 1: Computational results

References

- [1] A. BLOKHUIS AND M. LAVRAUW: Scattered spaces with respect to a spread in $\text{PG}(n, q)$, *Geom. Dedicata* **81** (2000), 231–243.
- [2] W. BOSMA, J. CANNON AND C. PLAYOUST: The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.
- [3] B. CSAJBÓK, G. MARINO AND O. POLVERINO: Classes and equivalence of linear sets in $\text{PG}(1, q^n)$, *J. Combin. Theory Ser. A* **157** (2018), 402–426.
- [4] B. CSAJBÓK, G. MARINO AND O. POLVERINO: A Carlitz type result for linearized polynomials, *Ars Mathematica Contemporanea* **16** (2019), 585–608.
- [5] B. CSAJBÓK, G. MARINO, O. POLVERINO AND Y. ZHOU: Maximum rank-distance codes with maximum left and right idealisers, <https://arxiv.org/abs/1807.08774>.
- [6] B. CSAJBÓK, G. MARINO, O. POLVERINO AND C. ZANELLA: A new family of MRD-codes, *Linear Algebra Appl.* **548** (2018), 203–220.
- [7] B. CSAJBÓK, G. MARINO, O. POLVERINO AND F. ZULLO: Maximum scattered linear sets and MRD-codes, *J. Algebraic Combin.* **46** (2017), 1–15.
- [8] B. CSAJBÓK, G. MARINO, O. POLVERINO AND F. ZULLO: A characterization of linearized polynomials with maximum kernel, *Finite Fields Appl.* **56** (2019), 109–130;
- [9] B. CSAJBÓK, G. MARINO, O. POLVERINO AND F. ZULLO: A special class of scattered subspaces, <https://arxiv.org/abs/1906.10590>.
- [10] B. CSAJBÓK, G. MARINO AND F. ZULLO: New maximum scattered linear sets of the projective line, *Finite Fields Appl.* **54** (2018), 133–150.
- [11] B. CSAJBÓK AND C. ZANELLA: On the equivalence of linear sets, *Des. Codes Cryptogr.* **81** (2016), 269–281.

- [12] B. CSAJBÓK AND C. ZANELLA: On scattered linear sets of pseudoregulus type in $\text{PG}(1, q^t)$, *Finite Fields Appl.* **41** (2016), 34–54.
- [13] A. COSSIDENTE, G. MARINO, AND F. PAVESE: Non-linear maximum rank distance codes, *Designs, Codes and Cryptography*, **79** (2016), 597–609.
- [14] P. DELSARTE: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25** (1978), 226–241.
- [15] N. DURANTE AND A. SICILIANO: Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries, *The Electronic Journal of Combinatorics*, **24** (2017).
- [16] E. GABIDULIN: Theory of codes with maximum rank distance, *Problems of information transmission*, **21(3)** (1985), 3–16.
- [17] L. GIUZZI AND F. ZULLO: Identifiers for MRD-codes, *Linear Algebra Appl.* **575** (2019), 66–86.
- [18] R. GOW AND R. QUINLAN: Galois extensions and subspaces of alternating bilinear forms with special rank properties, *Linear Algebra Appl.* **430** (2009), 2212–2224.
- [19] J.W.P. HIRSCHFELD: Projective Geometries over Finite Fields 2nd ed., *Clarendon Press*, Oxford (1998).
- [20] A. KSHEVETSKIY AND E. GABIDULIN: The new construction of rank codes. In *International Symposium on Information Theory, 2005. ISIT 2005. Proceedings*, 2105–2108..
- [21] M. LAVRAUW: Scattered spaces in Galois Geometry, *Contemporary Developments in Finite Fields and Applications*, 2016, 195–216.
- [22] M. LAVRAUW AND O. POLVERINO: Finite semifields. In L. Storme and J. De Beule, editors, *Current research topics in Galois Geometry*, chapter 6, pages 131–160. NOVA Academic Publishers, 2011.
- [23] D. LIEBHOLD AND G. NEBE: Automorphism groups of Gabidulin-like codes, *Archiv der Mathematik*, **107** (2016), 355–366.

- [24] G. LUNARDON: MRD-codes and linear sets, *J. Combin. Theory Ser. A* **149** (2017), 1–20.
- [25] G. LUNARDON AND O. POLVERINO: Blocking Sets and Derivable Partial Spreads, *J. Algebraic Combin.* **14** (2001), 49–56.
- [26] G. LUNARDON, R. TROMBETTI AND Y. ZHOU: Generalized Twisted Gabidulin Codes, *J. Combin. Theory Ser. A* **159** (2018), 79–106.
- [27] G. LUNARDON, R. TROMBETTI AND Y. ZHOU: On kernels and nuclei of rank metric codes, *J. Algebraic Combin.* **46** (2017), 313–340.
- [28] G. MCGUIRE AND J. SHEEKEY: A Characterization of the Number of Roots of Linearized and Projective Polynomials in the Field of Coefficients, *Finite Fields Appl.* **57** (2019), 68–91.
- [29] K. OTAL AND F. ÖZBUDAK: Additive rank metric codes, *IEEE Transactions on Information Theory* **63** (2017), 164–168.
- [30] K. OTAL AND F. ÖZBUDAK: Some new non-additive maximum rank distance codes, *Finite Fields and Their Applications* **50** (2018), 293–303.
- [31] O. POLVERINO: Linear sets in finite projective spaces, *Discrete Math.* **310** (2010), 3096–3107.
- [32] J. SHEEKEY: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10**(3) (2016), 475–488.
- [33] J. SHEEKEY: New Semifields and new MRD Codes from Skew Polynomial Rings, *J. Lond. Math. Soc.* (2) (2019), 1–25..
- [34] J. SHEEKEY AND G. VAN DE VOORDE: Rank-metric codes, linear sets and their duality, <https://arxiv.org/abs/1806.05929>.
- [35] R. TROMBETTI AND Y. ZHOU: A new family of MRD codes in $\mathbb{F}_q^{2n \times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$, *IEEE Transaction on Information Theory*, **65** (2019), 1054–1062.
- [36] F. ZULLO: Linear codes and Galois geometries: between two worlds, *Ph.D thesis*, Università degli Studi della Campania “Luigi Vanvitelli”.

Giuseppe Marino
Dipartimento di Matematica e Applicazioni “Renato Caccioppoli”
Università degli Studi di Napoli “Federico II”
Via Cintia, Monte S. Angelo I-80126 Napoli
Italy
giuseppe.marino@unina.it

Maria Montanucci
Technical University of Denmark
Asmussens Allé
Building 303B, room 150
2800 Kgs. Lyngby
Denmark
marimo@dtu.dk

Ferdinando Zullo
Dipartimento di Matematica e Fisica
Università degli Studi della Campania *Luigi Vanvitelli*
Viale Lincoln, 5
36100 Caserta
Italy
ferdinando.zullo@unicampania.it