View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by ELTE Digital Institutional Repository (EDIT)

arXiv:1701.06831v1 [math.CO] 24 Jan 2017

Maximum scattered linear sets and MRD-codes

Bence Csajbók, Giuseppe Marino, Olga Polverino, Ferdinando Zullo *

Abstract

The rank of a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1,q^n)$, rn even, is at most $rn/2$ as it was proved by Blokhuis and Lavrauw. Existence results and explicit constructions were given for infinitely many values of r, n, q (rn even) for scattered $\mathbb{F}_q$-linear sets of rank $rn/2$. In this paper we prove that the bound $rn/2$ is sharp also in the remaining open cases.

Recently Sheekey proved that scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1,q^n)$ of maximum rank n yield $\mathbb{F}_q$–linear MRD-codes with dimension $2n$ and minimum distance $n-1$. We generalize this result and show that scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(r-1,q^n)$ of maximum rank $rn/2$ yield $\mathbb{F}_q$–linear MRD-codes with dimension rn and minimum distance $n-1$.

1 Introduction

Let $\Lambda = \mathrm{PG}(V,\mathbb{F}_{q^n}) = \mathrm{PG}(r-1,q^n)$, $q=p^h$, p prime, V a vector space of dimension r over $\mathbb{F}_{q^n}$, and let L be a set of points of Λ. The set L is said to be an $\mathbb{F}_q$*–linear* set of Λ of rank k if it is defined by the non-zero vectors of an $\mathbb{F}_q$-vector subspace U of V of dimension k, i.e.

$$L = L_U = \{\langle \mathbf{u}\rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}. \tag{1}$$

We point out that different vector subspaces can define the same linear set. For this reason a linear set and the vector space defining it must be considered as coming in pair.

Let $\Omega = \mathrm{PG}(W,\mathbb{F}_{q^n})$ be a subspace of Λ and let L_U be an $\mathbb{F}_q$-linear set of Λ. Then $\Omega \cap L_U$ is an $\mathbb{F}_q$–linear set of Ω defined by the $\mathbb{F}_q$–vector subspace $U \cap W$ and, if $\dim_{\mathbb{F}_q}(W\cap U)=i$, we say that Ω has *weight* i in L_U. Hence

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

a point of Λ belongs to L_U if and only if it has weight at least 1 and if L_U has rank k, then $|L_U| \leq q^{k-1} + q^{k-2} + \cdots + q + 1$. For further details on linear sets see [40], [27], [28], [34], [35], [29], [12] and [13].

An $\mathbb{F}_q$–linear set L_U of Λ of rank k is *scattered* if all of its points have weight 1, or equivalently, if L_U has maximum size $q^{k-1} + q^{k-2} + \cdots + q + 1$. A scattered $\mathbb{F}_q$–linear set of Λ of highest possible rank is a *maximum scattered $\mathbb{F}_q$–linear set* of Λ; see [4]. Maximum scattered linear sets have a lot of applications in Galois Geometry, such as translation hyperovals [19], translation caps in affine spaces [2], two-intersection sets ([4], [5]), blocking sets ([41], [31], [32] [7], [1]), translation spreads of the Cayley generalized hexagon ([9], [6], [37]), finite semifields (see e.g. [33], [10], [38], [15], [34], [24], [25], [26]), coding theory and graph theory [8]. For a recent survey on the theory of scattered spaces in Galois Geometry and its applications see [23].

The rank of a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1, q^n)$, rn even, is at most $rn/2$ ([4, Theorems 2.1, 4.2 and 4.3]). For $n = 2$ scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(r-1, q^2)$ of rank r are the Baer subgeometries. When r is even there always exist scattered $\mathbb{F}_q$–linear sets of rank $\frac{rn}{2}$ in $\mathrm{PG}(r-1, q^n)$, for any $n \geq 2$ (see [22, Theorem 2.5.5] for an explicit example). Existence results were proved for r odd, $n-1 \leq r$, n even, and $q > 2$ in [4, Theorem 4.4], but no explicit constructions were known for r odd, except for the case $r = 3$, $n = 4$, see [1, Section 3]. Very recently families of scattered linear sets of rank $rn/2$ in $\mathrm{PG}(r-1, q^n)$, r odd, n even, were constructed in [2, Theorem 1.2] for infinitely many values of r, n and q.

The existence of scattered $\mathbb{F}_q$–linear sets of rank $\frac{3n}{2}$ in $\mathrm{PG}(2, q^n)$, $n \geq 6$ even, $n \equiv 0 \pmod 3$, $q \not\equiv 1 \pmod 3$ and $q > 2$ was posed as an open problem in [2, Section 4]. As it was pointed out in [2], the existence of such planar linear sets and the construction method of [2, Theorem 3.1] would imply that the bound $\frac{rn}{2}$ for the maximum rank of a scattered $\mathbb{F}_q$–linear set in $\mathrm{PG}(r-1, q^n)$ is also tight when r is odd and n is even. In Theorem 2.3 we construct linear sets of rank $3n/2$ of $\mathrm{PG}(2, q^n)$, n even, and hence we prove the sharpness of the bound also in the remaining open cases. Our construction relies on the existence of non-scattered linear sets of rank $3t$ of $\mathrm{PG}(1, q^{3t})$ (with $t = n/2$) defined by binomial polynomials.

In [42, Section 4] Sheekey showed that maximum scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1, q^n)$ correspond to $\mathbb{F}_q$-linear maximum rank distance codes (MRD-codes) of dimension $2n$ and minimum distance $n-1$. In Section 3 we extend this result showing that MRD-codes can be constructed from every scattered linear set of rank $rn/2$ of $\mathrm{PG}(r-1, q^n)$, rn even, and we point out some relations with Sheekey's construction. Finally, we exhibit the MRD-codes arising from maximum scattered linear sets constructed in Theorem 2.3 and those constructed in [2, Theorems 2.2 and 2.3]

2 Maximum scattered linear sets in $\mathrm{PG}(r-1,q^n)$

As it was pointed out in the Introduction, the existence of scattered $\mathbb{F}_q$–linear sets of rank $\frac{3n}{2}$ in $\mathrm{PG}(2,q^n)$, $n \geq 6$ even, $n \equiv 0 \pmod 3$, $q \not\equiv 1 \pmod 3$ and $q > 2$ would imply that the bound $\frac{rn}{2}$ for the rank of a maximum scattered $\mathbb{F}_q$–linear set in $\mathrm{PG}(r-1,q^n)$ is tight in the remaining open cases (cf. [2, Remark 2.11 and Section 4]).

In this section we show that binomials of the form $f(x) = ax^{q^i} + bx^{2t+i}$ defined over $\mathbb{F}_{q^{3t}}$ can be used to construct maximum scattered $\mathbb{F}_q$–linear sets in $\mathrm{PG}(2,q^{2t})$ for any $t \geq 2$ and for any prime power q.

Consider the finite field $\mathbb{F}_{q^{6t}}$ as a 3–dimensional vector space over its subfield $\mathbb{F}_{q^{2t}}$, $t \geq 2$, and let $\mathbb{P} = \mathrm{PG}(\mathbb{F}_{q^{6t}}, \mathbb{F}_{q^{2t}}) = \mathrm{PG}(2,q^{2t})$ be the associated projective plane. From [2, Section 2.2], the $\mathbb{F}_q$-subspace

$$U := \{\omega x + f(x) \colon x \in \mathbb{F}_{q^{3t}}\}, \tag{2}$$

of $\mathbb{F}_{q^{6t}}$ with $\omega \in \mathbb{F}_{q^{2t}} \setminus \mathbb{F}_{q^t}$, $f(x) = ax^{q^i} + bx^{q^{2t+i}}$, $a, b \in \mathbb{F}^*_{q^{3t}}$, $1 \leq i \leq 3t-1$ and $gcd(i, 2t) = 1$, defines a maximum scattered $\mathbb{F}_q$-linear set in the projective plane $\mathbb{P}$ of rank $3t$ if $\frac{f(x)}{x} \notin \mathbb{F}_{q^t}$ for each $x \in \mathbb{F}^*_{q^{3t}}$ (cf. [2, Prop. 2.7]). The q-polynomial $f(x)$ also defines an $\mathbb{F}_q$-linear set $L_f := \{\langle (x, f(x)) \rangle_{\mathbb{F}_{q^{3t}}} : x \in \mathbb{F}^*_{q^{3t}}\}$ of the projective line $\mathrm{PG}(\mathbb{F}_{q^{6t}}, \mathbb{F}_{q^{3t}}) = \mathrm{PG}(1,q^{3t})$. In what follows we determine some conditions on L_f in order to obtain maximum scattered $\mathbb{F}_q$-linear sets in $\mathbb{P}$ of rank $3t$.

If $h \mid n$, then by $\mathrm{N}_{q^n/q^h}(\alpha)$ we will denote the norm of $\alpha \in \mathbb{F}_{q^n}$ over the subfield $\mathbb{F}_{q^h}$, that is, $\mathrm{N}_{q^n/q^h}(\alpha) = \alpha^{1+q^h+\ldots+q^{n-h}}$. We will need the following preliminary result.

Lemma 2.1. *Let* $f := f_{i,a,b} : x \in \mathbb{F}_{q^{3t}} \mapsto ax^{q^i} + bx^{q^{2t+i}} \in \mathbb{F}_{q^{3t}}$, *with* $a, b \in \mathbb{F}^*_{q^{3t}}$, $\mathrm{N}_{q^{3t}/q^t}(a) \neq -\mathrm{N}_{q^{3t}/q^t}(b)$ *and* $\gcd(i,t) = 1$. *If*

$$L_f := \{\langle (x, f(x)) \rangle_{\mathbb{F}_{q^{3t}}} : x \in \mathbb{F}^*_{q^{3t}}\} \tag{3}$$

is not a scattered $\mathbb{F}_q$*–linear set of* $\mathrm{PG}(1,q^{3t})$, *then there exists* $c \in \mathbb{F}^*_{q^{3t}}$ *such that*

$$g_c(x) := \frac{f_{i,ca,cb}(x)}{x} \notin \mathbb{F}_{q^t} \quad \textit{for each } x \in \mathbb{F}^*_{q^{3t}}. \tag{4}$$

Proof. First we show that $0 \notin Im\, g_c$ for each c. If $cax_0^{q^i-1} = -cbx_0^{q^{2t+i}-1}$ for some $x_0 \in \mathbb{F}_{q^{3t}}^*$, then $-a/b = x_0^{q^i(q^{2t}-1)}$, where the right hand side is a (q^t-1)-th power and hence $\mathrm{N}_{q^{3t}/q^t}(-a/b) = 1$, a contradiction.

The non-zero elements of the one-dimensional $\mathbb{F}_{q^t}$-spaces of $\mathbb{F}_{q^{3t}}^*$ yield a partition of $\mathbb{F}_{q^{3t}}^*$ into $q^{2t}+q^t+1$ subsets of size q^t-1. More precisely, if μ is a primitive element of $\mathbb{F}_{q^{3t}}$, then

$$\mathbb{F}_{q^{3t}}^* = \bigcup_{k=0}^{q^{2t}+q^t} \mu^k \mathbb{F}_{q^t}^*.$$

Let $G_k := \mu^k \mathbb{F}_{q^t}^*$. We show that, for each k, either $Im\, g_1 \cap G_k = \emptyset$, or $|Im\, g_1 \cap G_k| \geq (q^t-1)/(q-1)$.

Suppose $g_1(x_0) \in G_k$. Then for each $\gamma \in \mathbb{F}_{q^t}^*$ we have

$$g_1(\gamma x_0) = \gamma^{q^i-1} g_1(x_0).$$

Since $\gcd(i,t) = 1$, it follows that

$$\{g_1(\gamma x_0) \colon \gamma \in \mathbb{F}_{q^t}^*\} = g_1(x_0)\{x \in \mathbb{F}_{q^t} \colon \mathrm{N}_{q^t/q}(x) = 1\} \subseteq G_k$$

and hence $|Im\, g_1 \cap G_k| \geq (q^t-1)/(q-1)$.

Next we show that there exists G_d such that $Im\, g_1 \cap G_d = \emptyset$. Suppose to the contrary $Im\, g_1 \cap G_j \neq \emptyset$ for each $j \in \{0, 1, \ldots, q^{2t}+q^t\}$. Then $|Im\, g_1| \geq (q^{2t}+q^t+1)(q^t-1)/(q-1) = (q^{3t}-1)/(q-1)$ and since $|Im\, g_1| = |L_f|$ we get a contradiction.

Suppose that $Im\, g_1 \cap G_d = \emptyset$ and let $c = \mu^{-d}$. Then $Im\, g_c \cap \mathbb{F}_{q^t} = \emptyset$. $\square$

Hence, by the previous lemma and by [2, Prop. 2.7], the existence of a non-scattered linear set in $\mathrm{PG}(1, q^{3t})$ of form (3) implies the existence of a binomial polynomial producing maximum scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(2, q^{2t})$ of rank $3t$.

Lemma 2.2. *Let $f := f_{i,a,b} \colon x \in \mathbb{F}_{q^{3t}} \mapsto ax^{q^i} + bx^{q^{2t+i}} \in \mathbb{F}_{q^{3t}}$, with $a, b \in \mathbb{F}_{q^{3t}}^*$ and $1 \leq i \leq 3t-1$. For any prime power $q \geq 2$ and any integer $t \geq 2$ there exist $a, b \in \mathbb{F}_{q^{3t}}^*$, with*

$$\mathrm{N}_{q^{3t}/q^t}(b) \neq -\mathrm{N}_{q^{3t}/q^t}(a), \tag{5}$$

such that

$$L_{f_{i,a,b}} := \{\langle (x, f_{i,a,b}(x)) \rangle_{\mathbb{F}_{q^{3t}}} : x \in \mathbb{F}_{q^{3t}}^*\},$$

is a non–scattered $\mathbb{F}_q$–linear set in $\mathrm{PG}(1, q^{3t})$ of rank $3t$.

Proof. First suppose $d := \gcd(i,t) > 1$. Then f is $\mathbb{F}_{q^d}$-linear and hence each point of L_f has wight at least d, i.e. L_f cannot be scattered. Since $q^t \geq 4$ we can always choose a, b such that (5) holds. From now on we assume $\gcd(i,t) = 1$.

The linear set L_f of $\mathrm{PG}(1, q^{3t})$ is not scattered if there exists a point $P_{x_0} = \langle (x_0, f(x_0)) \rangle_{\mathbb{F}_{q^{3t}}}$ of rank greater than 1, i.e. if there exist $x_0 \in \mathbb{F}_{q^{3t}}{}^*$ and $\lambda \in \mathbb{F}_{q^{3t}} \setminus \mathbb{F}_q$ such that $f(\lambda x_0) = \lambda f(x_0)$. The latter condition is equivalent to

$$a x_0^{q^i}(\lambda - \lambda^{q^i}) = b x_0^{q^{2t+i}}(\lambda^{q^{2t+i}} - \lambda). \tag{6}$$

Since $\gcd(2t+i, 3t), \gcd(i, 3t) \in \{1, 3\}$, the expressions in the two sides of (6) are non-zero when $\lambda \notin \mathbb{F}_{q^3}$. We first prove that there exists $\bar{\lambda} \in \mathbb{F}_{q^{3t}} \setminus \mathbb{F}_{q^3}$ such that

$$\mathrm{N}_{q^{3t}/q^t}(\alpha_{\bar{\lambda}}) \neq -1, \tag{7}$$

where $\alpha_{\bar{\lambda}} = \frac{\bar{\lambda} - \bar{\lambda}^{q^i}}{\bar{\lambda}^{q^{2t+i}} - \bar{\lambda}}$.

By way of contradiction, suppose that $\mathrm{N}_{q^{3t}/q^t}(\alpha_{\bar{\lambda}}) = -1$ for each $\bar{\lambda} \in \mathbb{F}_{q^{3t}} \setminus \mathbb{F}_{q^3}$. Then the polynomial

$$g(x) := (x - x^{q^i})(x^{q^t} - x^{q^{t+i}})(x^{q^{2t}} - x^{q^{i+2t}}) + (x^{q^{2t+i}} - x)(x^{q^i} - x^{q^t})(x^{q^{t+i}} - x^{q^{2t}}) \tag{8}$$

vanishes on $\mathbb{F}_{q^{3t}} \setminus \mathbb{F}_{q^3}$. It also vanishes on $\mathbb{F}_q$, thus it has at least $q^{3t} - q^3 + q$ roots. Put $i = c + mt$, with $m \in \{0, 1, 2\}$ and $1 \leq c < t$, the degree of $g(x)$ is

$$q^{2t+c} + q^{2t} + q^t \tag{9}$$

when $m = 0$ and

$$q^{2t+c} + q^{2t} + q^{t+c} \tag{10}$$

when $m \in \{1, 2\}$. Since $q^t - 2 \geq q^c$ we obtain

$$q^{2t+c} + q^{2t} + q^{t+c} = q^c(q^{2t} + q^t) + q^{2t} \leq (q^t - 2)(q^{2t} + q^t) + q^{2t} = q^{3t} - 2q^t.$$

For $t > 2$ this is a contradiction since $q^{3t} - 2q^t < q^{3t} - q^3 + q$. If $t = 2$, then $\gcd(i,t) = 1$ yields $c = 1$ and hence we obtain

$$\deg g \leq q^5 + q^4 + q^3 < q^6 - q^3 + q,$$

again a contradiction. It follows that there always exists an element $\bar{\lambda} \in \mathbb{F}_{q^{3t}} \setminus \mathbb{F}_{q^3}$ which is not a root of $g(x)$, and $\alpha_{\bar{\lambda}}$ satisfies Condition (7).

Choose $a, b \in \mathbb{F}_{q^{3t}}^*$ such that $\mathrm{N}_{q^{3t}/q^t}(\frac{b}{a}) = \mathrm{N}_{q^{3t}/q^t}(\alpha_{\bar{\lambda}})$, then there exists an element $x_0 \in \mathbb{F}_{q^{3t}}^*$ such that

$$x_0^{q^{2t+i}-q^i} = \frac{a}{b}\alpha_{\bar{\lambda}},$$

and hence x_0 is a non-zero solution of the equation $f(\bar{\lambda}x) = \bar{\lambda}f(x)$, i.e. with these choices of a and b the linear set $L_{f_{i,a,b}}$ is not scattered. □

Now we are able to prove the following result.

Theorem 2.3. *Let $w \in \mathbb{F}_{q^{2t}} \setminus \mathbb{F}_{q^t}$. For any prime power q and any integer $t \geq 2$, there exist $a, b \in \mathbb{F}_{q^{3t}}^*$ and an integer $1 \leq i \leq 3t-1$ such that the $\mathbb{F}_q$-linear set L_U of rank $3t$ of the projective plane $\mathrm{PG}(\mathbb{F}_{q^{6t}}, \mathbb{F}_{q^{2t}}) = \mathrm{PG}(2, q^{2t})$, where*

$$U = \{ax^{q^i} + bx^{q^{2t+i}} + wx \colon x \in \mathbb{F}_{q^{3t}}\},$$

is scattered.

Proof. According to Lemma 2.2 for any prime power q and any integers $t \geq 2$, $1 \leq i \leq 3t-1$ with $\gcd(i, 2t) = 1$ we can choose $\bar{a}, \bar{b} \in \mathbb{F}_{q^{3t}}^*$, with $\mathrm{N}_{q^{3t}/q^t}(\bar{b}) \neq -\mathrm{N}_{q^{3t}/q^t}(\bar{a})$ such that the linear set L_f of the line $\mathrm{PG}(\mathbb{F}_{q^{6t}}, \mathbb{F}_{q^{3t}}) = \mathrm{PG}(1, q^3)$ with $f(x) = \bar{a}x^{q^i} + \bar{b}x^{q^{2t+i}}$ is non-scattered. Then by Lemma 2.1 there exists $c \in \mathbb{F}_{q^{3t}}^*$ such that

$$\frac{\bar{a}cx^{q^i} + \bar{b}cx^{q^{2t+i}}}{x} \notin \mathbb{F}_{q^t}$$

for each $x \in \mathbb{F}_{q^{3t}}^*$. Then the theorem follows from [2, Proposition 2.7] with $a = \bar{a}c$ and $b = \bar{b}c$. □

As it was pointed out in [2], the existence of maximum scattered $\mathbb{F}_q$–linear sets of rank $3n$ in the projective plane $\mathrm{PG}(2, q^{2t})$ (proved in Theorem 2.3) and the construction method of [2, Theorem 3.1] imply the following.

Theorem 2.4. *For any integers $r, n \geq 2$, rn even, and for any prime power $q \geq 2$ the rank of a maximum scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1, q^n)$ is $rn/2$.*

Taking into account the previous result, from now on, a scattered $\mathbb{F}_q$–linear set L_U of $\mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$ of rank $\frac{rn}{2}$ (rn even) will be simply called a *maximum scattered linear set* and the $\mathbb{F}_q$-subspace U will be called a *maximum scattered subspace*.

We complete this section by showing a connection between scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1, q^{rn/2})$, r even, and scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(r-1, q^n)$.

Proposition 2.5. *Every maximum scattered $\mathbb{F}_q$-linear set of* $\mathrm{PG}(1, q^{rn/2})$, *r even, gives a maximum scattered $\mathbb{F}_q$-linear set of* $\mathrm{PG}(r-1, q^n)$.

Proof. Let L_U be a maximum scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(W, \mathbb{F}_{q^{rn/2}}) = \mathrm{PG}(1, q^{rn/2})$. Then for each $\mathbf{v} \in W$ the one dimensional $\mathbb{F}_{q^{rn/2}}$-subspace $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^{rn/2}}}$ meets U in an $\mathbb{F}_q$-subspace of dimension at most one. Since $\mathbb{F}_{q^n}$ is a subfield of $\mathbb{F}_{q^{rn/2}}$ (recall r even) the same holds for the subspace $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}$ and hence U also defines a scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$. $\square$

Note that the converse of the above result does not hold.

3 Maximum scattered subspaces and MRD-codes

The set of $m \times n$ matrices $\mathbb{F}_q^{m\times n}$ over $\mathbb{F}_q$ is a rank metric $\mathbb{F}_q$-space with rank metric distance defined by $d(A, B) = rk\,(A - B)$ for $A, B \in \mathbb{F}_q^{m\times n}$. A subset $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is called a rank distance code (RD-code for short). The minimum distance of $\mathcal{C}$ is

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

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 the dimension $\dim_q(\mathcal{C})$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$. If d is the minimum distance of $\mathcal{C}$ we say that $\mathcal{C}$ has parameters $(m, n, q; d)$.

The Singleton bound for an $m \times n$ rank metric code $\mathcal{C}$ with minimum rank distance d is

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

If this bound is achieved, then $\mathcal{C}$ is an MRD-code. MRD-codes have various applications in communications and cryptography; for instance, see [17, 21]. More properties of MRD-codes can be found in [14, 16, 18, 39].

Delsarte [14] and Gabidulin [16] constructed, independently, linear MRD-codes over $\mathbb{F}_q$ for any values of m and n and for arbitrary value of the minimum distance d. In the literature these are called *Gabidulin codes*, even if the first construction is due to Delsarte. These codes were later generalized by Kshevetskiy and Gabidulin in [20], they are the so called *generalized Gabidulin codes.*

A generalized Gabidulin code is defined as follows: under a given basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, each element a of $\mathbb{F}_{q^n}$ can be written as a (column) vector

$\mathbf{v}(a)$ in $\mathbb{F}_q^n$. Let $\alpha_1, \ldots, \alpha_m$ be a set of linearly independent elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, where $m \leq n$. Then

$$\left\{(\mathbf{v}(f(\alpha_1)), \ldots, \mathbf{v}(f(\alpha_m)))^T : f \in \mathcal{G}_{k,s}\right\} \tag{11}$$

is the original generalized Gabidulin code, where

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \ldots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}, \tag{12}$$

with $n, k, s \in \mathbb{Z}^+$ satisfying $k < n$ and $\gcd(n, s) = 1$.

All members of $\mathcal{G}_{k,s}$ are of the form $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, where $a_i \in \mathbb{F}_{q^n}$. A polynomial of this form is called a *linearized polynomial* (also a q-polynomial because its exponents are all powers of q). They are equivalent to $\mathbb{F}_q$-linear transformations from $\mathbb{F}_{q^n}$ to itself, i.e., elements of $\mathbb{E} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$. We refer to [30, Section 4] for their basic properties.

In the literature, there are different definitions of equivalence for rank metric codes; see [3, 39]. If $\mathcal{C}$ and $\mathcal{C}'$ are two sets of $\mathrm{GL}(U, \mathbb{F}_q)$, where U is an $\mathbb{F}_q$-space of dimension n, then up to an isomorphism we may consider U as the finite field $\mathbb{F}_{q^n}$ and it is natural to define equivalence in the language of q-polynomials, see [42]. For $\mathbb{F}_q$-linear maps between vector spaces of distinct dimensions we will use the following definition of equivalence.

Definition 3.1. *Let $U(n,q)$ and $V(m,q)$ be two $\mathbb{F}_q$-spaces, $n \neq m$, and let $\mathcal{C}$ and $\mathcal{C}'$ be two sets of $\mathbb{F}_q$-linear maps from U to V. They are equivalent if there exist two invertible $\mathbb{F}_q$-linear maps $L_1 \in \mathrm{GL}(V, \mathbb{F}_q)$, $L_2 \in \mathrm{GL}(U, \mathbb{F}_q)$ and $\rho \in Aut(\mathbb{F}_q)$ such that $\mathcal{C}' = \{L_1 \circ f^\rho \circ L_2 : \ f \in \mathcal{C}\}$, where $f^\rho(x) = f(x^{\rho^{-1}})^\rho$.*

Very recently, Sheekey made a breakthrough in the construction of new linear MRD-codes using linearized polynomials [42] (see also [36]).

In [42, Section 4], the author showed that maximum scattered linear sets of $\mathrm{PG}(1, q^n)$ correspond to $\mathbb{F}_q$-linear MRD-codes of dimension $2n$ and minimum distance $n-1$. The number of non-equivalent MRD-codes obtained from a maximum scattered linear set of $\mathrm{PG}(1, q^n)$ was studied in [11, Section 5.4].

Here we extend this result showing that MRD-codes of dimension rn and minimum distance $n-1$ can be constructed from every maximum scattered $\mathbb{F}_q$–linear set of $\mathrm{PG}(r-1, q^n)$, rn even, and we exhibit some relations with Sheekey's construction when r is even.

To this aim, recall that an $\mathbb{F}_q$-subspace U of $\mathbb{F}_{q^{rn}}$ is scattered with respect to $\mathbb{F}_{q^n}$ if it defines a scattered $\mathbb{F}_q$-linear set in $\mathrm{PG}(\mathbb{F}_{q^{rn}}, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$, i.e. $dim_{\mathbb{F}_q}(U \cap \langle x \rangle_{\mathbb{F}_{q^n}}) \leq 1$ for each $x \in \mathbb{F}_{q^{rn}}^*$.

Theorem 3.2. *Let U be an $rn/2$-dimensional $\mathbb{F}_q$-subspace of the r-dimensional $\mathbb{F}_{q^n}$-space $V = V(r, q^n)$, rn even, and let $i = \max\{\dim_{\mathbb{F}_q}(U \cap \langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}})\colon \mathbf{v} \in V\}$. For any $\mathbb{F}_q$-linear function $G\colon V \to W$, with $W = V(rn/2, q)$ such that $\ker G = U$, if $i < n$, then the pair (U, G) determines an RD-code $\mathcal{C}_{U,G}$ (cf. (13)) of dimension rn and with parameters $(rn/2, n, q; n-i)$. Also, $\mathcal{C}_{U,G}$ is an MRD-code if and only if U is a maximum scattered $\mathbb{F}_q$-subspace with respect to $\mathbb{F}_{q^n}$.*

Proof. For $\mathbf{v} \in V$ the set

$$R_{\mathbf{v}} := \{\lambda \in \mathbb{F}_{q^n} \colon \lambda \mathbf{v} \in U\}$$

is an $\mathbb{F}_q$-subspace with dimension the weight of the point $\langle \mathbf{v} \rangle_{\mathbb{F}_{q^n}}$ in the $\mathbb{F}_q$-linear set L_U of $\mathrm{PG}(V, \mathbb{F}_{q^n})$. Since i is the maximum weight of the points in L_U, it follows that $\dim_{\mathbb{F}_q} R_{\mathbf{v}} \leq i$ for each $\mathbf{v}$. Also, let $\tau_{\mathbf{v}}$ denote the map

$$\lambda \in \mathbb{F}_{q^n} \mapsto \lambda \mathbf{v} \in V.$$

Direct computation shows that the kernel of $G \circ \tau_{\mathbf{v}}$ is $R_{\mathbf{v}}$ for each $\mathbf{v} \in V$ and hence it has rank at least $n-i$. It remains to show that $G \circ \tau_{\mathbf{v}} \neq G \circ \tau_{\mathbf{w}}$ for $\mathbf{v} \neq \mathbf{w}$. Suppose, contrary to our claim, that there exist $\mathbf{v}, \mathbf{w} \in V$ with $\mathbf{v} \neq \mathbf{w}$ and with $G(\lambda \mathbf{v}) = G(\lambda \mathbf{w})$ for each $\lambda \in \mathbb{F}_{q^n}$. Note that $\mathbf{v} \mapsto G \circ \tau_{\mathbf{v}}$ is an $\mathbb{F}_q$-linear map and hence $G(\lambda(\mathbf{v} - \mathbf{w})) = 0$ for each $\lambda \in \mathbb{F}_{q^n}$. This means $\dim_{\mathbb{F}_q}(\ker G \circ \tau_{\mathbf{v}-\mathbf{w}}) = n = i$, a contradiction. Hence

$$\mathcal{C}_{U,G} = \{G \circ \tau_{\mathbf{v}} \colon \mathbf{v} \in V\} \tag{13}$$

is an $\mathbb{F}_q$-linear RD-code with dimension rn and with parameters $(rn/2, n, q; n-i)$. The second part is obvious since L_U is scattered if and only if $i = 1$. □

Now we will show that different choices of the function G give rise to equivalent RD-codes. Let's start by proving the following result.

Lemma 3.3. *Let U be an $rn/2$-dimensional $\mathbb{F}_q$-subspace of the r-dimensional $\mathbb{F}_{q^n}$-space $\mathbb{F}_{q^{rn}}$. Then there exists $\omega \in \mathbb{F}_{q^{rn}} \setminus \mathbb{F}_{q^{rn/2}}$ such that*

$$U = \{x + \omega f(x) \colon x \in \mathbb{F}_{q^{rn/2}}\}$$

where $f(x)$ is a q-polynomial over $\mathbb{F}_{q^{rn/2}}$.

Proof. Observe that $\mathbb{F}^*_{q^{rn}} = \bigcup_{a \in \mathbb{F}^*_{q^{rn}}} a\mathbb{F}^*_{q^{rn/2}}$ and for any $a, b \in \mathbb{F}^*_{q^{rn}}$ either $a\mathbb{F}^*_{q^{rn/2}} \cap b\mathbb{F}^*_{q^{rn/2}} = \emptyset$ or $a\mathbb{F}^*_{q^{rn/2}} = b\mathbb{F}^*_{q^{rn/2}}$ and the latter case happens if and only if $\frac{a}{b} \in \mathbb{F}^*_{q^{rn/2}}$. Since $U^* \cap a\mathbb{F}^*_{q^{rn/2}}$ is either empty or contains at least $q-1$

elements and since $|U^*| = q^{\frac{rn}{2}} - 1$, there exist $a, b \in \mathbb{F}^*_{q^{rn}}$, with $\frac{a}{b} \notin \mathbb{F}_{q^{rn/2}}$ such that $U^* \cap a\mathbb{F}^*_{q^{rn/2}} = U^* \cap b\mathbb{F}^*_{q^{rn/2}} = \emptyset$. We may assume $a \notin \mathbb{F}^*_{q^{rn/2}}$ and put $\omega := a$. Then $U \cap \omega\mathbb{F}_{q^{rn/2}} = \{0\}$ and taking into account that U has rank $\frac{rn}{2}$ and $\{1, \omega\}$ is an $\mathbb{F}_{q^{rn/2}}$–basis of $\mathbb{F}_{q^{rn}}$, we have $U = \{x + \omega f(x) \colon x \in \mathbb{F}_{q^{rn/2}}\}$ for some q-polynomial f over $\mathbb{F}_{q^{rn/2}}$. □

Hence, we are able to prove the following

Proposition 3.4. *Let U be an $rn/2$-dimensional $\mathbb{F}_q$-subspace of the r-dimensional $\mathbb{F}_{q^n}$-space $V = V(r, q^n)$, rn even, and let G and $\overline{G}$ be two $\mathbb{F}_q$-linear functions determining two RD-codes $\mathcal{C}_{U,G}$ and $\mathcal{C}_{U,\overline{G}}$ as in Theorem 3.2. Then $\mathcal{C}_{U,G}$ and $\mathcal{C}_{U,\overline{G}}$ are equivalent.*

Proof. Up to an isomorphism, we can always assume $V = \mathbb{F}_{q^{rn/2}} \times \mathbb{F}_{q^{rn/2}}$ and $W = \mathbb{F}_{q^{rn/2}}$. Then by Lemma 3.3 we have $U = \{(x, f(x)) : x \in \mathbb{F}_{q^{\frac{rn}{2}}}\}$, where $f(x)$ is a q-polynomial over $\mathbb{F}_{q^{rn/2}}$. Then $G, \overline{G} : \mathbb{F}_{q^{rn/2}} \times \mathbb{F}_{q^{rn/2}} \to \mathbb{F}_{q^{rn/2}}$ are two $\mathbb{F}_q$-linear maps such that $U = \ker G = \ker \overline{G}$. We want to show that there exist two permutation q-polynomials H and L over $\mathbb{F}_{q^{rn/2}}$ and $\mathbb{F}_{q^n}$, respectively, and $\sigma \in Aut(\mathbb{F}_q)$ such that

$$\mathcal{C}_{U,\overline{G}} = \{H \circ (G \circ \tau_{\mathbf{v}})^\sigma \circ L \ : \ v \in \mathbb{F}_{q^{rn}}\}.$$

Let $G_0, G_1, \overline{G}_0, \overline{G}_1 :\ \mathbb{F}_{q^{rn/2}} \to \mathbb{F}_{q^{rn/2}}$ be $\mathbb{F}_q$–linear maps such that

$$G(x, y) = G_0(x) - G_1(y) \quad \text{and} \quad \overline{G}(x, y) = \overline{G}_0(x) - \overline{G}_1(y),$$

for all $x, y \in \mathbb{F}_{q^{rn/2}}$. Since $\ker G = \ker \overline{G} = U$ it can be easily seen that $G_0 = G_1 \circ f$, $\overline{G}_0 = \overline{G}_1 \circ f$ and that G_1 and $\overline{G}_1$ are invertible maps. Hence, putting $H = \overline{G}_1 \circ G_1^{-1}$, $\sigma = id_{\mathbb{F}_q}$ and $L = id_{\mathbb{F}_{q^n}}$, we have

$$H \circ G \circ \tau_{\mathbf{v}} = \overline{G} \circ \tau_{\mathbf{v}},$$

for each $\mathbf{v} = (x, y) \in V$, and hence the assertion follows. □

First we show some results in the case r even. Starting with the following example for $r = 2$, we examine further the codes defined in Theorem 3.2. Later, in Theorem 3.7 we will also give a different construction of MRD-codes.

Example 3.5. *Let $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\}$ be a maximum scattered $\mathbb{F}_q$-subspace of the two-dimensional $\mathbb{F}_{q^n}$-space $V = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, where f is a q-polynomial over $\mathbb{F}_{q^n}$. Let*

$$G \colon (a, b) \in V \mapsto f(a) - b \in \mathbb{F}_{q^n}.$$

Then $\ker G = U_f$ *and Theorem 3.2 with* $r = 2$ *yields the MRD-code consisting of the maps* $G \circ \tau_{(a,b)}$*, i.e.*

$$\mathcal{C}_{U_f,G} = \{x \in \mathbb{F}_{q^n} \mapsto f(ax) - bx \in \mathbb{F}_{q^n} \colon (a,b) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}\}. \tag{14}$$

Note that the MRD-codes (14) are the adjoints of the codes constructed by Sheekey in [42, Sec. 5], see also after Remark 3.6.

Remark 3.6. *Let* U *be a maximum scattered* $\mathbb{F}_q$*-subspace of* $V = V(2, q^{rn/2})$*,* r *even. According to Proposition 2.5,* U *is also a maximum scattered* $\mathbb{F}_q$*-subspace of* V*, considered as an* r*-dimensional* $\mathbb{F}_{q^n}$*-space. Let* G *be an* $\mathbb{F}_q$*-linear* $V \to W = V(rn/2, q)$ *map with* $\ker G = U$*. When* V *is viewed as an* $\mathbb{F}_{q^n}$*-space, then the construction method of Theorem 3.2 yields the MRD-code*

$$\mathcal{C}_{U,G} = \{x \in \mathbb{F}_{q^n} \mapsto G \circ \tau_{\mathbf{v}}(x) \in W \colon \mathbf{v} \in V\}. \tag{15}$$

When V *is viewed as an* $\mathbb{F}_{q^{rn/2}}$*-space, then we obtain the MRD-code*

$$\mathcal{D}_{U,G} = \{x \in \mathbb{F}_{q^{rn/2}} \mapsto G \circ \tau_{\mathbf{v}}(x) \in W \colon \mathbf{v} \in V\}. \tag{16}$$

Since $\mathbb{F}_{q^n}$ *is a subfield of* $\mathbb{F}_{q^{rn/2}}$*, the latter code is the restriction of the former one on* $\mathbb{F}_{q^n}$*.*

Conversely, it may happen, even if r *is even, that an* $\mathbb{F}_q$*-subspace* U *of* $V = V(r, q^n)$ *of rank* $rn/2$ *is scattered with respect to* $\mathbb{F}_{q^n}$ *whereas it is not scattered when* V *is considered as a* 2*-dimensional* $\mathbb{F}_{q^{rn/2}}$*-space. Arguing as above, the MRD-code* $\mathcal{C}_{U,G}$ *described in (15) is the restriction of the RD-code* $\mathcal{D}_{U,G}$ *described in (16).*

Let ω_α be the map $\mathbb{F}_{q^{rn/2}} \to \mathbb{F}_{q^{rn/2}}$ defined by the rule $x \mapsto \alpha x$. By $(\omega_\alpha + \omega_\beta \circ f) \mid_{\mathbb{F}_{q^n}}$ we denote the restriction of the corresponding function over $\mathbb{F}_{q^n}$. From Example 3.5 and from Remark 3.6 it follows that if r is even and $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^{rn/2}}\}$ is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}^2_{q^{rn/2}}$ considered as an r-dimensional $\mathbb{F}_{q^n}$-space, then the MRD-code (cf. (14), (15) and (16))

$$\mathcal{C}_f = \{(\omega_\alpha + f \circ \omega_\beta) \mid_{\mathbb{F}_{q^n}} \colon \alpha, \beta \in \mathbb{F}_{q^{rn/2}}\}$$

is the restriction on $\mathbb{F}_{q^n}$ of the MRD-code

$$\mathcal{D}_f = \{(\omega_\alpha + f \circ \omega_\beta) \colon \alpha, \beta \in \mathbb{F}_{q^{rn/2}}\}.$$

The next result shows that $\{(\omega_\alpha + \omega_\beta \circ f) \mid_{\mathbb{F}_{q^n}} \colon \alpha, \beta \in \mathbb{F}_{q^{rn/2}}\}$ is also an MRD-code with the same parameters as $\mathcal{C}_f$. For $r = 2$ this is exactly the code defined by Sheekey.

Theorem 3.7. *Let r be even and $U_f := \{(x, f(x)) \colon x \in \mathbb{F}_{q^{rn/2}}\}$ be a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}^2_{q^{rn/2}}$ considered as $V(r, q^n)$, where f is a q-polynomial over $\mathbb{F}_{q^{rn/2}}$. Then $\mathcal{S}_f := \{(\omega_\alpha + \omega_\beta \circ f) \mid_{\mathbb{F}_{q^n}} : \alpha, \beta \in \mathbb{F}_{q^{rn/2}}\}$ is an MRD-code with parameters $(rn/2, n, q; n-1)$.*

Proof. Since U_f is scattered, the following holds. If $(x, f(x)) = \lambda(y, f(y))$ with $\lambda \in \mathbb{F}_{q^n}$, then $\lambda \in \mathbb{F}_q$, so for each $y \in \mathbb{F}^*_{q^{rn/2}}$

$$f(\lambda y) = \lambda f(y) \text{ with } \lambda \in \mathbb{F}_{q^n} \text{ implies } \lambda \in \mathbb{F}_q. \tag{17}$$

It also follows that for each $y \in \mathbb{F}^*_{q^{rn/2}}$ we have

$$f(\lambda y)/\lambda y = f(y)/y \text{ for some } \lambda \in \mathbb{F}^*_{q^n} \text{ if and only if } \lambda \in \mathbb{F}^*_q. \tag{18}$$

First we show that $(\alpha x + \beta f(x)) \mid_{\mathbb{F}_{q^n}} = 0$ implies $\alpha = \beta = 0$. Suppose the contrary. If $\beta \neq 0$, then $f(x) = xt$, with $t = -\alpha/\beta$ for each $x \in \mathbb{F}_{q^n}$, contradicting (17). If $\beta = 0$, then clearly also $\alpha = 0$. It follows that $|\mathcal{S}_f| = q^{rn}$.

The $\mathbb{F}_q$-linear map $(\alpha x + \beta f(x)) \mid_{\mathbb{F}_{q^n}}$ has rank less than $n-1$ if and only if $\beta \neq 0$ and there exist $x, y \in \mathbb{F}^*_{q^n}$ such that $\langle x \rangle_{\mathbb{F}_q} \neq \langle y \rangle_{\mathbb{F}_q}$ and $f(x)/x = f(y)/y = -\alpha/\beta$. But then for $\lambda := x/y \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$ we have $f(\lambda y)/\lambda y = f(y)/y$ contradicting (18). □

Sheekey in [42, Theorem 8] showed that when $r = 2$ the two $\mathbb{F}_q$–vector subspaces U_f and U_g defined as in Theorem 3.7 are equivalent under the action of the group $\Gamma\mathrm{L}(2, q^n)$ if and only if $\mathcal{S}_f$ and $\mathcal{S}_g$ are equivalent as MRD-codes. Here we will show that the same result is not true when we consider the restriction codes. To show this we will need the following two examples, where non-equivalent $\mathbb{F}_q$-subspaces yield the same MRD-code.

Example 3.8. *Consider $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^{tn}}\}$, with $t \geq 1$, $n \geq 3$ and with $f \colon \mathbb{F}_{q^{tn}} \to \mathbb{F}_{q^{tn}}$ an invertible $\mathbb{F}_{q^n}$-semilinear map with associated automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that $\mathrm{Fix}(\sigma) = \mathbb{F}_q$. Then L_{U_f} is a scattered $\mathbb{F}_q$–linear set of pseudoregulus type in $\mathrm{PG}(2t-1, q^n)$ (cf. [34, Sec. 3]). With this choice of f, we get*

$$\mathcal{S}_f = \{(\omega_\alpha + \omega_\beta \circ id^\sigma) \mid_{\mathbb{F}_{q^n}} : \alpha, \beta \in \mathbb{F}_{q^{tn}}\}.$$

Indeed, for every $\lambda \in \mathbb{F}_{q^n}$ we have $(\omega_\alpha + \omega_\beta \circ f)(\lambda) = \alpha\lambda + \beta f(\lambda) = \alpha\lambda + \beta\lambda^\sigma f(1)$.

Example 3.9. *Let $W = \{(x, y, x^q, y^{q^h}) \colon x, y \in \mathbb{F}_{q^n}\}$, with $n \geq 5$, $1 < h < n-1$ and with $\gcd(h, n) = 1$. Then W is a scattered $\mathbb{F}_q$-subspace of $V(4, q^n)$ and it defines an $\mathbb{F}_q$-linear set L_W of $\mathrm{PG}(3, q^n)$, which is not of pseudoregulus type, see [25, Proposition 2.5]. We may consider $V(4, q^n)$ as $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$. Take $\omega \in \mathbb{F}_{q^{2n}} \setminus \mathbb{F}_{q^n}$, so $\{1, \omega\}$ is an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^{2n}}$ and*

$$W = \{(x + \omega y, x^q + \omega y^{q^h}) \colon x, y \in \mathbb{F}_{q^n}\}.$$

Direct computations show that $W = \{(z, g(z)) \colon z \in \mathbb{F}_{q^{2n}}\} = U_g$, where g is the q-polynojmial over $\mathbb{F}_{q^{2n}}$ of the form

$$g(z) = a_1 z^q + a_h z^{q^h} + (1 - a_1) z^{q^{n+1}} - a_h z^{q^{n+h}},$$

with $a_1 = \frac{\omega^{q^{n+1}}}{\omega^{q^{n+1}} - \omega^q}$ and $a_h = \frac{1}{\omega^{q^h - 1} - \omega^{q^{h+n} - 1}}$. Hence $g(z) \mid_{\mathbb{F}_{q^n}} = z^q$, so

$$\mathcal{S}_g = \{(\omega_\alpha + \omega_\beta \circ id^q) \mid_{\mathbb{F}_{q^n}} : \alpha, \beta \in \mathbb{F}_{q^{2n}}\}.$$

Theorem 3.10. *In $V(4, q^n)$, $n \geq 5$, there exist two non-equivalent maximum scattered $\mathbb{F}_q$-subspaces U_f and U_g such that the codes $\mathcal{S}_f$ and $\mathcal{S}_g$ coincide.*

Proof. In Example 3.8 take $t = 2$ and $\sigma \colon x \mapsto x^q$. Then we obtain the same code as in Example 3.9, while the corresponding subspaces are non-equivalent because of [25, Proposition 2.5]. □

Let now r be odd and $n = 2t$. Some of the known families of maximum scattered $\mathbb{F}_q$-subspaces are given in the r-dimensional $\mathbb{F}_{q^{2t}}$-space $V = \mathbb{F}_{q^{2rt}}$ and they are of the form

$$U_f := \{x\omega + f(x) \colon x \in \mathbb{F}_{q^{rt}}\}, \tag{19}$$

with $\omega \in \mathbb{F}_{q^{2t}} \setminus \mathbb{F}_{q^t}$ and with $\omega^2 = \omega A_0 + A_1$, $A_0, A_1 \in \mathbb{F}_{q^t}$. In this case we show an explicit construction of $\mathbb{F}_q$-linear MRD-codes with parameters $(rt, 2t, q; 2t-1)$ obtained from Theorem 3.2. Indeed, in this case $\{\omega, 1\}$ is an $\mathbb{F}_{q^t}$-basis of $\mathbb{F}_{q^{2t}}$ and also an $\mathbb{F}_{q^{rt}}$-basis of $\mathbb{F}_{q^{2rt}}$. Then we can write any element $\lambda \in \mathbb{F}_{q^{2t}}$ as $\lambda = \lambda_0 \omega + \lambda_1$, with $\lambda_0, \lambda_1 \in \mathbb{F}_{q^t}$. We fix $G \colon \mathbb{F}_{q^{2rt}} \to \mathbb{F}_{q^{rt}}$ as the map $x\omega + y \mapsto f(x) - y$. For each $v = v_0 \omega + v_1 \in \mathbb{F}_{q^{2rt}}$ the map $\tau_v \colon \mathbb{F}_{q^{2t}} \to \mathbb{F}_{q^{2rt}}$ is as follows

$$\lambda \mapsto \lambda_0 v_0 A_1 + \lambda_1 v_1 + \omega(\lambda_0 v_1 + \lambda_1 v_0 + \lambda_0 v_0 A_0),$$

and τ_v can be viewed as a function defined on $\mathbb{F}_{q^t} \times \mathbb{F}_{q^t}$. Then the associated MRD-code consists of the following maps:

$$G \circ \tau_v \colon (x, y) \in \mathbb{F}_{q^t} \times \mathbb{F}_{q^t} \mapsto f(\lambda_0 v_1 + \lambda_1 v_0 + \lambda_0 v_0 A_0) - \lambda_0 v_0 A_1 - \lambda_1 v_1.$$

Example 3.11. *Put* $f(x) := ax^{q^i}$, $a \in \mathbb{F}^*_{q^{rt}}$, $1 \le i \le rt-1$, r *odd. For any* $q \ge 2$ *and any integer* $t \ge 2$ *with* $\gcd(t,r) = 1$, *such that*

(i) $\gcd(i,2t) = 1$ *and* $\gcd(i,rt) = r$,

(ii) $\mathrm{N}_{q^{rt}/q^r}(a) \notin \mathbb{F}_q$,

from [2, Theorem 2.2], we get the $\mathbb{F}_q$*-linear MRD-code with dimension* $2rt$ *and parameters* $(2t, rt, q; 2t-1)$*:*

$$\{F_v \colon v = \omega v_0 + v_1,\ v_0, v_1 \in \mathbb{F}_{q^{rt}}\},$$

where $F_v \colon \mathbb{F}_{q^t} \times \mathbb{F}_{q^t} \to \mathbb{F}_{q^{rt}}$ *is defined by the rule*

$$F_v(x,y) = x^{q^i} a(A_0^{q^i} v_0^{q^i} + v_1^{q^i}) - xA_1 v_0 + y^{q^i} a v_0^{q^i} - y v_1. \tag{20}$$

Note that, since $\gcd(i,rt) = r$, *the above MRD-code is* $\mathbb{F}_{q^r}$*-linear as well, since for each* $\mu \in \mathbb{F}_{q^r}$ *and* $v \in \mathbb{F}_{q^{2rt}}$ *we have* $\mu F_v = F_{\mu v}$.

Example 3.12. *Put* $f(x) := ax^{q^i}$, $a \in \mathbb{F}^*_{q^{rt}}$, $1 \le i \le rt-1$, r *odd. For any prime power* $q \equiv 1 \pmod r$ *and any integer* $t \ge 2$, *such that*

(i) $\gcd(i,2t) = \gcd(i,rt) = 1$,

(ii) $\left(\mathrm{N}_{q^{rt}/q}(a)\right)^{\frac{q-1}{r}} \neq 1$,

from [2, Theorem 2.3], we get the $\mathbb{F}_q$*-linear MRD-code with dimension* $2rt$ *and parameters* $(2t, rt, q; 2t-1)$*:*

$$\{F_v \colon v = \omega v_0 + v_1,\ v_0, v_1 \in \mathbb{F}_{q^{rt}}\},$$

where $F_v \colon \mathbb{F}_{q^t} \times \mathbb{F}_{q^t} \to \mathbb{F}_{q^{rt}}$ *is defined by the same rule as* (20).

Example 3.13. *Put* $f(x) := ax^{q^i} + bx^{q^{2t+i}}$, $a, b \in \mathbb{F}^*_{q^{3t}}$, $1 \le i \le 3t-1$ *(here* $r = 3$*). For any* $q \ge 2$ *and any integer* $t \ge 2$ *with* $\gcd(i,2t) = 1$ *choosing* a, b *as in the proof of Theorem 2.3, we get the* $\mathbb{F}_q$*-linear MRD-code with dimension* $6t$ *and parameters* $(2t, 3t, q; 2t-1)$*:*

$$\{F_v \colon v = v_0 + \omega v_1,\ v_0, v_1 \in \mathbb{F}_{q^{3t}}\},$$

where $F_v : \mathbb{F}_{q^t} \times \mathbb{F}_{q^t} \to \mathbb{F}_{q^{3t}}$ *is defined by the rule*

$$F_v(x,y) = x^{q^i}(aA_0^{q^i} v_0^{q^i} + av_1^{q^i} + bA_0^{q^i} v_0^{q^{2t+i}} + bv_1^{q^{2t+i}}) +$$
$$y^{q^i}(av_0^{q^i} + bv_0^{q^{2t+i}}) - xA_1 v_0 - y v_1.$$

Applying [2, Theorem 3.1] one can construct other MRD-codes after decomposing $V(r, q^n)$ into a direct sum of $\mathbb{F}_{q^n}$-subspaces of dimensions 2 and 3 and choosing for each of them a maximum scattered subspace.

References

[1] S. Ball, A. Blokhuis and M. Lavrauw: Linear $(q+1)$-fold blocking sets in $PG(2, q^4)$, *Finite Fields Appl.* **6** n. 4 (2000), 294–301.

[2] D. Bartoli, M. Giulietti, G. Marino and O. Polverino: Maximum scattered linear sets and complete caps in Galois spaces, http://arxiv.org/abs/1512.07467, to appear in *Combinatorica*.

[3] T. Berger: Isometries for rank distance and permutation group of Gabidulin codes, *IEEE Trans. Inform. Theory* **49** (2003), 3016-3019.

[4] A. Blokhuis and M. Lavrauw: Scattered spaces with respect to a spread in $PG(n, q)$, *Geom. Dedicata* **81** No.1–3 (2000), 231–243.

[5] A. Blokhuis and M. Lavrauw: On two-intersection sets with respect to hyperplanes in projective spaces, *J. Combin. Theory Ser. A*, **99** No.2 (2002), 377–382.

[6] G. Bonoli and O. Polverino: The twisted cubic of $PG(3, q)$ and translation spreads of $H(q)$, *Discrete Math.* **296** (2005), 129–142.

[7] G. Bonoli and O. Polverino: $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$, *Innov. Incidence Geom.* (2005), 35–56.

[8] R. Calderbank and W.M. Kantor: The geometry of two-weight codes, *Bull. Lond. Math. Soc.* **18** (1986), 97–122.

[9] I. Cardinali, G. Lunardon, O. Polverino and R. Trombetti: Translation Spreads of the Classical Generalized Hexagon, *European J. Combin.* **23** (2002), 367–376.

[10] I. Cardinali, O. Polverino and R. Trombetti: Semifield planes of order q^4 with kernel $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$, *European J. Combin.* **27** (2006), 940–961.

[11] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$. Submitted manuscript. https://arxiv.org/abs/1607.06962

[12] B. Csajbók and C. Zanella: On the equivalence of linear sets, *Des. Codes Cryptogr.*, DOI 10.1007/s10623-015-0141-z.

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

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

[15] G. L. Ebert, G. Marino, O. Polverino and R. Trombetti: Infinite families of new semifields, *Combinatorica*, **29** n.6 (2009), 637–663.

[16] E. Gabidulin: Theory of codes with maximum rank distance, *Probl. Inf. Transm.* **21**(3) (1985), 3–16.

[17] E. Gabidulin.: Public-key cryptosystems based on linear codes over large alphabets: efficiency and weakness. *Codes and Cyphers*, 17–31. Formara Limited 1995.

[18] M. Gadouleau and Z. Yan: Properties of codes with the rank metric. *IEEE Global Telecommunications Conference 2006*, 1–5.

[19] D. Glynn and G. Steinke: Laguerre planes of even order and translation ovals, *Geom. Dedicata* **51** (1994), 105–112.

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

[21] R. Koetter and F. Kschischang: Coding for errors and erasure in random network coding. *IEEE Trans. Inform. Theory*, 54(8):3579–3591, Aug. 2008.

[22] M. Lavrauw: *Scattered Spaces with respect to Spreads and Eggs in Finite Projective Spaces*, Ph.D. Thesis, 2001.

[23] M. Lavrauw: Scattered spaces in Galois Geometry, *Contemporary Developments in Finite Fields and Applications*, 2016, 195–216.

[24] M. Lavrauw, G. Marino, O. Polverino and R. Trombetti: $\mathbb{F}_q$–pseudoreguli of $PG(3,q^3)$ and scattered semifields of order q^6, *Finite Fields Appl.*, **17** (2011), 225–239.

[25] M. Lavrauw, G. Marino, O. Polverino and R. Trombetti: Solution to an isotopism question concerning rank 2 semifields, *J. Combin. Des.*, **23** (2015), 60–77.

[26] M. Lavrauw, G. Marino, O. Polverino and R. Trombetti: The isotopism problem of a class of 6-dimensional rank 2 semifields and its solution, *Finite Fields Appl.* **34** (2015) , 250–264.

[27] M. Lavrauw and G. Van de Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* **56** (2010), 89–104.

[28] M. Lavrauw and G. Van de Voorde: Scattered linear sets and pseudoreguli, *Electron. J. Combin.* **20**(1) (2013).

[29] M. Lavrauw and G. Van de Voorde: Field reduction and linear sets in finite geometry, in: Gohar Kyureghyan, Gary L. Mullen, Alexander Pott (Eds.), Topics in Finite Fields, Contemp. Math. AMS (2015).

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

[31] G. Lunardon and O. Polverino: Blocking sets of size $q^t+q^{t-1}+1$, *J. Combin. Theory Ser. A* **90** (2000), 148–158.

[32] G. Lunardon: Linear $k-$blocking sets, *Combinatorica* **21(4)** (2001), 571–581.

[33] G. Lunardon: Translation ovoids, *J. Geom.* **76** (2003), 200–215.

[34] G. Lunardon, G. Marino, O. Polverino and R. Trombetti: Maximum scattered linear sets of pseudoregulus type and the Segre Variety $\mathcal{S}_{n,n}$, J. Algebraic. Combin. **39** (2014), 807–831.

[35] G. Lunardon and O. Polverino: Translation ovoids of orthogonal polar spaces, *Forum Math.* **16** (2004), 663–669.

[36] G. Lunardon, R. Trombetti and Y. Zhou: Generalized Twisted Gabidulin Codes, http://arxiv.org/abs/1507.07855.

[37] G. Marino and O. Polverino: On translation spreads of $H(q)$, *J. Algebraic Combin.* **42** n.3 (2005), 725–744.

[38] G. Marino, O. Polverino and R. Trombetti: On $\mathbb{F}_q$–linear sets of $\mathrm{PG}(3,q^3)$ and semifields, *J. Combin. Theory Ser. A* **114** (2007), 769–788.

[39] K. Morrison: Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes. *IEEE Trans. Inform. Theory*, **60** n.11 (2014), 7035–7046.

[40] O. Polverino: Linear sets in finite projective spaces, *Discrete Math.* **310** (2010), 3096–3107.

[41] P. Polito and O. Polverino: On small blocking sets, *Combinatorica* **18** No.1 (1998), 133–137.

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

Bence Csajbók
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli",
I– 81100 Caserta, Italy
and
MTA–ELTE Geometric and Algebraic Combinatorics Research Group,
Eötvös Loránd University,
H– 1117 Budapest, Pázmány Péter Sétány 1/C, Hungary
csajbok.bence@gmail.com

Giuseppe Marino, Olga Polverino and Ferdinando Zullo
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli",
I– 81100 Caserta, Italy
giuseppe.marino@unina2.it, *olga.polverino@unina2.it*, *ferdinando.zullo@unina2.it*