A new family of MRD-codes

Bence Csajbók, Giuseppe Marino, Olga Polverino, Corrado Zanella *

Abstract

We introduce a family of linear sets of $\mathrm{PG}(1, q^{2n})$ arising from maximum scattered linear sets of pseudoregulus type of $\mathrm{PG}(3, q^n)$. For $n = 3, 4$ and for certain values of the parameters we show that these linear sets of $\mathrm{PG}(1, q^{2n})$ are maximum scattered and they yield new MRD-codes with parameters $(6, 6, q; 5)$ for $q > 2$ and with parameters $(8, 8, q; 7)$ for q odd.

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

Keywords: Scattered subspace, MRD-code, linear set

1 Introduction

Linear sets are natural generalizations of subgeometries. Let $\Lambda = \mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(r-1, q^n)$, where V is a vector space of dimension r over $\mathbb{F}_{q^n}$. A point set L of Λ 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 a k-dimensional $\mathbb{F}_q$-vector subspace U of V, i.e.

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

The maximum field of linearity of an $\mathbb{F}_q$-linear set L_U is $\mathbb{F}_{q^t}$ if $t \mid n$ is the largest integer such that L_U is an $\mathbb{F}_{q^t}$-linear set.

Two linear sets L_U and L_W of Λ are said to be $\mathrm{P\Gamma L}$-*equivalent* (or simply *equivalent*) if there is an element ϕ in $\mathrm{P\Gamma L}(r, q^n)$, the collineation group of

---

[*] 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). The first author was partially supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and by OTKA Grant No. K 124950.

Λ, such that $L_U^{\phi} = L_W$. It may happen that two $\mathbb{F}_q$–linear sets L_U and L_W of Λ are PΓL-equivalent even if the two $\mathbb{F}_q$-vector subspaces U and W are not in the same orbit of $\Gamma\mathrm{L}(r, q^n)$, the group of invertible $\mathbb{F}_{q^n}$-semilinear transformations of V (see [8] and [5] for further details).

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

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

In [11] the Singleton bound for an $m \times n$ rank metric code $\mathcal{C}$ with minimum rank distance d was proved:

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

If this bound is achieved, then $\mathcal{C}$ is an MRD-code. MRD-codes have various applications in communications and cryptography; see for instance [12, 17]. More properties of MRD-codes can be found in [11, 12, 13, 33]. 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 $(m, n, q; d)$.

In [35, Section 4], the author showed that scattered linear sets of $\mathrm{PG}(1, q^m)$ of rank m yield $\mathbb{F}_q$-linear MRD-codes of dimension $2m$ and minimum distance $m - 1$. Also, codes arising in this way have *middle nucleus* of order q^m (which is an invariant with respect to the equivalence on MRD-codes, see Section 6). In Proposition 6.1 we prove that every code with these parameters can be obtained from a suitable scattered linear set of rank m of $\mathrm{PG}(1, q^m)$. The correspondence between MRD codes and linear sets of $\mathrm{PG}(1, q^m)$ has been recently generalized in [6]. The number of non-equivalent MRD-codes obtained from a scattered linear set of $\mathrm{PG}(1, q^m)$ of rank m was studied in [5, Section 5.4]. In [24] the author investigated in detail the relationship between linear sets of $\mathrm{PG}(n - 1, q^n)$ of rank n and $\mathbb{F}_q$-linear MRD-codes.

So far, the known non-equivalent families of $\mathbb{F}_q$-linear MRD-codes of dimension $2m$, minimum distance $m - 1$ and with middle nucleus $\mathbb{F}_{q^m}$ arise from the following maximum scattered $\mathbb{F}_q$–vector subspaces of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$:

1. $U_1 := \{(x, x^{q^s}) \colon x \in \mathbb{F}_{q^m}\}$, $1 \leq s \leq m - 1$ $\gcd(s, m) = 1$ ([4]) gives Gabidulin codes when $s = 1$, and generalized Gabidulin codes when $s > 1$;

2. $U_2 := \{(x, \delta x^{q^s} + x^{q^{m-s}}) \colon x \in \mathbb{F}_{q^m}\}$, $\mathrm{N}_{q^m/q}(\delta) \neq 1$ ([1]), $\gcd(s,m) = 1$ ([27] for $s = 1$) gives MRD-codes found by Sheekey in [35] as part of a larger family. The equivalence issue for these codes was studied also by Lunardon, Trombetti and Zhou in [28].

In this paper we present a family of $\mathbb{F}_q$-linear sets of rank m of $\mathrm{PG}(1, q^m)$, $m = 2n$ and $n > 1$, arising from $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3, q^n)$ of pseudoregulus type. These linear sets are defined by the following $\mathbb{F}_q$-vector subspaces of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$:

$$U_{b,s} := \{(x, bx^{q^s} + x^{q^{s+n}}) \colon x \in \mathbb{F}_{q^{2n}}\} \tag{2}$$

with $\mathrm{N}_{q^{2n}/q^n}(b) \neq 1$, $1 \leq s \leq 2n-1$ and $\gcd(s,n) = 1$.

We will show that each point of $L_{U_{b,s}}$ has weight at most 2 (cf. Proposition 4.1) and when $L_{U_{b,s}}$ is scattered and $m > 4$, then, as we will see in Section 6, the corresponding MRD-code is not equivalent to any previously known MRD-code with the same parameters. Finally, in the last section, we exhibit for $m = 6$ and $m = 8$ infinite examples of scattered $\mathbb{F}_q$-subspaces of type $U_{b,s}$ and hence new infinite families of MRD-codes.

2 Linear sets

Let L_U be an $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(r-1, q^n)$, $q = p^h$, p prime, of rank k. 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, 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 $w_{L_U}(\Omega) := \dim_{\mathbb{F}_q}(W \cap U) = i$, we say that Ω has *weight* i w.r.t. L_U. Hence 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 [34] and [23].

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 $q^{k-1} + q^{k-2} + \cdots + q + 1$. The associated $\mathbb{F}_q$–vector subspace U is said to be *scattered*. 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. For a recent survey on the theory of scattered spaces in Galois Geometry and its applications see [19].

---

[1] $\mathrm{N}_{q^m/q}(\cdot)$ denotes the norm function from $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

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 [18, 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 [2, Section 3]. Very recently in [3, Theorem 1.2] and in [6, Section 2] maximum scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(r-1,q^n)$ of rank $rn/2$ have been constructed for any integers $r,n \geq 2$, rn even, and for any prime power $q \geq 2$.

2.1 Scattered linear sets of pseudoregulus type in $\mathrm{PG}(3,q^n)$

In [26], generalizing results contained in [32], [20] and [22], a family of maximum scattered linear sets of $\mathrm{PG}(2h-1,q^n)$ of rank hn $(h,n \geq 2)$, called of *pseudoregulus type*, is introduced. In particular, a maximum scattered $\mathbb{F}_q$–linear set L_U of $\Lambda=\mathrm{PG}(3,q^n)$ of rank $2n$ is of *pseudoregulus type* if (i) there exist q^n+1 pairwise disjoint lines of L_U of weight n w.r.t. L_U, say $s_1,s_2,\ldots,s_{q^n+1}$;
(ii) there exist exactly two skew lines t_1 and t_2 of Λ, disjoint from L_U, such that $t_j \cap s_i \neq \emptyset$ for each $i=1,\ldots,q^n+1$ and for each $j=1,2$.

The set of lines $\mathcal{P}_{L_U}=\{s_i \colon i=1,\ldots,q^n+1\}$ is called the $\mathbb{F}_q$*–pseudoregulus* (or simply *pseudoregulus*) of Λ associated with L_U and t_1 and t_2 are the *transversal lines* of $\mathcal{P}_{L_U}$ (or *transversal lines* of L_U). Note that by [26, Corollary 3.3], if $n>2$ the pseudoregulus $\mathcal{P}_{L_U}$ associated with L_U and its transversal lines are uniquely determined.

In [20, Sec. 2] and in [26, Theorems 3.5 and 3.9], $\mathbb{F}_q$–linear sets of pseudoregulus type of $\mathrm{PG}(2h-1,q^n)$ of rank hn $(h,n \geq 2)$ have been algebraically characterized. In particular, in $\mathrm{PG}(3,q^n)$ we have the following result.

Theorem 2.1. *Let $t_1=\mathrm{PG}(U_1,\mathbb{F}_{q^n})$ and $t_2=\mathrm{PG}(U_2,\mathbb{F}_{q^n})$ be two disjoint lines of $\Lambda=\mathrm{PG}(V,\mathbb{F}_{q^n})=\mathrm{PG}(3,q^n)$ and let Φ_f be a strictly semilinear collineation between t_1 and t_2 defined by the $\mathbb{F}_{q^n}$-semilinear map f with companion automorphism an element $\sigma \in Aut(\mathbb{F}_{q^n})$ such that $Fix(\sigma)=\mathbb{F}_q$. Then, for each $\rho \in \mathbb{F}^*_{q^n}$, the set*

$$L_{\rho,f}=\{\langle \mathbf{u}+\rho f(\mathbf{u})\rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U_1 \setminus \{\mathbf{0}\}\}$$

is an $\mathbb{F}_q$-linear set of Λ of pseudoregulus type whose associated pseudoregulus is $\mathcal{P}_{L_{\rho,f}}=\{\langle P, P^{\Phi_f}\rangle : P \in t_1\}$, with transversal lines t_1 and t_2.

Conversely, each $\mathbb{F}_q$–linear set of pseudoregulus type of $\Lambda = \mathrm{PG}(3, q^n)$ *can be obtained as described above.*

In [26], $\mathbb{F}_q$-linear sets of pseudoregulus type of the projective line $\Lambda = \mathrm{PG}(V, \mathbb{F}_{q^n}) = \mathrm{PG}(1, q^n)$ ($n \geq 2$) are also introduced. Let $P_1 = \langle \mathbf{w} \rangle$ and $P_2 = \langle \mathbf{v} \rangle$ be two distinct points of the line Λ and let τ be an $\mathbb{F}_q$-automorphism of $\mathbb{F}_{q^n}$ such that $Fix(\tau) = \mathbb{F}_q$; then for each $\rho \in \mathbb{F}^*_{q^n}$ the set

$$W_{\rho,\tau} = \{\lambda \mathbf{w} + \rho \lambda^\tau \mathbf{v} \colon \lambda \in \mathbb{F}_{q^n}\}, \tag{3}$$

is an $\mathbb{F}_q$–vector subspace of V of dimension n and $L_{\rho,\tau} := L_{W_{\rho,\tau}}$ is a maximum scattered $\mathbb{F}_q$-linear set of Λ. The linear sets $L_{\rho,\tau}$ are called of *pseudoregulus type* and the points P_1 and P_2 are their *transversal points*. Also, if $n > 2$, then these transversal points are uniquely determined ([26, Prop. 4.3]). For more details on such linear sets see [9]. Also, by [26, Remark 4.5], if L_U is an $\mathbb{F}_q$-linear set of pseudoregulus type of $\mathrm{PG}(3, q^n)$, and s is a line of weight n w.r.t. L_U, then $L_U \cap s$ is an $\mathbb{F}_q$-linear set of pseudoregulus type of the line s whose transversal points are the intersection points of s with the transversal lines of $\mathcal{P}_{L_U}$ (see also [21, Prop. 2.5] and [31, Theorem 2.8] for further details).

3 Linear sets and dual linear sets in $\mathrm{PG}(1, q^n)$

Let $\mathbb{V} = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ and let L_U be an $\mathbb{F}_q$–linear set of rank n of $\mathrm{PG}(1, q^n) = \mathrm{PG}(\mathbb{V}, \mathbb{F}_{q^n})$. We can always assume (up to a projectivity) that L_U does not contain the point $\langle (0, 1) \rangle_{\mathbb{F}_{q^n}}$. Then $U = U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\}$, for some q-polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$. For the sake of simplicity we will write L_f instead of L_{U_f} to denote the linear set defined by U_f.

Consider the non-degenerate symmetric bilinear form of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ defined by the following rule

$$< x, y > := \mathrm{Tr}_{q^n/q}(xy).(^2) \tag{4}$$

Then the *adjoint map* $\hat{f}$ of an $\mathbb{F}_q$-linear map $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ of $\mathbb{F}_{q^n}$ (with respect to the bilinear form (4)) is

$$\hat{f}(x) := \sum_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}. \tag{5}$$

---

[2] $\mathrm{Tr}_{q^n/q}(\cdot)$ denotes the trace function from $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Let $\eta : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{F}_{q^n}$ be the non-degenerate alternating bilinear form of $\mathbb{V}$ defined by $\eta((x,y),(u,v)) = xv - yu$. Then η induces a symplectic polarity τ on the line $\mathrm{PG}(\mathbb{V}, \mathbb{F}_{q^n})$ and

$$\eta'((x,y),(u,v)) := \mathrm{Tr}_{q^n/q}(\eta((x,y),(u,v))) = \mathrm{Tr}_{q^n/q}(xv - yu) \tag{6}$$

is a non-degenerate alternating bilinear form on $\mathbb{V}$, when $\mathbb{V}$ is regarded as a $2n$-dimensional vector space over $\mathbb{F}_q$. We will always denote in the paper by $\perp$ and $\perp'$ the orthogonal complement maps defined by η and η' on the lattices of the $\mathbb{F}_{q^n}$-subspaces and the $\mathbb{F}_q$-subspaces of $\mathbb{V}$, respectively. Direct calculation shows that

$$U_f^{\perp'} = U_{\hat{f}}, \tag{7}$$

and the $\mathbb{F}_q$–linear set of rank n of $\mathrm{PG}(\mathbb{V}, \mathbb{F}_{q^n})$ defined by the orthogonal complement $U^{\perp'}$ is called *the dual linear set of* L_U with respect to the polarity τ.

Recall the following lemma.

Lemma 3.1 ([3, Lemma 2.6], [5, Lemma 3.1])**.** *Let* $L_f = \{\langle (x, f(x))\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\}$ *be an* $\mathbb{F}_q$*–linear set of* $\mathrm{PG}(1, q^n)$ *of rank* n*, with* $f(x)$ *a* q*-polynomial over* $\mathbb{F}_{q^n}$*, and let* $\hat{f}$ *be the adjoint of* f *with respect to the bilinear form (4). Then for each point* $P \in \mathrm{PG}(1, q^n)$ *we have* $w_{L_f}(P) = w_{L_{\hat{f}}}(P)$*. In particular,* $L_f = L_{\hat{f}}$ *and the maps defined by* $f(x)/x$ *and* $\hat{f}(x)/x$ *have the same image.*

4 From the geometry in $\mathrm{PG}(3, q^n)$ to the geometry in $\mathrm{PG}(1, q^{2n})$

From now on, we will consider $\mathbb{V} = \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ both as a 2-dimensional vector space over $\mathbb{F}_{q^{2n}}$ and as a 4-dimensional vector space over $\mathbb{F}_{q^n}$. In the former case the linear set of $\Sigma_1 := \mathrm{PG}(\mathbb{V}, \mathbb{F}_{q^{2n}}) = \mathrm{PG}(1, q^{2n})$ defined by an $\mathbb{F}_q$-subspace $U \leq \mathbb{V}$ will be denoted as L_U, in the latter case the linear set of $\Sigma_3 := \mathrm{PG}(\mathbb{V}, \mathbb{F}_{q^n}) = \mathrm{PG}(3, q^n)$ defined by U will be denoted by $\bar{L}_U$.

Consider the following two skew lines of Σ_3: $\ell_0 := \{\langle (x, 0)\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^{2n}}^*\}$ and $\ell_1 := \{\langle (0, y)\rangle_{\mathbb{F}_{q^n}} : y \in \mathbb{F}_{q^{2n}}^*\}$. By Theorem 2.1, $\mathbb{F}_q$-linear sets of pseudoregulus type in Σ_3 with transversal lines ℓ_0 and ℓ_1 are of the form $\bar{L}_f := \bar{L}_{U_f}$, where $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^{2n}}\}$, and $f(x)$ is a strictly $\mathbb{F}_{q^n}$-semilinear invertible map of $\mathbb{F}_{q^{2n}}$ with companion automorphism σ, $Fix(\sigma) = \mathbb{F}_q$. It is easy to see that this happens if and only if $f(x) = \alpha x^\sigma + \beta x^{\sigma q^n}$, where

$\sigma\colon x \mapsto x^{q^s}$, $1 \le s \le 2n-1$, $\gcd(s,n)=1$, and $\mathrm{N}_{q^{2n}/q^n}(\alpha) \neq \mathrm{N}_{q^{2n}/q^n}(\beta)$. That is,

$$U_f = \{(x, \alpha x^{\sigma} + \beta x^{\sigma q^n})\colon x \in \mathbb{F}_{q^{2n}}\}, \tag{8}$$

with the same conditions as above. In Σ_1 the $\mathbb{F}_q$-linear set $L_f := L_{U_f}$ is not necessarily scattered, but as the next result shows, it cannot contain points with weight greater than two.

Proposition 4.1. *Each point of the* $\mathbb{F}_q$*-linear set* L_f *of* $\mathrm{PG}(1,q^{2n})$*,* $n \ge 2$*, where*

$$U_f = \{(x, f(x))\colon x \in \mathbb{F}_{q^{2n}}\},$$

with $f(x) = \alpha x^{\sigma} + \beta x^{\sigma q^n}$*,* $\sigma\colon x \mapsto x^{q^s}$*,* $1 \le s \le 2n-1$*,* $\gcd(s,n)=1$*, and* $\mathrm{N}_{q^{2n}/q^n}(\alpha) \neq \mathrm{N}_{q^{2n}/q^n}(\beta)$*, has weight at most two.*

Proof. We first recall that the pseudoregulus associated with $\bar{L}_f$ in $\Sigma_3 = \mathrm{PG}(3,q^n)$ consists of q^n+1 lines, and these are the only lines with weight n w.r.t. $\bar{L}_f$ ([26, Prop. 3.2]).

Let $Q := \langle (x_0, f(x_0)) \rangle_{\mathbb{F}_{q^{2n}}}$ be a point of L_f. In Σ_3 this point corresponds to a line ℓ_Q disjoint from both ℓ_0 and ℓ_1 and meeting at least one line of the pseudoregulus associated with $\bar{L}_f$, say m. Note that $w_{L_f}(Q) = w_{\bar{L}_f}(\ell_Q)$. By [1, Theorem 5.1] a plane of Σ_3 has weight either n or $n+1$ w.r.t. $\bar{L}_f$, hence if the weight of Q w.r.t. L_f is greater than one, then the plane π of Σ_3 spanned by the lines ℓ_Q and m has weight $n+1$. Since $\ell_Q \cap m$ is a point with weight one w.r.t. $\bar{L}_f$, the Grassmann formula gives that the weight of ℓ_Q w.r.t $\bar{L}_f$ is two and hence the weight of Q w.r.t. L_f is two. $\square$

5 A family of $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1,q^{2n})$

In this section we investigate the family of $\mathbb{F}_q$–linear sets of $\mathrm{PG}(1,q^{2n})$ defined by $\mathbb{F}_q$–vector subspaces of form (8). Let U_f and U_g be two $\mathbb{F}_q$–vector subspaces of $\mathbb{V} = \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ of form (8), where $f(x) = \alpha x^{q^s} + \beta x^{q^{s+n}}$ and $g(x) = \alpha' x^{q^s} + \beta' x^{q^{s+n}}$, with $1 \le s \le 2n-1$ and $\gcd(s,n)=1$. Since we are interested in the study of scattered linear sets of $\mathrm{PG}(1,q^{2n})$ not of pseudoregulus type, we can assume $\alpha\beta \neq 0$ (cf. [26, Sec. 4]). If $\mathrm{N}_{q^{2n}/q^n}(\alpha\beta') = \mathrm{N}_{q^{2n}/q^n}(\alpha'\beta)$ then there exists $a \in \mathbb{F}^*_{q^{2n}}$ such that $\beta\alpha' = \beta'\alpha a^{q^s(q^n-1)}$ and direct computations show that $U_f^{\varphi} = U_g$, where

$$\varphi\colon (x,y) \in \mathbb{V} \mapsto (xa, y a^{q^s} \alpha'/\alpha) \in \mathbb{V}.$$

From the previous arguments it follows that L_f is defined, up to the action of the group $\mathrm{GL}(2,q^n)$, by an $\mathbb{F}_q$–vector subspace of $\mathbb{V}$ of type

$$U_{b,s} := \{(x, bx^{q^s} + x^{q^{s+n}}) \colon x \in \mathbb{F}_{q^{2n}}\}, \tag{9}$$

with $b \in \mathbb{F}^*_{q^{2n}}$ and $1 \leq s \leq 2n-1$ such that $\mathrm{N}_{q^{2n}/q^n}(b) \neq 1$ and $\gcd(s,n) = 1$. We will denote by $L_{b,s}$ the corresponding $\mathbb{F}_q$–linear set $L_{U_{b,s}}$.

Also we can restrict our study to the choice of the integers s' such that $1 \leq s \leq n$ and $\gcd(s,n) = 1$. Indeed, by using the notation of Section 3, we have

$$U^{\perp'}_{b,s} = \{(x, b^{q^{2n-s}} x^{q^{2n-s}} + x^{q^{n-s}}) \colon x \in \mathbb{F}_{q^{2n}}\} = U_{b^{q^{2n-s}}, 2n-s}$$

and it can be easily seen that $U_{b,s}$ and $U^{\perp'}_{b,s}$ are equivalent via the linear invertible map $\phi \colon (x,y) \in \mathbb{V} \mapsto (\alpha y, \beta x) \in \mathbb{V}$, where α is any element satisfying $\alpha^{q^n-1} = -\frac{1}{b^{q^n-1}}$ and $\beta = (b^{2q^n}\alpha^{q^n} + \alpha)^{q^{n-s}}$.

Moreover we have the following result.

Proposition 5.1. *Two $\mathbb{F}_q$-subspaces $U_{b,s}$ and $U_{\bar{b},\bar{s}}$ of $\mathbb{V} = \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ of form (9) with $b, \bar{b} \in \mathbb{F}^*_{q^{2n}}$, $N_{q^{2n}/q^n}(b) \neq 1$, $N_{q^{2n}/q^n}(\bar{b}) \neq 1$, $1 \leq s, \bar{s} < n$ and $\gcd(n,s) = \gcd(n,\bar{s}) = 1$, are $\Gamma\mathrm{L}(2,q^{2n})$-equivalent if and only if either*

$$s = \bar{s} \quad \textit{and} \quad \mathrm{N}_{q^{2n}/q^n}(\bar{b}) = \mathrm{N}_{q^{2n}/q^n}(b)^\sigma$$

or

$$s + \bar{s} = n \quad \textit{and} \quad \mathrm{N}_{q^{2n}/q^n}(\bar{b})\, \mathrm{N}_{q^{2n}/q^n}(b)^\sigma = 1,$$

for some automorphism $\sigma \in Aut(\mathbb{F}_{q^n})$.

Proof. $U_{b,s}$ and $U_{\bar{b},\bar{s}}$ are $\Gamma\mathrm{L}(2,q^{2n})$-equivalent if and only if there exist elements $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^{2n}}$, with $\alpha\delta \neq \beta\gamma$ and an automorphism $\sigma \in Aut(\mathbb{F}_{q^{2n}})$ such that

$$\forall\, x \in \mathbb{F}_{q^{2n}}, \exists\, y \in \mathbb{F}_{q^{2n}} : \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x^\sigma \\ (bx^{q^s} + x^{q^{s+n}})^\sigma \end{pmatrix} = \begin{pmatrix} y \\ \bar{b} y^{q^{\bar{s}}} + y^{q^{\bar{s}+n}} \end{pmatrix}.$$

Put $z := x^\sigma$, the last equation implies that for each $z \in \mathbb{F}_{q^{2n}}$, there exists $y \in \mathbb{F}_{q^{2n}}$ such that

$$\begin{cases} \alpha z + \beta(b^\sigma z^{q^s} + z^{q^{n+s}}) = y, \\ \gamma z + \delta(b^\sigma z^{q^s} + z^{q^{n+s}}) = \bar{b} y^{q^{\bar{s}}} + y^{q^{n+\bar{s}}}. \end{cases} \tag{10}$$

Putting the first in the second equation of System (10), we get that

$$\gamma z+\delta(b^{\sigma}z^{q^s}+z^{q^{n+s}}) = \bar{b}(\alpha z+\beta(b^{\sigma}z^{q^s}+z^{q^{n+s}}))^{q^{\bar{s}}}+(\alpha z+\beta(b^{\sigma}z^{q^s}+z^{q^{n+s}}))^{q^{n+\bar{s}}} \tag{11}$$

for each $z \in \mathbb{F}_{q^{2n}}$.

If $s = \bar{s}$, since the monomials $z, z^{q^s}, z^{q^{2s}}, z^{q^{n+s}}, z^{q^{n+2s}}$ are pairwise distinct modulo $z^{q^{2n}} - z$, from the previous polynomial identity we get

$$\begin{cases} \gamma = 0 \\ \delta b^{\sigma} = \bar{b}\alpha^{q^s} \\ \delta = \alpha^{q^{n+s}} \\ \bar{b}\beta^{q^s} b^{\sigma q^s} + \beta^{q^{n+s}} = 0 \\ \bar{b}\beta^{q^s} + \beta^{q^{n+s}} b^{\sigma q^{n+s}} = 0. \end{cases} \tag{12}$$

Since $\mathrm{N}_{q^{2n}/q^n}(b) \neq 1$, System (12) is equivalent to

$$\begin{cases} \gamma = 0 \\ \beta = 0 \\ \delta b^{\sigma} = \bar{b}\alpha^{q^s} \\ \delta = \alpha^{q^{n+s}}, \end{cases}$$

which admits solutions if and only if $\mathrm{N}_{q^{2n}/q^n}(\bar{b}) = \mathrm{N}_{q^{2n}/q^n}(b)^{\sigma}$, with $\sigma \in Aut(\mathbb{F}_{q^n})$.

If $s \neq \bar{s}$, since $1 \leq s, \bar{s} < n$ and $\gcd(s,n) = \gcd(\bar{s},n) = 1$, we get

$$\{z^{q^s}, z^{q^{\bar{s}}}\} \cap \{z, z^{q^{n+s}}, z^{q^{n+\bar{s}}}, z^{q^{s+\bar{s}}}, z^{q^{n+s+\bar{s}}}\} = \emptyset$$

modulo $z^{q^{2n}} - z$. Hence polynomial identity (11) yields $\alpha = \delta = 0$ and Equation (11) becomes

$$\gamma z = (\bar{b}\beta^{q^{\bar{s}}} b^{\sigma q^{\bar{s}}} + \beta^{q^{n+\bar{s}}}) z^{q^{s+\bar{s}}} + (\bar{b}\beta^{q^{\bar{s}}} + \beta^{q^{n+\bar{s}}} b^{\sigma q^{n+\bar{s}}}) z^{q^{n+s+\bar{s}}}$$

for each $z \in \mathbb{F}_{q^{2n}}$. Also, since $s + \bar{s} < 2n$, the monomials z and $z^{q^{s+\bar{s}}}$ are different modulo $z^{q^{2n}} - z$. Hence, if $s + \bar{s} \neq n$ we immediately get $\gamma = 0$, a contradiction. It follows that $s + \bar{s} = n$ and comparing the coefficients of the terms of degree 1 and $q^{s+\bar{s}}$ we get

$$\begin{cases} \gamma = \bar{b}\beta^{q^{\bar{s}}} + \beta^{q^{n+\bar{s}}} b^{\sigma q^{n+\bar{s}}} \\ \bar{b}\beta^{q^{\bar{s}}} b^{\sigma q^{\bar{s}}} + \beta^{q^{n+\bar{s}}} = 0, \end{cases}$$

which admits solutions if and only if $\mathrm{N}_{q^{2n}/q^n}(\bar{b} b^{\sigma q^{\bar{s}}}) = 1$, i.e. if and only if $\mathrm{N}_{q^{2n}/q^n}(\bar{b})\, \mathrm{N}_{q^{2n}/q^n}(b^{q^{\bar{s}}})^{\sigma} = 1$, for some automorphism $\sigma \in Aut(\mathbb{F}_{q^n})$. $\square$

We finish this section by determining the linear automorphism group of $U_{b,s}$ and with some results on the geometric structure of a linear set $L_{b,s}$.

Corollary 5.2. *The $\mathbb{F}_{q^{2n}}$-linear automorphism group $\mathcal{G}_{b,s}$ of an $\mathbb{F}_q$–vector subspace $U_{b,s}$ of $\mathbb{V} = \mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ of form (9) consists of the following matrices*

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{q^s} \end{pmatrix},$$

with $\alpha \in \mathbb{F}^*_{q^n}$.

Proof. In the previous theorem choosing $s = \bar{s}$ and $b = \bar{b}$, by System (12) we get $\beta = \gamma = 0$ and $\delta = \alpha^{q^s} = \alpha^{q^{n+s}}$. The assertion follows. $\square$

The previous corollary allows us to prove the following result.

Proposition 5.3. *Let $L_{b,s}$ be the $\mathbb{F}_q$–linear set of $\mathrm{PG}(1, q^{2n})$ of rank $2n$ defined by an $\mathbb{F}_q$–vector subspace $U_{b,s}$ of type (9) and let $P\mathcal{G}_{b,s}$ be the projectivity group induced on the line $\mathrm{PG}(1, q^{2n})$ by $\mathcal{G}_{b,s}$. Then the following properties hold:*

i) the linear collineation group $P\mathcal{G}_{b,s}$ preserves $L_{b,s}$, it has order $\frac{q^n-1}{q-1}$, fixes the two points $\langle(1, 0)\rangle_{\mathbb{F}_{q^{2n}}}$ and $\langle(0, 1)\rangle_{\mathbb{F}_{q^{2n}}}$ and any other point–orbit has size $\frac{q^n-1}{q-1}$;

ii) $L_{b,s}$ is a union of orbits of points under the $P\mathcal{G}_{b,s}$–action;

iii) all points of $L_{b,s}$ belonging to the same $P\mathcal{G}_{b,s}$–orbit have the same weight w.r.t. $L_{b,s}$.

Proof. Let ϕ_λ be the linear collineation of $P\mathcal{G}_{b,s}$ induced by the element $\varphi_\lambda := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{q^s} \end{pmatrix} \in \mathcal{G}_{b,s}$, with $\lambda \in \mathbb{F}^*_{q^n}$. Since $\mathrm{Fix}(\sigma) \cap \mathbb{F}^*_{q^n} = \mathbb{F}_q$, the group $P\mathcal{G}_{b,s}$ has order $\frac{q^n-1}{q-1}$. Also, it can be easily seen that if P is a point of $\mathrm{PG}(1, q^{2n})$ different from $\langle(1, 0)\rangle_{\mathbb{F}_{q^{2n}}}$ and $\langle(0, 1)\rangle_{\mathbb{F}_{q^{2n}}}$, then $P^{\phi_\lambda} = P$ if and only if ϕ_λ is the identity map. Hence Statements *i)* and *ii)* follow.

Let now $P = \langle(x_0, f(x_0))\rangle_{\mathbb{F}_{q^{2n}}}$ be a point of $L_{b,s}$, i.e. $f(x_0) = bx_0^{q^s} + x_0^{q^{n+s}}$. Then $P^{\phi_\lambda} = \langle(\lambda x_0, f(\lambda x_0))\rangle_{\mathbb{F}_{q^{2n}}}$ and

$$w_{L_{b,s}}(P) = \dim_q(\langle(x_0, f(x_0))\rangle_{\mathbb{F}_{q^{2n}}} \cap U_{b,s}) = \dim_q \varphi_\lambda(\langle(x_0, f(x_0))\rangle_{\mathbb{F}_{q^{2n}}} \cap U_{b,s})$$

$$= \dim_q \Big(\langle(\lambda x_0, f(\lambda x_0))\rangle_{\mathbb{F}_{q^{2n}}} \cap \varphi_\lambda(U_{b,s})\Big)$$

$$= \dim_q \Big(\langle (\lambda x_0, f(\lambda x_0)) \rangle_{\mathbb{F}_{q^{2n}}} \cap U_{b,s} \Big) = w_{L_{b,s}}(P^{\phi_\lambda}),$$

and Property *iii)* is proved. □

From the previous proposition we get the following result.

Corollary 5.4. *Let $L_{b,s}$ be the $\mathbb{F}_q$–linear set of $\mathrm{PG}(1,q^{2n})$ of rank $2n$ defined by an $\mathbb{F}_q$–vector subspace $U_{b,s}$ of type (9). The size of $L_{b,s}$ is a multiple of $\frac{q^n-1}{q-1}$. Furthermore, the set of points of weight 2 w.r.t. $L_{b,s}$ is a union of orbits under the action of the linear collineation group $P\mathcal{G}_{b,s}$.* □

6 Scattered $\mathbb{F}_q$-subspaces of type $U_{b,s}$ and the corresponding MRD-codes

We start this section by recalling some important notion regarding RD-codes. The *middle nucleus* of a code $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ (cf. [29], or [30] where the term *left idealiser* was used), is defined as

$$\mathcal{N}(\mathcal{C}) := \{Z \in \mathbb{F}_q^{m\times m} \colon ZC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\},$$

and by [29, Theorem 5.4] it turns out to be a field of order at least q.

We will use the following equivalence definition for codes of $\mathbb{F}_q^{m\times m}$. If $\mathcal{C}$ and $\mathcal{C}'$ are two codes then they are equivalent if and only if there exist two invertible matrices $A, B \in \mathbb{F}_q^{m\times m}$ and a field automorphism σ such that $\{AC^\sigma B \colon C \in \mathcal{C}\} = \mathcal{C}'$, or $\{AC^{T\sigma}B \colon C \in \mathcal{C}\} = \mathcal{C}'$, where T denotes transposition. The code $\mathcal{C}^T$ is also called the *adjoint* of $\mathcal{C}$.

In [35, Section 5] Sheekey showed that scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1,q^m)$ of rank m yield $\mathbb{F}_q$-linear MRD-codes with parameters $(m,m,q;m-1)$. We briefly recall here the construction from [35]. Let $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^m}\}$ be any maximum scattered $\mathbb{F}_q$–vector subspace of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ for some q-polynomial $f(x)$ over $\mathbb{F}_{q^m}$. Then, after fixing an $\mathbb{F}_q$-bases for $\mathbb{F}_{q^m}$, the set of $\mathbb{F}_q$-linear maps of $\mathbb{F}_{q^m}$

$$\mathcal{C}_f := \{x \mapsto af(x) + bx \colon a, b \in \mathbb{F}_{q^m}\} \tag{13}$$

corresponds to $m \times m$ matrices over $\mathbb{F}_q$ forming an $\mathbb{F}_q$-linear MRD-code with parameters $(m,m,q;m-1)$. Also, since $\mathcal{C}_f$ is an $\mathbb{F}_{q^m}$-subspace of $End(\mathbb{F}_{q^m}, \mathbb{F}_q)$, its middle nucleus $\mathcal{N}(\mathcal{C}_f)$ contains the set of scalar maps $\mathcal{F}_m := \{x \in \mathbb{F}_{q^m} \mapsto \alpha x \in \mathbb{F}_{q^m} : \alpha \in \mathbb{F}_{q^m}\}$, i.e. $|\mathcal{N}(\mathcal{C}_f)| \geq q^m$.

On the other hand $\mathcal{N}(\mathcal{C}_f)$ is an $\mathbb{F}_q$-subspace of invertible maps together with the zero map (cf. [29, Corollary 5.6]), it is also an MRD-code with parameters $(m, m, q; m)$. Then (1) gives $|\mathcal{N}(\mathcal{C}_f)| \leq q^m$, thus $\mathcal{N}(\mathcal{C}_f) = \mathcal{F}_m$.

Regarding the converse we can state the following.

Proposition 6.1. *If $\mathcal{C}$ is an MRD-code with parameters $(m, m, q; m-1)$ and with middle nucleus isomorphic to $\mathbb{F}_{q^m}$, then $\mathcal{C}$ is equivalent to some code $\mathcal{C}_f$ (cf. (13)).*

Proof. By using a ring isomorphism between $\mathbb{F}_q^{m\times m}$ and $End(\mathbb{F}_{q^m}, \mathbb{F}_q)$, we may suppose that $\mathcal{C} \subset End(\mathbb{F}_{q^m}, \mathbb{F}_q)$. Since $\mathcal{N}(\mathcal{C}) \setminus \{\mathbf{0}\}$ and $\mathcal{F}_m \setminus \{\mathbf{0}\}$ are two Singer cyclic subgroups of $\mathrm{GL}(\mathbb{F}_{q^m}, \mathbb{F}_q)$, there exists $H \in \mathrm{GL}(\mathbb{F}_{q^m}, \mathbb{F}_q)$ such that

$$H^{-1} \circ \mathcal{N}(\mathcal{C}) \circ H = \mathcal{F}_m,$$

see for example [15, pg. 187]. With $\mathcal{C}' := H^{-1} \circ \mathcal{C}$ we can see that $\mathcal{N}(\mathcal{C}') = \mathcal{F}_m$. It means that $\mathcal{C}'$ is a 2-dimensional vector space over $\mathcal{F}_m$ and hence it can be written as

$$\mathcal{C}' = \{\alpha r(x) + \beta s(x) \colon \alpha, \beta \in \mathbb{F}_{q^m}\},$$

for some q-polynomials $r(x), s(x)$ over $\mathbb{F}_{q^m}$. Since each MRD-code with parameters $(m, m, q; m-1)$ contains invertible elements (cf. [29, Lemma 2.1]), we may take $h(x) \in \mathcal{C}'$ invertible. Then $h^{-1} \circ \mathcal{C}'$ has the desired form, i.e. $h^{-1} \circ \mathcal{C}' = \mathcal{C}_f$ for some q-polynomial $f(x)$ over $\mathbb{F}_{q^m}$. □

Proposition 6.2. *The known $\mathbb{F}_q$-linear MRD-codes with parameters $(m, m, q; m-1)$ and with middle nucleus isomorphic to $\mathbb{F}_{q^m}$, up to equivalence, arise from one of the following maximum scattered subspaces of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$:*

1. $U_1 = \{(x, x^{q^s}) \colon x \in \mathbb{F}_{q^m}\}$, $1 \leq s \leq m-1$ $\gcd(s, m) = 1$.
2. $U_2 = \{(x, \delta x^{q^s} + x^{q^{m-s}}) \colon x \in \mathbb{F}_{q^m}\}$, $\mathrm{N}_{q^m/q}(\delta) \neq 1$, $\gcd(s, m) = 1$.

Proof. The known $\mathbb{F}_q$-linear MRD-codes with parameters $(m, m, q; m-1)$, written as $\mathbb{F}_q$-linear maps over $\mathbb{F}_{q^m}$, are of the form

$$\mathcal{H}_{2,s}(\mu, h) := \{x \mapsto a_0 x + a_1 x^{q^s} + \mu a_0^{q^h} x^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^m}\},$$

with $\gcd(s, m) = 1$ and $\mathrm{N}_{q^{sm}/q^s}(\mu) \neq 1$.

By [29, Corollary 5.9] the middle nuclei of the codes $\mathcal{H}_{2,s}(\mu, h)$ are isomorphic to $\mathbb{F}_{q^m}$ if and only if $\mu = 0$ or $m \mid 2s - h$. In the former case we obtain generalized Gabidulin codes arising from maximum scattered linear sets of pseudoregulus type, i.e. from maximum scattered subspaces of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$ of type U_1. If $m \mid 2s-h$, by [28, Proposition 4.3] the adjoint code of $\mathcal{H}_{2,s}(\mu, h)$ is equivalent to $\mathcal{H}_{2,s}(1/\mu, 2s-h) = \mathcal{H}_{2,s}(1/\mu, 0)$ and direct computations show that such a code is equivalent to a code arising from a maximum scattered subspace of type U_2. The assertion follows from the fact that the families of MRD-codes arising from maximum scattered subspaces of type U_1 and U_2, respectively, are both closed under the adjoint operation (following the terminology of [35, 16, 25], the adjoint code of $\mathcal{C}_f$ is $\mathcal{C}_{\hat{f}}$). □

Put $m = 2n$, $n > 1$ in the previous proposition. Note that if $n = 2$ then a scattered $\mathbb{F}_q$–vector subspace $U_{b,s}$ (which means $\mathrm{N}_{q^4/q}(b) \neq 1$, cf. [10]) is of type either U_2 or $U_2^{\perp'}$. Now, we are able to prove that MRD-codes arising from scattered subspaces of form (9) with $n > 2$ are new.

By using the same arguments as in Corollary 5.2, the linear automorphism group $\mathcal{G}_i$ of U_i, $i \in \{1, 2\}$, is

$$\mathcal{G}_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{q^s} \end{pmatrix} : a \in \mathbb{F}_{q^{2n}}^* \right\}, \qquad \mathcal{G}_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{q^s} \end{pmatrix} : a \in \mathbb{F}_{q^2}^* \right\}.$$

This allows us to prove the following:

Theorem 6.3. *If $n > 2$, the $\mathbb{F}_q$–vector subspace of $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$*

$$U_{b,s} = \{(x, bx^{q^s} + x^{q^{s+n}}) \colon x \in \mathbb{F}_{q^{2n}}\},$$

with $b \in \mathbb{F}_{q^{2n}}^*$ and $1 \leq s \leq n-1$ such that $\mathrm{N}_{q^{2n}/q^n}(b) \neq 1$ and $\gcd(s, n) = 1$, is not equivalent to any subspace U_i, $i \in \{1, 2\}$, under the action of the group $\Gamma\mathrm{L}(2, q^{2n})$.

Proof. If there exists an element $\varphi \in \Gamma\mathrm{L}(2, q^{2n})$ such that $U_{b,s}^{\varphi} = U_i$, for some $i \in \{1, 2\}$, then the corresponding linear automorphism groups will be isomorphic via the map

$$\omega \in \mathcal{G}_{b,s} \mapsto \varphi \circ \omega \circ \varphi^{-1} \in \mathcal{G}_i,$$

but this is a contradiction by comparing the sizes of the related groups (cf. Corollary 5.2). □

Let $\mathcal{C}_f$ and $\mathcal{C}_g$ be two MRD-codes arising from maximum scattered subspaces U_f and U_g of $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$. In [35, Theorem 8] the author showed that there exist invertible matrices A, B such that $A\mathcal{C}_f B = \mathcal{C}_g$ if and only if U_f and U_g are $\Gamma\mathrm{L}(2, q^m)$-equivalent. Hence, by Theorem 6.3, we get the following result.

Theorem 6.4. *If $n > 2$, the linear MRD-code of dimension $4n$ and minimum distance $2n-1$ arising from a scattered $\mathbb{F}_q$–vector subspace $U_{b,s} = \{(x, bx^{q^s} + x^{q^{s+n}}) \colon x \in \mathbb{F}_{q^{2n}}\}$ of $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ is not equivalent to any previously known MRD-code with the same parameters.* $\square$

In the next section we will show that when $n = 3$ and $q > 2$ and when $n = 4$ and q is odd there exist values of b and s for which the $\mathbb{F}_q$-subspace $U_{b,s}$ of $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ is scattered, and from the above arguments the corresponding MRD-codes are new.

7 New maximum scattered subspaces

7.1 The $n = 3$ case

We want to show that there exists $b \in \mathbb{F}^*_{q^6}$ such that

$$U_{b,1} := \{(x, bx^q + x^{q^4}) \colon x \in \mathbb{F}_{q^6}\}$$

is a maximum scattered $\mathbb{F}_q$-subspace.

$U_{b,1}$ is scattered if and only if for each $m \in \mathbb{F}_{q^6}$

$$\frac{bx^q + x^{q^4}}{x} = -m$$

has at most q solutions. Those m which admit exactly q solutions correspond to points $\langle(1, -m)\rangle_{\mathbb{F}_{q^6}}$ of $L_{U_{b,1}}$ with weight one. It follows that $U_{b,1}$ is scattered if and only if for each $m \in \mathbb{F}_{q^6}$ the kernel of

$$r_{m,b}(x) := mx + bx^q + x^{q^4}$$

has dimension less than two, or, equivalently, the Dickson matrix

$$D_{m,b} := \begin{pmatrix} m & b & 0 & 0 & 1 & 0 \\ 0 & m^q & b^q & 0 & 0 & 1 \\ 1 & 0 & m^{q^2} & b^{q^2} & 0 & 0 \\ 0 & 1 & 0 & m^{q^3} & b^{q^3} & 0 \\ 0 & 0 & 1 & 0 & m^{q^4} & b^{q^4} \\ b^{q^5} & 0 & 0 & 1 & 0 & m^{q^5} \end{pmatrix}$$

associated to $r_{m,b}(x)$ has rank at least five (cf. [36, Proposition 4.4]). Equivalently, $D_{m,b}$ has a non-zero 5×5 minor. We will denote by $M_{i,j}$ the determinant of the matrix obtained from $D_{m,b}$ by removing the i-th row and the j-th column. We will use the following:

$$M_{6,1} = b^{q^2} - b^{1+q^2+q^3} - b^{q+q^2+q^4} + b^{1+q+q^2+q^3+q^4} - b^{q^4} m^{q+q^2+q^3} - b m^{q^2+q^3+q^4}, \tag{14}$$

$$M_{6,5} = -b^{q^2} m + b^{q+q^2+q^4} m - b m^{q^3} + b^{1+q+q^4} m^{q^3} + b^{q^4} m^{1+q+q^2+q^3}. \tag{15}$$

We will show that for certain choices of b and q there is no $m \in \mathbb{F}_{q^6}$ such that both of the above expressions are zero.

Theorem 7.1. *For $q > 4$ we can always find $b \in \mathbb{F}_{q^2}^*$, such that $U_{b,1}$ is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$.*

Proof. We want to find $b \in \mathbb{F}_{q^2}^*$ such that at least one of (14) and (15) is non-zero. Suppose the contrary, i.e. for each $b \in \mathbb{F}_{q^2}$:

$$0 = b(1 - 2b^{q+1} + b^{2q+2} - m^{q+q^2+q^3} - m^{q^2+q^3+q^4}), \tag{16}$$

$$0 = b(-m + b^{q+1} m - m^{q^3} + b^{q+1} m^{q^3} + m^{1+q+q^2+q^3}). \tag{17}$$

Put $x = m^{1+q+q^2}$ and $z = 1 - b^{q+1}$. Obviously $z \neq 1$ and dividing (16) by b gives

$$z^2 = x^q + x^{q^2}, \tag{18}$$

multiplying (17) by $m^{q^4+q^5}/b$ gives

$$z(x^{q^3} + x^{q^4}) = x^{q^3+1}. \tag{19}$$

Since $b \in \mathbb{F}_{q^2}$, it follows that $b^{q+1} \in \mathbb{F}_q$ and hence $z \in \mathbb{F}_q$. Then (18) yields $x^q + x^{q^2} \in \mathbb{F}_q$ and hence $x \in \mathbb{F}_{q^2}$. Then (18) and (19) give:

$$z^2 = x + x^q, \tag{20}$$

$$z^3 = x^{q+1}. \tag{21}$$

Thus x and x^q are roots of the equation

$$X^2 - z^2 X + z^3 = 0. \tag{22}$$

From now on we distinguish two cases according to the parity of q. First suppose q odd. If (22) can be solved in $\mathbb{F}_q$, then $x = x^q \in \mathbb{F}_q$ and hence (20) and (21) give $z = x = 0$, or $z = 4$, $x = 8$. If we can find $z \in \mathbb{F}_q \setminus \{0, 1, 4\}$

such that (22) has roots in $\mathbb{F}_q$, then we obtain a contradiction meaning that the two minors in consideration cannot vanish at the same time. Then $U_{b,1}$ is scattered for each $b \in \mathbb{F}_{q^2}$ which satisfies $1 - b^{q+1} = z$. Equation (22) has roots in $\mathbb{F}_q$ if and only if $z^4 - 4z^3$ is a square, hence, when $z^2 - 4z$ is a square. Note that $z = 2$ gives $z^2 - 4z = -4$, which is always a square when $q \equiv 1 \pmod 4$. So from now on, we may assume $q \equiv 3 \pmod 4$ and hence $q \geq 7$. Consider the conic $\mathcal{C}$ of $\mathrm{PG}(2, q)$ with equation $X_0^2 - 4X_0X_2 - X_1^2 = 0$. It is easy to see that $\mathcal{C}$ is always non-singular, and that the line with equation $X_0 = 0$ is a tangent to $\mathcal{C}$. For $q \geq 7$ $\mathcal{C}$ has more than 7 points and hence we can find a point of $\mathcal{C}$ not on the lines $X_0 = 0$, $X_0 - 4X_2 = 0$, $X_0 - X_2 = 0$ and $X_2 = 0$. It means that we can always find a point $\langle (x_0, x_1, 1) \rangle_{\mathbb{F}_q} \in \mathrm{PG}(2, q)$ such that $x_0^2 - 4x_0 = x_1^2$ and $x_0 \in \mathbb{F}_q \setminus \{0, 1, 4\}$. It follows that we can always find z, and hence b, with the given conditions.

Now consider the case when q is even. For $z \neq 0$ (22) has a solution in $\mathbb{F}_q$ if and only if the S-invariant of the equation, that is $\mathrm{Tr}_{q/2}(1/z)$, equals to zero. If there is a solution in $\mathbb{F}_q$, then (20) and (21) give $z = 0$, so it is enough to prove that there exists $z \in \mathbb{F}_q \setminus \{0, 1\}$, such that $\mathrm{Tr}_{q/2}(1/z) = 0$. The existence of such z gives a contradiction meaning that the two minors in consideration cannot vanish at the same time. The equation $\mathrm{Tr}_{q/2}(x) = 0$ has $q/2$ pairwise distinct roots in $\mathbb{F}_q$, thus $\mathrm{Tr}_{q/2}(1/z) = 0$ has $q/2 - 1$ non-zero solutions. It follows that for $q \geq 8$ we can find such z. □

7.2 The $n = 4$ case

We will show that there exists $b \in \mathbb{F}_{q^8}^*$ such that

$$U_{b,1} := \{(x, bx^q + x^{q^5}) \colon x \in \mathbb{F}_{q^8}\}$$

is a maximum scattered $\mathbb{F}_q$-subspace for each odd q.

$U_{b,1}$ is scattered if and only if for each $m \in \mathbb{F}_{q^8}$

$$\frac{bx^q + x^{q^5}}{x} = -m$$

has at most q solutions. Those m which admit exactly q solutions correspond to points $\langle (1, -m) \rangle_{\mathbb{F}_{q^8}}$ of $L_{U_{b,1}}$ with weight one. It follows that $U_{b,1}$ is scattered if and only if for each $m \in \mathbb{F}_{q^8}$ the kernel of

$$r_{m,b}(x) := mx + bx^q + x^{q^5}$$

has dimension less than two, or, equivalently, the Dickson matrix

$$D_{m,b} := \begin{pmatrix} m & b & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & m^q & b^q & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & m^{q^2} & b^{q^2} & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & m^{q^3} & b^{q^3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & m^{q^4} & b^{q^4} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & m^{q^5} & b^{q^5} & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & m^{q^6} & b^{q^6} \\ b^{q^7} & 0 & 0 & 0 & 1 & 0 & 0 & m^{q^7} \end{pmatrix}$$

of $r_{m,b}(x)$ has a non-zero 7×7 minor. If we remove the first two columns and last two rows of the above matrix, then the remaining 6×6 submatrix M has determinant $(b^{q+q^5} - 1)m^{q^3+q^4}$. It follows that with $\mathrm{N}_{q^8/q^4}(b) \neq 1$ the only point of $L_{U_{b,s}}$ with weight larger than 2 is $\langle(1,0)\rangle_{\mathbb{F}_{q^8}}$. On the other hand, it is easy to see that $\langle(1,0)\rangle_{\mathbb{F}_{q^8}}$ is a point of $L_{U_{b,s}}$ if and only if $\mathrm{N}_{q^8/q^4}(b) = 1$.

We will denote by $M_{i,j}$ the determinant of the matrix obtained from $D_{m,b}$ by cancelling the i-row and the j-th column. We will use the following:

$$M_{8,2} = (b^{1+q^4} - 1)^{q+q^2}(b^{q^3+q^4}m + m^{q^4}) + m^{1+q^3+q^4+q^5}(b^{q^6}m^{q^2} + b^q m^{q^6}). \tag{23}$$

Theorem 7.2. *For odd q and $b^2 = -1$ the $\mathbb{F}_q$-subspace $U_{b,1}$ is maximum scattered in $\mathbb{F}_{q^8} \times \mathbb{F}_{q^8}$.*

Proof. We will show that there is no $m \in \mathbb{F}_{q^8}^*$ such that (23) vanishes. Applying $b^2 = -1$, the vanishing of (23) would give

$$0 = 4(b^{q+1}m + m^{q^4}) + m^{1+q^3+q^4+q^5}(bm^{q^2} + b^q m^{q^6}). \tag{24}$$

Now we distinguish two cases, according to $b \in \mathbb{F}_q$ (i.e., $q \equiv 1 \pmod 4$), or $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ (i.e., $q \equiv 3 \pmod 4$). First suppose that the former case holds. Then

$$0 = 4(-m + m^{q^4}) + bm^{1+q^3+q^4+q^5}(m^{q^2} + m^{q^6}). \tag{25}$$

Considering the $\mathbb{F}_{q^8} \to \mathbb{F}_{q^4}$ trace of both sides of (25) and using the $\mathbb{F}_{q^4}$-linearity of this function, it follows that $\mathrm{Tr}_{q^8/q^4}(m^{q^3+q^5}) = 0$. It is easy to see that $\mathrm{Tr}_{q^8/q^4}(x) = \mathrm{Tr}_{q^8/q^4}(y) = 0$ implies $xy \in \mathbb{F}_{q^4}$ for any two $x, y \in \mathbb{F}_{q^8}$, thus $m^{q^3+q^5}m^{q^2+q^4}$ and $m^{q^3+q^5}m^{q^4+q^6}$ are in $\mathbb{F}_{q^4}$. It follows that $bm^{1+q^3+q^4+q^5}(m^{q^2} + m^{q^6}) = m\lambda$ for some $\lambda \in \mathbb{F}_{q^4}$ and hence (25) gives $m^{q^4-1} \in \mathbb{F}_{q^4}$. But also $m^{q^4+1} \in \mathbb{F}_{q^4}$ and hence $m^2 \in \mathbb{F}_{q^4}$ giving either $m \in \mathbb{F}_{q^4}$, or $\mathrm{Tr}_{q^8/q^4}(m) = 0$, but (25) gives $m = 0$ in both cases.

Now consider the $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ case. Then $b^{q+1} = 1$ and $b^q = -b$, thus (24) gives

$$0 = 4(m + m^{q^4}) + bm^{1+q^3+q^4+q^5}(m^{q^2} - m^{q^6}). \tag{26}$$

Since $4(m + m^{q^4}) \in \mathbb{F}_{q^4}$ and $bm^{1+q^4} \in \mathbb{F}_{q^4}$, it follows that $m^{q^3+q^5}(m^{q^2} - m^{q^6}) \in \mathbb{F}_{q^4}$. It is easy to see that $\mathrm{Tr}_{q^8/q^4}(x) = 0$ and $xy \in \mathbb{F}_{q^4}$ implies $\mathrm{Tr}_{q^8/q^4}(y) = 0$ for any two $x, y \in \mathbb{F}_{q^8}$, thus $\mathrm{Tr}_{q^8/q^4}(m^{q^3+q^5}) = 0$. Then, as in the previous case, $m^2 \in \mathbb{F}_{q^4}$ follows, which gives a contradiction. □

Remark 7.3. *It follows from Theorem 6.3 that the maximum scattered subspaces of this section are new, i.e. they cannot be obtained from previously known maximum scattered subspaces under the action of* $\Gamma\mathrm{L}(2, q^n)$*,* $n = 6, 8$*.*

As we mentioned in the Introduction, it can happen that two $\mathbb{F}_q$*–vector subspaces of* $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ *lie on different orbits of* $\Gamma\mathrm{L}(2, q^n)$ *but they define* $\mathbb{F}_q$*-linear sets which are equivalent under the group* $\mathrm{P}\Gamma\mathrm{L}(2, q^n)$*. In [7, Theorem 4.3] the authors prove that the maximum scattered linear sets defined by the maximum scattered subspaces constructed in Theorems 7.1 and 7.2 are not equivalent to the previously known maximum scattered linear sets under the group* $\mathrm{P}\Gamma\mathrm{L}(2, q^n)$*.*

Remark 7.4. *Computations with* `GAP` *yield the following results.*

With respect to the cases not covered by Theorem 7.1: there exist $b \in \mathbb{F}_{q^6}^*$ *such that the subspace* $\{(x, bx^q + x^{q^4}) \colon x \in \mathbb{F}_{q^6}\}$ *is scattered in* $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$ *also for* $q \in \{3, 4\}$*, but not for* $q = 2$*.*

With respect to Theorem 7.2: for $q \leq 8$*,* q *even, there is no* $b \in \mathbb{F}_{q^8}^*$ *such that* $\{(x, bx^q + x^{q^5}) \colon x \in \mathbb{F}_{q^8}\}$ *is scattered in* $\mathbb{F}_{q^8} \times \mathbb{F}_{q^8}$ *and for* $q \leq 11$*,* q *odd, the corresponding subspace is scattered if and only if* $b^{q^4+1} = -1$*. According to the first paragraph of Section 5, each of these subspaces is equivalent to the scattered subspace found in Theorem 7.2.*

There is no $b \in \mathbb{F}_{q^{2n}}^*$ *such that* $\{(x, bx^{q^s} + x^{q^{n+s}}) \colon x \in \mathbb{F}_{q^{2n}}\}$*,* $\gcd(s, n) = 1$*, is scattered in* $\mathbb{F}_{q^{2n}} \times \mathbb{F}_{q^{2n}}$ *when* $q \leq 5$ *and* $n \in \{5, 6, 7, 8\}$*, or* $q = 7$ *and* $n \in \{5, 6, 7\}$*, or* $q = 7$ *and* $n = 8$*, or* $q = 8$ *and* $n = 5$*.*

Conjecture 7.5. *According to the first paragraph of Section 5,* $f_1(x) = b_1x^q + x^{q^4} \in \mathbb{F}_{q^6}[x]$ *and* $f_2(x) = b_2x^q + x^{q^4} \in \mathbb{F}_{q^6}[x]$ *define equivalent subspaces when* $\mathrm{N}_{q^6/q^3}(b_1) = \mathrm{N}_{q^6/q^3}(b_2)$*. We conjecture that the size of the set*

$$\{\mathrm{N}_{q^6/q^3}(b) \colon f(x) = bx^q + x^{q^4} \textit{ defines a maximum scattered } \mathbb{F}_q\textit{-space } U_{b,1}\}$$

is $\lfloor (q^2+q+1)(q-2)/2 \rfloor$*, and hence there might be further examples of maximum scattered subspaces in this family. By* `GAP` *we verified this conjecture for* $q \leq 32$*.*

Remark 7.6. *The maximum number of directions determined by an* $\mathbb{F}_q$*-linear function over* $\mathbb{F}_{q^n}$ *is* $(q^n-1)/(q-1)$*. Also, the maximum size of an* $\mathbb{F}_q$*-linear blocking set of Rédei type of* $\mathrm{PG}(2,q^n)$ *is* $q^n+(q^n-1)/(q-1)$*. According to [5, Section 5.3] our new examples of maximum scattered spaces yield new examples of functions and of blocking sets which attain these bounds.*

In [14, pg. 132] the maximal cardinality of the image set $\mathrm{Im}(L(x)/x)$ *is considered (with* $x \mapsto 1/x$ *defined to take 0 to 0), where* $L(x)$ *is an* $\mathbb{F}_p$*-linear function over* $\mathbb{F}_q$*,* p *is a prime and* q *is a power of* p*. If for some invertible* p*-polynomial* f*, the subspace* $U_f=\{(x,f(x))\colon x\in\mathbb{F}_q\}$ *is scattered, then the cardinality of* $\mathrm{Im}(L(x)/x)$ *reaches its maximum, which is* $1+(q-1)/(p-1)$*. It follows that the maximum scattered subspaces constructed in this paper yield such functions.*

Acknowledgement

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).

References

[1] A. Blokhuis and M. Lavrauw: Scattered Spaces with Respect to a Spread in $\mathrm{PG}(n,q)$, *Geom. Dedicata* 81, No.1-3 (2000), 230–243.

[2] 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.

[3] D. Bartoli, M. Giulietti, G. Marino and O. Polverino: Maximum scattered linear sets and complete caps in Galois spaces, *Combinatorica* (2017), 1–24, DOI: 10.1007/s00493-016-3531-6.

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

[5] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$. To appear in J. Combin. Theory Ser. A. https://arxiv.org/abs/1607.06962

[6] B. Csajbók, G. Marino, O. Polverino and F. Zullo: Maximum scattered linear sets and MRD-codes, *J. Algebraic. Combin.* **46** (2017), 517–531.

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

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

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

[10] B. Csajbók and C. Zanella: Maximum scattered $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1, q^4)$. *Discrete Math.*, **341** (2018), 74–80

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

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

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

[14] F. Göloğlu and G. McGuire: On theorems of Carlitz and Payne on permutation polynomials over finite fields with an application to $x^{-1} + L(x)$, *Finite Fields Appl.* **27** (2014), 130–142.

[15] B. Huppert Endliche Gruppen, volume 1. Springer Berlin-Heidelberg-New York, 1967.

[16] W. M. Kantor: Commutative semifields and symplectic spreads, *J. Algebra*, **270** (1) (2003), 96-114.

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

[18] M. Lavrauw: *Scattered Spaces with respect to Spreads and Eggs in Finite Projective Spaces*, Ph. D. thesis, Technical University of Eindhoven, The Netherlands, 2001.

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

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

[21] 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.

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

[23] 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).

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

[25] G. Lunardon, G. Marino, O. Polverino and R. Trombetti: Symplectic semifield spreads of $PG(5, q)$ and the Veronese surface, *Ricerche mat.* **60** (2011), 125-142.

[26] 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.

[27] G. Lunardon and O. Polverino: Blocking sets and derivable partial spreads, *J. Algebraic Combin.*, **14** (2001), 49–56.

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

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

[30] D. Liebhold and G. Nebe: Automorphism groups of Gabidulin-like codes, *Archiv der Mathematik* **107** (4) (2016), 355–366.

[31] G. Marino and O. Polverino: On translation spreads of $H(q)$, *J. Algebraic Combin.* **42** (2015), 725–744.

[32] 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.

[33] 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.

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

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

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

Bence Csajbók
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
ELTE Eötvös Loránd University, Budapest, Hungary
Department of Geometry
1117 Budapest, Pázmány P. stny. 1/C, Hungary
csajbok.bence@gmail.com

Giuseppe Marino, Olga Polverino
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli",
Viale Lincoln 5, I- 81100 Caserta, Italy
giuseppe.marino@unicampania.it, *olga.polverino@unicampania.it*

Corrado Zanella
Dipartimento di Tecnica e Gestione dei Sistemi Industriali,
Università di Padova,
Stradella S. Nicola, 3, I-36100 Vicenza, Italy
corrado.zanella@unipd.it