Non-linear maximum rank distance codes in the cyclic model for the field reduction of finite geometries

Nicola Durante

Dipartimento di Matematica e Applicazioni “Renato Caccioppoli”
Università degli Studi di Napoli Federico II
Napoli, Italy

ndurante@unina.it

Alessandro Siciliano

Dipartimento di Matematica, Informatica ed Economia
Università degli Studi della Basilicata
Potenza, Italy

alessandro.siciliano@unibas.it

Submitted: Apr 29, 2016; Accepted: May 16, 2017; Published: Jun 16, 2017
Mathematics Subject Classifications: 94B05, 15A63

Abstract

In this paper we construct infinite families of non-linear maximum rank distance codes by using the setting of bilinear forms of a finite vector space. We also give a geometric description of such codes by using the cyclic model for the field reduction of finite geometries and we show that these families contain the non-linear maximum rank distance codes recently provided by Cossidente, Marino and Pavese.

1 Introduction

Let $M_{m,m'}(\mathbb{F}_q)$, $m \leqslant m'$, be the rank metric space of all the $m \times m'$ matrices with entries in the finite field $\mathbb{F}_q$ with q elements, $q = p^h$, p a prime. The *distance* between two matrices by definition is the rank of their difference. An $(m, m', q; s)$*-rank distance code* (also *rank metric code*) is any subset $\mathcal{X}$ of $M_{m,m'}(\mathbb{F}_q)$ such that the minimum distance between two of its distinct elements is $s + 1$. An $(m, m', q; s)$-rank distance code is said to be *linear* if it is a linear subspace of $M_{m,m'}(\mathbb{F}_q)$.

It is known [11] that the size of an $(m, m', q; s)$-rank distance code $\mathcal{X}$ is bounded by the *Singleton-like bound*:

$$|\mathcal{X}| \leqslant q^{m'(m-s)}.$$

When this bound is achieved, $\mathcal{X}$ is called an $(m, m', q; s)$-*maximum rank distance code*, or $(m, m', q; s)$-*MRD code*, for short.

Although MRD codes are very interesting by their own and they caught the attention of many researchers in recent years [1, 9, 32], such codes have also applications in error-correction for random network coding [18, 22, 37], space-time coding [38] and cryptography [17, 36].

Obviously, investigations of MRD codes can be carried out in any rank metric space isomorphic to $M_{m,m'}(\mathbb{F}_q)$. In his pioneering paper [11], Ph. Delsarte constructed linear MRD codes for all the possible values of the parameters m, m', q and s by using the framework of bilinear forms on two finite-dimensional vector spaces over a finite field (Delsarte used the terminology *Singleton systems* instead of maximum rank distance codes).

Few years later, Gabidulin [16] independently constructed Delsarte's linear MRD codes as evaluation codes of linearized polynomials over a finite field [26]. That construction was generalized in [21] and these codes are now known as *Generalized Gabidulin codes*.

In the case $m' = m$, a different construction of Delsarte's MRD codes was given by Cooperstein [7] in the framework of the tensor product of a vector space over $\mathbb{F}_q$ by itself. Very recently, Sheekey [35] and Lunardon, Trombetti and Zhou [28] provide some new linear MRD codes by using linearized polynomials over $\mathbb{F}_{q^m}$.

In finite geometry, $(m, m, q; m-1)$-MRD codes are known as *spread sets* [12]. To the extent of our knowledge the only non-linear MRD codes that are not spread sets are the $(3, 3, q; 1)$-MRD codes constructed by Cossidente, Marino and Pavese in [8]. They got such codes by looking at the geometry of certain algebraic curves of the projective plane $\mathrm{PG}(2, q^3)$. Such curves, called C_F^1-*sets*, were introduced and studied by Donati and Durante in [13]. In this paper, we construct infinite families of non-linear $(m, m, q; m-2)$-MRD codes, for $q \geqslant 3$ and $m \geqslant 3$. We also show that the Cossidente, Marino and Pavese non-linear MRD codes belong to these families. Our investigation will carry out in the framework of bilinear forms on a finite dimensional vector space over $\mathbb{F}_q$.

Let $\Omega = \Omega(V, V)$ be the set of all bilinear forms on V, where $V = V(m, q)$ denotes an m-dimensional vector space over $\mathbb{F}_q$. Clearly, Ω is an m^2-dimensional vector space over $\mathbb{F}_q$.

The *left radical* $\mathrm{Rad}(f)$ of any $f \in \Omega$ by definition is the subspace of V consisting of all vectors v satisfying $f(v, v') = 0$ for every $v' \in V$. The *rank* of f is the codimension of $\mathrm{Rad}(f)$, i.e.

$$\mathrm{rk}(f) = m - \dim_{\mathbb{F}_q}(\mathrm{Rad}(f)).$$

Let $u_1, \ldots, u_m$ be a basis of V. For a given $f \in \Omega$, the matrix $(f(u_i, u_j))_{i,j=1,\ldots,m}$, is called the *matrix* of f in the basis $u_1, \ldots, u_m$ and the map

$$\begin{array}{rccc} \nu = \nu_{\{u_1,\ldots,u_m\}}: & \Omega & \to & M_{m,m}(\mathbb{F}_q) \\ & f & \mapsto & (f(u_i, u_j))_{i,j=1,\ldots,m} \end{array}$$

is an isomorphism of rank metric spaces giving $\mathrm{rk}(f) = \mathrm{rk}(\nu(f))$.

The group $H = \mathrm{GL}(V) \times \mathrm{GL}(V)$ acts on Ω as a subgroup of $\mathrm{Aut}_{\mathbb{F}_q}(\Omega)$: for every $(g, g') \in H$, the (g, g')−image of any $f \in \Omega$ is defined to be the bilinear form $f^{(g,g')}$ given by

$$f^{(g,g')}(v,v') = f(gv, g'v').$$

Any $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ naturally defines a semilinear transformation of V. For any $f \in \Omega$ and $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, we define the bilinear form $f^\theta(v,v') = f(v^{\theta^{-1}}, v'^{\theta^{-1}})^\theta$.

The involutorial operator $\top : f \in \Omega \to f^\top \in \Omega$, where $f^\top$ is given by

$$f^\top(v,v') = f(v',v),$$

is an automorphism of Ω. It turns out that the above automorphisms are all the elements in $\mathrm{Aut}_{\mathbb{F}_q}(\Omega)$, i.e. $\mathrm{Aut}_{\mathbb{F}_q}(\Omega) = (\mathrm{GL}(V) \times \mathrm{GL}(V)) \rtimes \langle \top \rangle \rtimes \mathrm{Aut}(\mathbb{F}_q)$.

Two MRD codes $\mathcal{X}_1$ and $\mathcal{X}_2$ are said to be *equivalent* if there exists $\varphi \in \mathrm{Aut}_{\mathbb{F}_q}(\Omega)$ such that $\mathcal{X}_2 = \mathcal{X}_1^\varphi$.

This paper is organized as follows. In Section 2 we introduce a cyclic model of Ω. In this model we construct infinite families of non-linear MRD codes. More precisely, for $q \geqslant 3$, $m \geqslant 3$ and I any subset of $\mathbb{F}_q \setminus \{0,1\}$, we provide a subset $\mathcal{F}_{m,q;I}$ of Ω which turns out to be a non-linear $(m,m,q;m-2)$-MRD code (Theorem 19).

In Section 3 we give a geometric description of such codes. If a given rank distance code $\mathcal{X}$ is considered as a subset of $V(m^2,q)$, then one can consider the corresponding set of projective points in $\mathrm{PG}(m^2-1,q)$ under the canonical homomorphism $\psi : \mathrm{GL}(V(m^2,q)) \to \mathrm{PGL}(m^2,q)$. We prove (Theorem 24) that the projective set defined by $\mathcal{F}_{m,q;I}$, with $|I| = k$, is a subset of a Desarguesian m-spread of $\mathrm{PG}(m^2-1,q)$ [34] consisting of two spread elements, k pairwise disjoint Segre varieties $\mathcal{S}_{m,m}(\mathbb{F}_q)$ [20] and $q-1-k$ hyperreguli [30]. Additionally, if one consider the projective space $\mathrm{PG}(m^2-1,q)$ as the field reduction of $\mathrm{PG}(m-1,q^m)$ over $\mathbb{F}_q$, then the projective set defined by $\mathcal{F}_{m,q;I}$ is, in fact, the field reduction of the union of two projective points, k mutually disjoint $(m-1)$-dimensional $\mathbb{F}_q$-subgeometries and $q-1-k$ scattered $\mathbb{F}_q$-linear sets of pseudoregulus type of $\mathrm{PG}(m-1,q^m)$ [13, 24, 29]. The main tool we use to get the above geometric description is the field reduction of $V(m,q^m)$ over $\mathbb{F}_q$ in the cyclic model for the tensor product $\mathbb{F}_{q^m} \otimes V$ as described in [7].

2 The non-linear MRD codes in the cyclic model of bilinear forms

In the paper [7], the cyclic model of the m-dimensional vector space $V = V(m,q)$ over $\mathbb{F}_q$ was introduced by taking eigenvectors, say $v_1, \dots, v_m$, of a given Singer cycle σ of V, where a *Singer cycle* of V is an element of $\mathrm{GL}(V)$ of order $q^m - 1$. Since the vectors $v_1, \dots, v_m$ have distinct eigenvalues over $\mathbb{F}_{q^m}$, they form a basis of the extension $\widehat{V} = V(m,q^m)$ of V. In this basis the vector space V is represented by

$$V = \left\{ \sum_{j=1}^{m} a^{q^{j-1}} v_j : a \in \mathbb{F}_{q^m} \right\}. \tag{1}$$

We call $v_1, \dots, v_m$ a *Singer basis* of V and the above representation is called the *cyclic model for V* [19, 15].

The set of all $1-$dimensional $\mathbb{F}_q-$subspaces of $\widehat{V}$ spanned by vectors in the cyclic model for V is called the *cyclic model for the projective space* $\mathrm{PG}(V)$. Note that the above cyclic model corresponds to the cyclic model of $\mathrm{PG}(V)$ where the points are identified with the elements of the group $\mathbb{Z}_{q^{m-1}+q^{m-2}+\cdots+q+1}$ [19, pp. 95–98] [15]. Very recently, the cyclic model for $V(3,q)$ has been used to give an alternative model for the triality quadric $Q^+(7,q)$ [2].

Let $\widehat{V}^*$ be the dual vector space of $\widehat{V}$ with basis $v_1^*,\ldots,v_m^*$, the dual basis of the Singer basis $v_1,\ldots,v_m$. Then the dual vector space of V is

$$V^* = \left\{ \sum_{i=1}^{m} \alpha^{q^{i-1}} v_i^* : \alpha \in \mathbb{F}_{q^m} \right\}.$$

A linear transformation from V to itself is called an *endomorphism* of V. We will denote the set of all endomorphisms of V by $\mathrm{End}(V)$.

An $m \times m$ *Dickson matrix* (or *q-circulant matrix*) over $\mathbb{F}_{q^m}$ is a matrix of the form

$$D_{(a_0,a_1,\ldots,a_{m-1})} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{m-1} \\ a_{m-1}^q & a_0^q & \cdots & a_{m-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{m-1}} & a_2^{q^{m-1}} & \cdots & a_0^{q^{m-1}} \end{pmatrix}$$

with $a_i \in \mathbb{F}_{q^m}$. We say that the above matrix is *generated by the array* $(a_0,a_1,\ldots,a_{m-1})$.

Let $\mathcal{D}_m(\mathbb{F}_{q^m})$ denote the *Dickson matrix algebra* formed by all $m\times m$ Dickson matrices over $\mathbb{F}_{q^m}$. The set $\mathcal{B}_m(\mathbb{F}_{q^m})$ of all invertible Dickson $m\times m$ matrices is known as the *Betti-Mathieu group* [6].

Proposition 1. *[39, Lemma 4.1]* $\mathrm{End}(V) \simeq \mathcal{D}_m(\mathbb{F}_{q^m})$ *and* $\mathrm{GL}(V) \simeq \mathcal{B}_m(\mathbb{F}_{q^m})$.

A polynomial of the form

$$L(x) = \sum_{i=0}^{m-1} \alpha_i x^{q^i}, \qquad \alpha_i \in \mathbb{F}_{q^m},$$

is called a *linearized polynomial* (or *q-polynomial*) over $\mathbb{F}_{q^m}$. It is known that every endomorphism of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ can be represented by a unique $q-$polynomial [33].

Let $\mathcal{L}_m(\mathbb{F}_{q^m})$ be the set of all q-polynomials over $\mathbb{F}_{q^m}$. In the paper [39], it was showed that the map

$$\begin{array}{cccc} \varphi: & \mathcal{L}_m(\mathbb{F}_{q^m}) & \longrightarrow & \mathcal{D}_m(\mathbb{F}_{q^m}) \\ & \sum_{i=0}^{m-1} \alpha_i x^{q^i} & \longmapsto & D_{(\alpha_0,\ldots,\alpha_{m-1})} \end{array}$$

is an isomorphism between the non-commutative $\mathbb{F}_q-$algebras $\mathcal{L}_m(\mathbb{F}_{q^m})$ and $\mathcal{D}_m(\mathbb{F}_{q^m})$. From Proposition 1 we see that any Singer basis of V realizes this isomorphism.

Proposition 2. *Let $v_1,\ldots,v_n$ be a Singer basis of V. Then the matrix of any $f \in \Omega$ with respect to $v_1,\ldots,v_n$ is an $m\times m$ Dickson matrix. Conversely, every $m\times m$ Dickson matrix defines a bilinear form on $V \times V$.*

Proof. Let $D_{\mathbf{a}}$ be an $m \times m$ Dickson matrix generated by the m-ple $\mathbf{a} = (a_0, a_1, \ldots, a_{m-1})$ over $\mathbb{F}_{q^m}$. Let $f_{\mathbf{a}}$ be the bilinear mapping on $\widehat{V} \times \widehat{V}$ defined by

$$f_{\mathbf{a}}(v_i, v_j) = a_{m-i+j}^{q^{i-1}} \quad \text{for } i, j = 1, \ldots, m$$

where subscripts are taken modulo m, and then extended over $\widehat{V}$ by linearity. Set $L_{\mathbf{a}}(x) = \sum_{i=0}^{m-1} a_i x^{q^i}$ and let Tr denote the trace function from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$:

$$\mathrm{Tr} : y \in \mathbb{F}_{q^m} \to \mathrm{Tr}(y) = \sum_{j=0}^{m-1} y^{q^j} \in \mathbb{F}_q.$$

It is easily seen that the action of $f_{\mathbf{a}}$ on $V \times V$ is given by

$$f_{\mathbf{a}}(v, v') = f_{\mathbf{a}}(x, x') = \mathrm{Tr}(L_{\mathbf{a}}(x')x), \tag{2}$$

with $v = \sum_{i=1}^{m} x^{q^{i-1}} v_i$, $v' = \sum_{j=1}^{m} x'^{q^{j-1}} v_j$, which is a bilinear form on $V \times V$. The assertion follows from consideration on the size of $\mathcal{D}_m(\mathbb{F}_{q^m})$. □

For any m-ple $\mathbf{a} = (a_0, \ldots, a_{m-1})$ over $\mathbb{F}_{q^m}$, $f_{\mathbf{a}}$ will denote the bilinear form having matrix $D_{\mathbf{a}}$ in the Singer basis $v_1, \ldots, v_m$. For any set $\mathcal{A}$ of $m-$ples over $\mathbb{F}_{q^m}$ we put

$$\mathcal{F}_{\mathcal{A}} = \{f_{\mathbf{a}} \in \Omega : \mathbf{a} \in \mathcal{A}\}.$$

Corollary 3. *Let* $\mathbf{a} = (a_0, \ldots, a_{m-1})$. *Then*

$$\begin{array}{rccc} \nu_{\{v_1,\ldots,v_m\}} : & \Omega & \to & \mathcal{D}_m(\mathbb{F}_{q^m}) \\ & f_{\mathbf{a}} & \mapsto & D_{(a_0,\ldots,a_{m-1})} \end{array} \tag{3}$$

is an isomorphism of rank metric spaces giving $\mathrm{rk}(f_{\mathbf{a}}) = \mathrm{rk}(D_{(a_0,\ldots,a_{m-1})})$.

Remark 4. By Proposition 1, $\mathrm{Aut}_{\mathbb{F}_q}(\Omega)$ is represented by the group $(\mathcal{B}_m(\mathbb{F}_{q^m}) \times \mathcal{B}_m(\mathbb{F}_{q^m})) \rtimes \langle t \rangle \rtimes \mathrm{Aut}(\mathbb{F}_q)$ in the Singer basis $v_1, \ldots, v_m$. Here, t denote transposition in $M_{m,m}(\mathbb{F}_{q^m})$ and it corresponds to the operator $\top$.

Remark 5. Note that (2) coincides with the bilinear form (6.1) in [11] when $m' = m$.

Remark 6. Since a change of basis in $\widehat{V} \times \widehat{V}$ preserves the rank of bilinear forms, for any given $f \in \Omega$ we can consider its matrix representation in the Singer basis $v_1, \ldots, v_m$. Therefore, we can assume $f = f_{\mathbf{a}}$ for some m-ple $\mathbf{a}$ over $\mathbb{F}_{q^m}$, so that $\mathrm{Rad}(f_{\mathbf{a}})$ is the set of vectors $v' = x'v_1 + \cdots + x'^{q^{m-1}} v_m \in V$, $x' \in \mathbb{F}_{q^m}$, such that $L_{\mathbf{a}}(x') = 0$.

We are now in position to construct non-linear MRD codes as subsets of Ω.

Let N denote the norm map from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$:

$$N : x \in \mathbb{F}_{q^m} \to N(x) = \prod_{j=0}^{m-1} x^{q^j} \in \mathbb{F}_q.$$

For every nonzero element $\alpha \in \mathbb{F}_{q^m}$, let

$$\pi_\alpha = \{(\lambda x, \lambda\alpha x^q, \lambda\alpha^{1+q} x^{q^2}, \ldots, \lambda\alpha^{1+q+\cdots+q^{m-2}} x^{q^{m-1}}) : \lambda, x \in \mathbb{F}_{q^m} \setminus \{0\}\}.$$

Remark 7. The matrix of the Singer cycle σ of V in the basis $v_1, \ldots, v_m$ is given by $\mathrm{diag}(\mu, \mu^q, \ldots, \mu^{q^{m-1}})$, where μ is a generator of the multiplicative group of $\mathbb{F}_{q^m}$ [7]. If S is the Singer cyclic group generated by σ, then the set $\mathcal{F}_{\pi_a}$ is the $(S \times S)$-orbit of the bilinear form $f_{\mathbf{a}}$, with $\mathbf{a} = (1, \alpha, \alpha^{1+q}, \ldots, \alpha^{1+\cdots+q^{m-2}})$. It turns out that the bilinear forms in $\mathcal{F}_{\pi_a}$ have constant rank.

Proposition 8. *$\pi_\alpha = \pi_\beta$ if and only if $N(\alpha) = N(\beta)$.*

Proof. Let $\alpha, \beta \in \mathbb{F}_{q^m} \setminus \{0\}$ such that $N(\alpha) = N(\beta)$. By Remark 7 it suffices to show that $(1, \alpha, \alpha^{1+q}, \ldots, \alpha^{1+q+\cdots+q^{m-2}})$ is in π_β.

Since $N(\alpha) = N(\beta)$, then $\alpha = \beta c^{q-1}$ for some $c \in \mathbb{F}_{q^m} \setminus \{0\}$. As $(1 + q + \cdots + q^k)(q - 1) = q^{k+1} - 1$, we have

$$\alpha^{1+q+\cdots+q^k} = c^{-1} \beta^{1+q+\cdots+q^k} c^{q^{k+1}}.$$

Conversely, let $\pi_\alpha = \pi_\beta$. Then

$$\begin{array}{rcl} 1 & = & \lambda x \\ \alpha & = & \lambda \beta x^q \\ \alpha^{1+\cdots+q^{m-2}} & = & \lambda \beta^{1+\cdots+q^{m-2}} x^{q^{m-1}} \end{array} \tag{4}$$

for some $\lambda, x \in \mathbb{F}_{q^m} \setminus \{0\}$. From the last equation we get

$$\alpha^{q+q^2+\cdots+q^{m-1}} = \lambda^q \beta^{q+q^2+\cdots+q^{m-1}} x.$$

By taking into account the first and second equation of (4) we get $N(\alpha) = \lambda^q \lambda N(\beta) x x^q = N(\beta)$. □

We will write π_a instead of π_α, if α is an element of $\mathbb{F}_{q^m} \setminus \{0\}$ with $N(\alpha) = a$.

Lemma 9. *Every π_a has size $(q^m - 1)^2/(q - 1)$.*

Proof. Let $\alpha \in \mathbb{F}_{q^m} \setminus \{0\}$ with $N(\alpha) = a$. Clearly, we have

$$(\lambda x, \lambda \alpha x^q, \lambda \alpha^{1+q} x^{q^2}, \ldots, \lambda \alpha^{1+\cdots+q^{m-2}} x^{q^{m-1}}) = (\rho y, \rho \alpha y^q, \rho \alpha^{1+q} y^{q^2}, \ldots, \rho \alpha^{1+\cdots+q^{m-2}} x^{q^{m-1}})$$

if and only if $\lambda x^{q^i} = \rho y^{q^i}$, for $i = 0, \ldots, m - 1$. If we compare the equalities with $i = 0$ and $i = 1$, we get $x^{q-1} = y^{q-1}$. For every fixed $x \in \mathbb{F}_{q^m}$ there are exactly $q - 1$ elements y in $\mathbb{F}_{q^m}$ such that $y^{q-1} = x^{q-1}$.

Let λ and x be fixed elements in $\mathbb{F}_{q^m} \setminus \{0\}$. Then, for each element $y \in \mathbb{F}_{q^m}$ such that $y^{q-1} = x^{q-1}$ we get the unique element $\rho = \lambda x y^{-1}$ and the result is proved. □

Lemma 10. *i) If $\mathbf{a} \in \pi_1$, then $\mathrm{rk}(f_{\mathbf{a}}) = 1$.*

ii) If $a \in \mathbb{F}_q \setminus \{0, 1\}$, then $\mathrm{rk}(f_{\mathbf{a}}) = m$, for any $\mathbf{a} \in \pi_a$.

iii) If $a, b \in \mathbb{F}_q \setminus \{0, 1\}$, then $\mathrm{rk}(f_{\mathbf{a}} - f_{\mathbf{b}}) \geqslant m - 1$, for any $\mathbf{a} \in \pi_a$ and $\mathbf{b} \in \pi_b$, with $\mathbf{b} \neq \mathbf{a}$ if $a = b$.

Proof. i) Let $\mathbf{a} = (\lambda x, \lambda x^q, \ldots, \lambda x^{q^{m-1}}) \in \pi_1$. It suffices to note that $L_{\mathbf{a}}(z) = (\lambda x)z + (\lambda x^q)z^q + \cdots (\lambda x^{q^{m-1}})z^{q^{m-1}} = 0$ is the equation of a hyperplane in the cyclic model of V.

ii) By Remark 7, we may assume $\mathbf{a} = (1, \alpha, \ldots, \alpha^{1+\cdots+q^{m-2}})$, with $N(\alpha) = a \neq 1$.

For any $z \in \mathrm{Rad}(f_{\mathbf{a}})$, we have

$$L_a(z) = z + \alpha z^q + \cdots + \alpha^{1+\cdots+q^{m-2}} z^{q^{m-1}} \quad = \quad 0, \tag{5}$$

giving $\alpha[L_{\mathbf{a}}(z)]^q - L_{\mathbf{a}}(z) = (N(\alpha) - 1)z = 0$. As $N(\alpha) = a \neq 1$, we get $z = 0$.

iii) Let $\mathbf{a} = (1, \alpha, \ldots, \alpha^{1+\cdots+q^{m-2}})$, with $N(\alpha) = a \neq 1$, and

$$\mathbf{b} = (\lambda x, \lambda\beta x^q, \ldots, \lambda\beta^{1+q+\cdots+q^{m-2}} x^{q^{m-1}}),$$

with $N(\beta) = b \neq 1$.

For any $z \in \mathrm{Rad}(f_{\mathbf{a}} - f_{\mathbf{b}})$, we have

$$\begin{aligned} L_{\mathbf{a}-\mathbf{b}}(z) \quad &= \quad (1 - \lambda x)z + (\alpha - \lambda\beta x^q)z^q + \\ &\cdots + (\alpha^{1+\cdots+q^{m-2}} - \lambda\beta^{1+\cdots+q^{m-2}} x^{q^{m-1}})z^{q^{m-1}} \quad = \quad 0 \end{aligned} \tag{6}$$

and

$$\begin{aligned} &(\alpha^{q+\cdots+q^{m-1}} - \lambda^q\beta^{q+\cdots+q^{m-1}} x)z + (1 - \lambda^q x^q)z^q + \\ &\cdots + (\alpha^{q+\cdots+q^{m-2}} - \lambda^q\beta^{q+\cdots+q^{m-2}} x^{q^{m-1}})z^{q^{m-1}} \quad = 0, \end{aligned} \tag{7}$$

for $i = 1, 2$.

After subtracting Equation (6) side-by-side from Equation (7) multiplied by α, we get

$$\begin{aligned} &[a - 1 + (\lambda - \lambda^q\alpha\beta^{q+\cdots+q^{m-1}})x]z + (\lambda\beta - \lambda^q\alpha)x^q z^q + \\ &\cdots + (\lambda\beta - \lambda^q\alpha)\beta^{q+\cdots+q^{m-2}} x^{q^{m-1}} z^{q^{m-1}} \quad = \quad 0. \end{aligned} \tag{8}$$

Suppose $\lambda\beta = \lambda^q\alpha$. Then, $[a - 1 - (b - 1)\lambda x]z = 0$. Suppose $a - 1 - (b - 1)\lambda x = 0$, i.e. $\lambda = \dfrac{a-1}{b-1}x^{-1}$. By plugging this value in $\mathbf{b}$, we get

$$\mathbf{b} = \frac{a-1}{b-1}\left(1, \beta x^{q-1}, \beta^{1+q} x^{q^2-1}, \ldots, \beta^{1+q+\cdots+q^{m-2}} x^{q^{m-1}-1}\right)$$

Note that if $b = a$, we can assume $\beta = \alpha$ giving $x \notin \mathbb{F}_q$ as $\mathbf{b} \neq \mathbf{a}$.

We claim that the bilinear form $f_{\mathbf{a}} - f_{\mathbf{b}}$ has maximum rank m. Indeed, suppose there exists a nonzero $z \in \mathbb{F}_{q^m}$ such that $L_{\mathbf{a}-\mathbf{b}}(z) = 0$. By plugging that value of λ in Equation (8) we get

$$\begin{aligned} &\frac{a-1}{b-1}\Big[(\beta - \alpha(x^{-1})^{q-1})\beta^{q+\cdots+q^{m-1}} z + (\beta x^{q-1} - \alpha)z^q + \\ &\cdots + (\beta x^{q^{m-1}-1} - \alpha x^{q^{m-1}-q})\beta^{q+\cdots+q^{m-2}} z^{q^{m-1}}\Big] \quad = \quad 0 \end{aligned}$$

or, equivalently,

$$\left(\frac{\beta}{x} - \frac{\alpha}{x^q}\right)(\beta^{q+\cdots+q^{m-1}} xz + (xz)^q + \beta^q(xz)^{q^2} + \cdots + \beta^{q+\cdots+q^{m-2}}(xz)^{q^{m-1}}) \quad = \quad 0,$$

where $\dfrac{\beta}{x}-\dfrac{\alpha}{x^q}\neq 0$ since either $b\neq a$ or $x^q\neq x$ if $b=a$. Therefore, the following equation holds:

$$\beta^{q+\cdots+q^{m-1}}y+y^q+\beta^q y^{q^2}+\beta^{q+q^2}y^{q^3}+\cdots+\beta^{q+\cdots+q^{m-2}}y^{q^{m-1}} \;=\; 0 \tag{9}$$

given

$$\beta^{q^2+\cdots+q^{m-1}}y+\beta^{1+q^2+\cdots+q^{m-1}}y^q+y^{q^2}+\beta^{q^2}y^{q^3}+\cdots+\beta^{q^2+\cdots+q^{m-2}}y^{q^{m-1}} \;=\; 0. \tag{10}$$

By subtracting Equation (9) from (10) multiplied by β^q we get $b=1$, a contradiction. Hence, we may assume $a-1-(b-1)\lambda x\neq 0$, giving $z=0$.

If $\Delta=\lambda\beta-\lambda^q\alpha\neq 0$, we set $\nabla=a-1+(\lambda-\lambda^q\alpha\beta^{q+\cdots+q^{m-1}})x$. From Equation (8), then we get

$$\frac{\nabla}{\Delta}z+(xz)^q+\cdots+\beta^{q+\cdots+q^{m-2}}(xz)^{q^{m-1}}=0. \tag{11}$$

If we multiply by β^q the q-th power of equation (11) and then subtract it from (11), we get the q-polynomial

$$\left(x^q-\beta^q\frac{\nabla^q}{\Delta^q}\right)z^q+\left(\frac{\nabla}{\Delta}-\beta^{q+\cdots+q^{m-1}}x\right)z=0. \tag{12}$$

If $\nabla-\beta^{q+\cdots+q^{m-1}}x\Delta=0$, then $\lambda=\dfrac{a-1}{b-1}x^{-1}$ which implies $\mathrm{rk}(f_{\mathbf{a}}-f_{\mathbf{b}})=m$. Therefore, we may assume $\beta^{q+\cdots+q^{m-1}}x\Delta-\nabla\neq 0$, giving (12) is a nonzero polynomial of degree at most q. This means, $\mathrm{rk}(f_{\mathbf{a}}-f_{\mathbf{b}})\geqslant m-1$. ☐

For every nonzero element $\alpha\in\mathbb{F}_{q^m}$, let

$$J_\alpha=\{(\lambda x,0,\ldots,0,-\lambda\alpha x^{q^{m-1}}):\lambda,x\in\mathbb{F}_{q^m}\setminus\{0\}\}.$$

Remark 11. Note that the set $\mathcal{F}_{J_\alpha}$ is the $(S\times S)$-orbit of the bilinear form $f_{\mathbf{a}}$, with $\mathbf{a}=(1,0,\ldots,0,-\alpha)$. It turns out that the bilinear forms in $\mathcal{F}_{J_\alpha}$ have constant rank.

By arguing similarly to the proof of Proposition 8 and Lemma 9, we get the following result.

Lemma 12. *Each set J_α has size $(q^m-1)^2/(q-1)$ and $J_\alpha=J_\beta$ if and only if $N(\alpha)=N(\beta)$.*

We will write J_a instead of J_α, if α is an element of $\mathbb{F}_{q^m}$ with $N(\alpha)=a$.

Lemma 13. *For any $\mathbf{a}=(x,0,\ldots,0,y)$ with $x,y\in\mathbb{F}_{q^m}$ not both zero, $\mathrm{rk}(f_{\mathbf{a}})\geqslant m-1$.*

Proof. The bilinear form $f_{\mathbf{a}}$, is equivalent to the bilinear form $f_{\hat{\mathbf{a}}}$, with $\hat{\mathbf{a}}=(x,y^q,0,\ldots,0)$, via the automorphism $\top$. The result then follows from Remark 5 and Theorem 6.3 in [11]. ☐

Corollary 14. *Let a, b be nonzero elements in $\mathbb{F}_q$. Then* $\mathrm{rk}(f_{\mathbf{a}} - f_{\mathbf{b}}) \geqslant m-1$, *for any* $\mathbf{a} \in J_a$ *and* $\mathbf{b} \in J_b$, *with* $\mathbf{a} \neq \mathbf{b}$ *if a=b.*

Lemma 15. *Let a, b be distinct nonzero elements in $\mathbb{F}_q$. Then* $\mathrm{rk}(f_{\mathbf{a}} - f_{\mathbf{b}}) \geqslant m-1$ *for any* $\mathbf{a} \in \pi_a$ *and* $\mathbf{b} \in J_b$.

Proof. By Remark 7 we can assume $\mathbf{a} = (1, \alpha, \ldots, \alpha^{1+\cdots+q^{m-2}})$ with $N(\alpha) = a$. By arguing as in the proof of Lemma 10 we see that the triple

$$(a - 1 + (\lambda + \alpha\beta^q\lambda^q)x, -\alpha\lambda^q x^q, -\lambda\beta x^{q^{m-1}}) \tag{13}$$

is a solution of the linear system

$$\begin{cases} z_1 X_1 + z_1^q X_2 + z_1^{q^{m-1}} X_3 &= 0 \\ z_2 X_1 + z_2^q X_2 + z_2^{q^{m-1}} X_3 &= 0 \end{cases} \tag{14}$$

for some $z_1, z_2 \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ with $\Delta = \begin{vmatrix} z_1 & z_1^q \\ z_2 & z_2^q \end{vmatrix} \neq 0$. Any solution (x_1, x_2, x_3) of (14) satisfies

$$x_2 = -\frac{\Delta'}{\Delta} x_3$$

where $\Delta' = \begin{vmatrix} z_1 & z_1^{q^{m-1}} \\ z_2 & z_2^{q^{m-1}} \end{vmatrix}$. Since $\Delta'^q = \begin{vmatrix} z_1^q & z_1 \\ z_2^q & z_2 \end{vmatrix} = -\Delta$ we get $x_2 = \dfrac{1}{\Delta'^{q-1}} x_3$ giving $N(x_2) = N(x_3)$. As a solution of (14), the triple (13) must satisfies $aN(\lambda)N(x) = bN(\lambda)N(x)$ giving either $\lambda x = 0$ or $a = b$, a contradiction. □

Let $A_1 = \{(x, 0, 0, \ldots, 0) : x \in \mathbb{F}_{q^m} \setminus \{0\}\}$ and $A_2 = \{(0, 0, 0, \ldots, x) : x \in \mathbb{F}_{q^m} \setminus \{0\}\}$.

Lemma 16. $\mathrm{rk}(f_{\mathbf{a}}) = m$, *for any* $\mathbf{a} \in A_i$, $i = 1, 2$. *Further,* $\mathrm{rk}(f_{\mathbf{a}} - f_{\mathbf{b}}) \geqslant m-1$, *for any* $\mathbf{a} \in A_1$ *and* $\mathbf{b} \in A_2$.

Proof. The first part can be easily proved by taking the Dickson matrix $D_{\mathbf{a}}$ with $\mathbf{a} \in A_i$. The second part follows from Lemma 13. □

Lemma 17. *Let $a \in \mathbb{F}_q \setminus \{0, 1\}$. Then* $\mathrm{rk}(f_{\mathbf{a}} - f_{\mathbf{b}}) \geqslant m-1$, *for any* $\mathbf{a} \in \pi_a$ *and* $\mathbf{b} \in A_i$, $i = 1, 2$.

Proof. By Remark 7 we can assume $\mathbf{a} = (1, \alpha, \ldots, \alpha^{1+\cdots+q^{m-2}})$ with $N(\alpha) = a$. Let $\mathbf{b} = (x, 0, \ldots, 0)$. By proceeding as in the proof of Lemma 10 we see the pair $(a-(1-x), -\alpha x^q)$ is a solution of the linear system

$$\begin{cases} z_1 X_1 + z_1^q X_2 &= 0 \\ z_2 X_1 + z_2^q X_2 &= 0 \end{cases}$$

with $\Delta = \begin{vmatrix} z_1 & z_1^q \\ z_2 & z_2^q \end{vmatrix} \neq 0$. Then the above linear system has the unique solution $(0, 0)$ giving $x = 0$ and $a = 1$, a contradiction.

For $i = 2$, similar arguments lead to the same contradiction. □

Lemma 18. *Let $a \in \mathbb{F}_q \setminus \{0\}$. Then $\mathrm{rk}(f_{\mathbf{a}} - f_{\mathbf{b}}) \geqslant m-1$, for any $\mathbf{a} \in J_a$ and $\mathbf{b} \in A_i$, $i = 1, 2$.*

Proof. Use Lemma 13. ☐

Finally, we have the main theorem.

Theorem 19. *Let $q > 2$ be a prime power and $m \geqslant 3$ a positive integer. For any subset I of $\mathbb{F}_q \setminus \{0,1\}$, put $\Pi_I = \bigcup_{a \in I} \pi_a$, $\Gamma_I = \bigcup_{b \in \mathbb{F}_q \setminus (I \cup \{0\})} J_b$ and set*

$$\mathcal{A}_{m,q;I} = \Pi_I \cup \Gamma_I \cup A_1 \cup A_2 \cup \{\mathbf{0}\}$$

where $\mathbf{0}$ is the zero $m-$ple. Then the subset $\mathcal{F}_{m,q;I} = \{f_{\mathbf{a}} : \mathbf{a} \in \mathcal{A}_{m,q;I}\}$ of Ω is a non-linear $(m, m, q; m-2)$-MRD code.

Proof. By Lemmas 9, 12 we get that $\mathcal{A}_{m,q;I}$ has size q^{2m}. By Lemmas 10, 13, 15, 16, 17 and Corollary 14, we see that $\mathcal{F}_{m,q;I}$ has minimum distance $m-1$, i.e. it is a $(m, m, q; m-2)$-MRD code. To show the non-linearity of $\mathcal{F}_{m,q;I}$, it suffices to find two distinct elements in it whose $\mathbb{F}_q$-span is not contained in $\mathcal{F}_{m,q;I}$.

Let $f_{\mathbf{a}} \in \mathcal{F}_{A_2}$ and $f_{\mathbf{b}} \in \mathcal{F}_{\pi_a}$, $a \in I$. By corollary 3, we can work with the Dickson matrices $D_{\mathbf{a}}$ and $D_{\mathbf{b}}$, or equivalently, with m-ples $\mathbf{a}$ and $\mathbf{b}$ as arrays in $V(m, q^m)$. Let $\mathbf{a} = (0, \ldots, 0, \mu)$ and $\mathbf{b} = (\lambda x, \lambda \alpha x^q, \ldots, \lambda \alpha^{1+\cdots+q^{m-2}} x^{q^{m-1}})$. Suppose $\mathbf{a} + \mathbf{b} \in \pi_b$, for some $b \in \mathbb{F}_q$. Then

$$\left(\frac{\lambda \alpha^{1+\cdots+q^{m-3}} x^{q^{m-2}}}{\lambda \alpha^{1+\cdots+q^{m-4}} x^{q^{m-3}}} \right)^q = \alpha^{q^{m-2}} x^{q^{m-1}-q^{m-2}} = \frac{\mu + \lambda \alpha^{1+\cdots+q^{m-2}} x^{q^{m-1}}}{\lambda \alpha^{1+\cdots+q^{m-3}} x^{q^{m-2}}}$$

giving $\mu = 0$. Therefore, the subspace spanned by $\mathbf{a}$ and $\mathbf{b}$ meets trivially every π_b if $b \neq a$, or just in the 1-dimensional subspace spanned by $\mathbf{b}$ if $b = a$. The result then follows. ☐

3 A geometric description for the non-linear MRD codes

Let $\mathrm{PG}(t-1, q^s)$ be the projective space whose points are the 1-dimensional subspaces of $V(t, q^s)$. For any $v \in V(t, q^s) \setminus \{0\}$, $[v]$ will denote the corresponding point of $\mathrm{PG}(t-1, q^s)$. For any subset X of $V(t, q^s) \setminus \{0\}$, we set $[X] = \{[v] : v \in X, v \neq 0\}$. The set $[X]$ is said to be an $\mathbb{F}_q$-*linear set of rank* r if X is an r-dimensional $\mathbb{F}_q$-linear subspace of $V(t, q^s)$. An $\mathbb{F}_q$-linear set $[X]$ of rank r is said to be *scattered* if the size of $[X]$ equals $|\mathrm{PG}(r-1, q)|$; see [31] for more details on $\mathbb{F}_q$-linear sets and [27] for a relationship between linear MRD-codes and $\mathbb{F}_q$-linear sets.

Consider the set $\mathcal{A}_{m,q;I}$ defined in Theorem 19 as a subset of $\widehat{V} = V(m, q^m)$, by setting $a_0 v_1 + a_1 v_2 + \cdots + a_{m-1} v_m$, for any $\mathbf{a} = (a_0, \ldots, a_{m-1}) \in \mathcal{A}_{m,q;I}$; here, $v_1, \ldots, v_m$ is the Singer basis of V defined in Section 2. Therefore, $[\pi_1] = [V]$ is a scattered $\mathbb{F}_q$-linear set of rank m of $\mathrm{PG}(m-1, q^m)$ isomorphic to the projective space $\mathrm{PG}(m-1, q)$.

For any $\alpha \in \mathbb{F}_{q^m} \setminus \{0\}$, the endomorphism

$$\tau_\alpha : \begin{array}{ccc} \widehat{V} & \rightarrow & \widehat{V} \\ a_0v_1 + a_1v_2 + \cdots + a_{m-1}v_m & \mapsto & a_0v_1 + \alpha a_1v_2 + \cdots + \alpha^{1+\cdots+q^{m-2}}a_{m-1}v_m \end{array}$$

maps π_1 into π_a, with $a = N(\alpha)$, and J_1 into J_b, with $b = a^{m-1}$.

Let W be the span of v_1 and v_m in $\widehat{V}$. For any $a \in \mathbb{F}_q \setminus \{0\}$, $[J_a]$ is a scattered $\mathbb{F}_q$-linear set of rank m of $[W]$. In particular $[J_a]$ is a maximum scattered $\mathbb{F}_q$-linear set of pseudoregulus type of $[W]$ [24, 29].

Summarizing we have the following result.

Theorem 20. *Let $q > 2$ be a prime power and $m > 2$ a positive integer. Let I be any nonempty subset of $\mathbb{F}_q \setminus \{0, 1\}$ with $k = |I|$. Then, the projective image of $\mathcal{A}_{m,q;I}$ in* $\mathrm{PG}(m-1, q^m)$ *is union of two points $[A_1], [A_2]$, k mutually disjoint $(m-1)$-dimensional $\mathbb{F}_q$-subgeometries $[\pi_a]$, $a \in I$, and $q-1-k$ mutually disjoint $\mathbb{F}_q$-linear sets $[J_b], b \in \mathbb{F}_q \setminus (I \cup \{0\})$, of pseudoregulus type of rank m contained in the line spanned by $[A_1]$ and $[A_2]$.*

We now investigate the geometry in $\mathrm{PG}(m^2 - 1, q)$ of the projective set defined by each MRD code $\mathcal{F}_{m,q;I}$ viewed as a subset of $V(m^2, q)$.

Let $V = V(m, q)$ be the $\mathbb{F}_q$-span of $u_1, \ldots, u_m$ and set $\widehat{V} = V(m, q^m) = \mathbb{F}_{q^m} \otimes V(m, q)$. The *rank* of a vector $v = a_1u_1 + a_2u_2 + \cdots + a_mu_m \in \widehat{V}$ by definition is the maximum number of linearly independent coordinates a_i over $\mathbb{F}_q$.

If we consider $\mathbb{F}_{q^m}$ as the m-dimensional vector space V, then every $\alpha \in \mathbb{F}_{q^m}$ can be uniquely written as $\alpha = x_1u_1 + x_2u_2 + \cdots + x_mu_m$, with $x_i \in \mathbb{F}_q$. Hence, $\widehat{V}$ can be viewed as $V \otimes V$, the tensor product of V with itself, with basis $\{u_{(i,j)} = u_i \otimes u_j : i, j = 1, \ldots, m\}$. Elements of $V \otimes V$ are called *tensors* and those of the form $v \otimes v'$, with $v, v' \in V$ are called *fundamental tensors*. In $\mathrm{PG}(V \otimes V)$, the set of fundamental tensors correspond to the Segre variety $\mathcal{S}_{m,m}(\mathbb{F}_q)$ of $\mathrm{PG}(V \otimes V)$ [20].

Let ϕ be the map defined by

$$\phi = \phi_{\{u_1,\ldots,u_m\}} : \begin{array}{ccc} \widehat{V} & \longrightarrow & V \otimes V \\ \alpha_1u_1 + \cdots + \alpha_mu_m & \longmapsto & \sum_{i=1}^m x_{i1}\, u_{(i,1)} + \cdots + \sum_{i=1}^m x_{im}\, u_{(i,m)}, \end{array}$$

with $\alpha_k = x_{1k}u_1 + x_{2k}u_2 + \cdots + x_{mk}u_m$, $x_{ik} \in \mathbb{F}_q$. We call this map the *field reduction of $\widehat{V}$ over $\mathbb{F}_q$ with respect to the basis $u_1, \ldots, u_m$*. The projective space $\mathrm{PG}(V \otimes V)$ is the *the field reduction* of $\mathrm{PG}(\widehat{V})$ *over $\mathbb{F}_q$ with respect to the basis $u_1, \ldots, u_m$*.

Under ϕ, every 1-dimensional subspace $\langle v\rangle$ of $\widehat{V}$ is mapped to the m-dimensional $\mathbb{F}_q$-subspace $k_v = \phi(\langle v\rangle)$ of $V \otimes V$. It turns out that the set $\mathcal{K} = \{k_v : v \in \widehat{V}, v \neq 0\}$ is a partition of the nonzero vectors of $V \otimes V$. In particular $\mathcal{K}$ is a *Desarguesian* partition, i.e. the stabilizer of $\mathcal{K}$ in $\mathrm{GL}(V \otimes V)$ contains a cyclic subgroup acting regularly on the components of $\mathcal{K}$ [14, 34].

To any component k_v of $\mathcal{K}$ there corresponds a projective $(m-1)-$dimensional subspace $[k_v]$ of $\mathrm{PG}(V \otimes V)$. The set $\mathcal{S} = \{[k_v] : v \in \widehat{V}, v \neq 0\}$ is so called a *Desarguesian* $(m-1)-$*spread* of $\mathrm{PG}(V \otimes V)$ [34], [14].

In addition, the projective set of $\mathrm{PG}(V \otimes V)$ corresponding to the ϕ-image of the 1-dimensional subspaces spanned by non-zero vectors in V is the Segre variety $\mathcal{S}_{m,m}(\mathbb{F}_q)$.

Let ν be the map defined by

$$\nu = \nu_{\{u_1,\ldots,u_m\}} : \quad \begin{array}{ccc} V \otimes V & \longrightarrow & M_{m,m}(\mathbb{F}_q) \\ \sum_{i,j} x_{ij} u_{(i,j)} & \longrightarrow & (x_{ij})_{i,j=1,\ldots,m}. \end{array}$$

For every $v = \alpha_1 u_1 + \cdots + \alpha_m u_m \in \widehat{V}$, the k-th column of the matrix $\nu(\phi(v))$ is the m-ple $(x_{1k}, \ldots, x_{mk})$ of the coordinates of α_k with respect to the basis $u_1, \ldots, u_m$ of $\mathbb{F}_{q^m}$. From [16], the rank of v equals the rank of $\nu(\phi(v))$, for all $v \in \widehat{V}$. In addition, the ν-image of fundamental tensors is precisely the set of rank 1 matrices.

Remark 21. Evidently, ν is an isomorphism of rank metric spaces which also provides an isomorphism between the field reduction $V \otimes V$ of $\widehat{V}$ with respect to $u_1, \ldots, u_m$ and the metric space Ω of all bilinear forms on $V = \langle u_1, \ldots, u_m \rangle_{\mathbb{F}_q}$.

Now embed $V \otimes V$ into $\widehat{V} \otimes \widehat{V}$ by extending the scalars from $\mathbb{F}_q$ to $\mathbb{F}_{q^m}$. By taking a Singer basis $v_1, \ldots, v_m$ of V defined by the Singer cycle σ, Cooperstein [7] defined a cyclic model for $V \otimes V$ within $\widehat{V} \otimes \widehat{V}$ with basis $v_{(i,j)} = v_i \otimes v_j$, $i, j = 1, \ldots, m$. Let

$$\Phi(j) = \{\sum_{i=1}^{m} a^{q^{i-1}} v_{(i,j-1+i)} : a \in \mathbb{F}_{q^m}\},$$

where the subscript $j-1+i$ is taken modulo m. As an $\mathbb{F}_q$-space, $\Phi(j)$ has dimension m and by consideration on dimension we have

$$V \otimes V = \bigoplus_{j=1}^{m} \Phi(j);$$

see [7]. We call this representation the *cyclic representation of the tensor product* $V \otimes V$.

Proposition 22. *Let $v_1, \ldots, v_m$ be a Singer basis of V and $\widetilde{\phi}$ be the map defined by*

$$\widetilde{\phi} = \phi_{\{v_1,\ldots,v_m\}} : \quad \begin{array}{ccc} \widehat{V} & \longrightarrow & \widehat{V} \otimes \widehat{V} \\ \alpha_1 v_1 + \cdots + \alpha_m v_m & \longmapsto & \sum_{i=1}^{m} \alpha_1^{q^{i-1}} v_{(i,i)} + \cdots + \sum_{i=1}^{m} \alpha_m^{q^{i-1}} v_{(i,m-1+i)}. \end{array}$$

Then $\mathrm{Im}(\widetilde{\phi})$ *is precisely* $\mathrm{Im}(\phi)$ *within* $\widehat{V} \otimes \widehat{V}$.

Proof. We notice that, for any given vector $u \in V$ we may write $u = \sum_{i=1}^{m} x_i u_i = \sum_{i=1}^{m} a^{q^{i-1}} v_i$, for some $x_i \in \mathbb{F}_q$, $i = 1, \ldots, m$ and $a \in \mathbb{F}_{q^m}$. Let $v = \sum_{i=1}^{m} \alpha_i v_i \in \widehat{V}$ be linear combination of k vectors of rank 1, $1 \leqslant k \leqslant m$.

Assume first $k = 1$, i.e. $v = \lambda(\sum_{i=1}^m a^{q^{i-1}} v_i)$, and set $\lambda = \sum_{i=1}^m l_i u_i$, $a = \sum_{i=1}^m x_i u_i$, with $l_i, x_i \in \mathbb{F}_q$. Therefore, $v = \lambda(\sum_{i=1}^m x_i u_i)$ and

$$\begin{array}{rcl} \widetilde{\phi}(v) & = & (\sum_{i=1}^m \lambda^{q^{i-1}} v_i) \otimes (\sum_{i=1}^m a^{q^{i-1}} v_i) \\ & = & (\sum_{i=1}^m l_i u_i) \otimes (\sum_{i=1}^m x_i u_i) \\ & = & \sum_{i=1}^m l_i x_1 u_{(i1)} + \cdots + \sum_{i=1}^m l_i x_m u_{(im)} \\ & = & \phi(v). \end{array}$$

Now assume $v = \lambda_1(\sum_{i=1}^m a_1^{q^{i-1}} v_i) + \cdots + \lambda_k(\sum_{i=1}^m a_k^{q^{i-1}} v_i)$, $k > 1$. Set $\lambda_j = \sum_{i=1}^m l_{ij} u_i$, $a_j = \sum_{i=1}^m x_{ij} u_i$, with $l_{ij}, x_{ij} \in \mathbb{F}_q$. Therefore,

$$v = \lambda_1(\sum_{i=1}^m x_{i1} u_i) + \cdots + \lambda_k(\sum_{i=1}^m x_{ik} u_i) = \sum_{i=1}^m (\lambda_1 x_{i1} + \cdots + \lambda_k x_{ik}) u_i$$

giving $\phi(v) = \sum_{i=1}^m (l_{i1} x_{11} + \cdots + l_{ik} x_{1k}) u_{(i,1)} + \cdots + \sum_{i=1}^m (l_{i1} x_{m1} + \cdots + l_{ik} x_{mk}) u_{(i,m)}$.

On the other hand, we have

$$\begin{array}{rcl} \widetilde{\phi}(v) & = & (\sum_{i=1}^m \lambda_1^{q^{i-1}} v_i) \otimes (\sum_{i=1}^m a_1^{q^{i-1}} v_i) + \cdots + (\sum_{i=1}^m \lambda_k^{q^{i-1}} v_i) \otimes (\sum_{i=1}^m a_k^{q^{i-1}} v_i) \\ & = & (\sum_{i=1}^m l_{i1} u_i) \otimes (\sum_{i=1}^m x_{i1} u_i) + \cdots + (\sum_{i=1}^m l_{ik} u_i) \otimes (\sum_{i=1}^m x_{ik} u_i) \\ & = & \sum_{i=1}^m l_{i1} x_{11} u_{(i1)} + \cdots + \sum_{i=1}^m l_{i1} x_{m1} u_{(im)} + \cdots \\ & & + \sum_{i=1}^m l_{ik} x_{1k} u_{(i1)} + \cdots + \sum_{i=1}^m l_{ik} x_{mk} u_{(im)} \\ & = & \sum_{i=1}^m (l_{i1} x_{11} + \cdots + l_{ik} x_{1k}) u_{(i1)} + \cdots + \sum_{i=1}^m (l_{i1} x_{m1} + \cdots + l_{ik} x_{mk}) u_{(im)} \\ & = & \phi(v). \end{array}$$

□

We call the map $\widetilde{\phi}$ the *field reduction of* $\widehat{V}$ *over* $\mathbb{F}_q$ *with respect to the Singer basis* $v_1, \ldots, v_m$ and its image the *cyclic model for the field reduction of* $\widehat{V}$ over $\mathbb{F}_q$. The projective space whose points are the 1-dimensional $\mathbb{F}_q$−subspaces generated by the elements of $\widetilde{\phi}(\widehat{V})$ is the *cyclic model for the field reduction* of $\mathrm{PG}(\widehat{V})$ over $\mathbb{F}_q$.

Let $\widetilde{\nu}$ be the map defined by

$$\widetilde{\nu} = \nu_{\{v_1,\ldots,v_m\}} : \quad \begin{array}{ccc} \widehat{V} \otimes \widehat{V} & \longrightarrow & M_{m,m}(\mathbb{F}_{q^m}) \\ \sum_{i,j} x_{ij} v_{(i,j)} & \longrightarrow & (x_{ij})_{i=1,\ldots,m}^{j=1,\ldots,m}. \end{array}$$

Then, for any $v = \alpha_1 v_1 + \cdots + \alpha_m v_m \in \widehat{V}$, the matrix $\widetilde{\nu}(\widetilde{\phi}(v))$ is the Dickson matrix $D_{(\alpha_1,\ldots,\alpha_m)}$. Since the cyclic model for the field reduction of $\widehat{V}$ is obtained from the field reduction $\phi(\widehat{V})$ by changing a basis in $\widehat{V} \otimes \widehat{V}$, we get that the rank of $\widetilde{\nu}(\widetilde{\phi}(v))$ equals the rank of $\nu(\phi(v))$, for any $v \in \widehat{V}$.

In addition, the element $k_v = \widetilde{\phi}(\langle v \rangle)$ of the m-partition $\mathcal{K}$ is

$$k_v = \{\sum_{i=1}^m (\lambda\alpha_1)^{q^{i-1}} v_{(i,i)} + \cdots + \sum_{i=1}^m (\lambda\alpha_m)^{q^{i-1}} v_{(i,m-1+i)} : \lambda \in \mathbb{F}_{q^m}\}.$$

In particular, $\bigcup_{v\in V\setminus\{0\}} \widetilde{\nu}(k_v)$ is the set of all rank 1 matrices in $\mathcal{D}_m(\mathbb{F}_{q^m})$.

From the arguments above, we see that the set $\mathcal{F}_{m,q;I}$ can be considered, via the isomorphism (3), as the field reduction of the set $\mathcal{A}_{m,q;I}$ with respect to the Singer basis $v_1,\dots,v_m$.

As $[\pi_1]=[V]$, then the set $\mathcal{F}_{\pi_1}=\widetilde{\phi}(\pi_1)$ defines the Segre variety $\mathcal{S}_{m,m}(\mathbb{F}_q)$ of $\mathrm{PG}(V\otimes V)$ and $\mathcal{F}_{\pi_a}$ defines a Segre variety projectively equivalent to $\mathcal{S}_{m,m}(\mathbb{F}_q)$ under the element of $\mathrm{PGL}(V\otimes V)$ corresponding to the linear transformation τ_α with $N(\alpha)=a$.

Remark 23. Note that, whenever $a\neq 1$, elements in $\mathcal{F}_{\pi_a}$ have rank bigger than 1 by Lemma 10. This is explained by the fact that the linear transformation of $V\otimes V = V(m^2,q)$ corresponding to τ_α is not in $\mathrm{Aut}_{\mathbb{F}_q}(V\otimes V)$.

Let $W=\langle v_1,v_m\rangle\subset\widehat{V}$. Then $\widetilde{\phi}(W)$ is a $2m$-dimensional vector subspace of $V\otimes V$. In $[\widetilde{\phi}(W)]$, the set $[\widetilde{\phi}(J_1)]$ is the Bruck norm-surface

$$\mathcal{N}=\mathcal{N}_{(-1)^m}=\{[\widetilde{\phi}(xv_1+yv_m)] : x,y\in\mathbb{F}_{q^m},\ N(y/x)=(-1)^m\}$$

introduced in [3] and widely investigated in [4, 5] and recently in [10, 23]. For any $x\in\mathbb{F}_{q^m}\setminus\{0\}$ set $J_x=\{\lambda x v_1-\lambda x^{q^{m-1}}v_m : \lambda\in\mathbb{F}_{q^m}\}$. Then $[\widetilde{\phi}(J_x)]\subset\mathcal{N}$ and the set $\{[\widetilde{\phi}(J_x)] : x\in\mathbb{F}_{q^m}\}$ is a so-called *hyper-regulus* of $\mathrm{PG}(\widetilde{W})$ [30]. It turns out, that under the linear transformation τ_α with $N(\alpha)=a$, also J_a defines a hyper-regulus of $[\widetilde{\phi}(W)]$.

The following result, which summarizes all above arguments, gives a geometric description of the MRD codes $\mathcal{F}_{m,q;I}$.

Theorem 24. *Let $q>2$ be a prime power and $m>2$ a positive integer. Let I be any nonempty subset of $\mathbb{F}_q\setminus\{0,1\}$ with $k=|I|$. The projective image of the MRD code $\mathcal{F}_{m,q;I}$ in $\mathrm{PG}(m^2-1,q)$ is a subset of a Desarguesian spread which is union of two spread elements, k mutually disjoint Segre varieties $\mathcal{S}_{m,m}(\mathbb{F}_q)$ and $q-1-k$ mutually disjoint hypereguli all contained in the $(2m-1)$-dimensional projective subspace generated by the two spread elements.*

4 The Cossidente-Marino-Pavese non-linear MRD code

Recently, Cossidente, Marino and Pavese constructed non-linear $(3,3,q;1)$-MRD codesin a totally geometric setting [8, Theorem 3.6].

In $\mathrm{PG}(2,q^3)$, $q\geqslant 3$, let $\mathcal{C}$ be the set of points whose coordinates satisfy the equation $X_1X_2^q-X_3^{q+1}=0$, that is a C_F^1*-set* of $\mathrm{PG}(2,q^3)$ as introduced and studied in [13]. The set $\mathcal{C}$ is the projective image of a subset of $V(3,q^3)$ which is the union of A_1, $A_2'=\{(0,x,0) : x\in\mathbb{F}_{q^3}\setminus\{0\}\}$ and the $q-1$ sets $\gamma_a=\{(\lambda,,\lambda x^{q+1},\lambda x^q) : \lambda,x\in\mathbb{F}_{q^3}\setminus\{0\}, N(x)=a\}$, with a a nonzero element of $\mathbb{F}_q$.

For any nonzero $a\in\mathbb{F}_q$, let $\alpha\in\mathbb{F}_{q^3}$ with $N(\alpha)=a$ and set $Z_a=\{(\lambda x,-\lambda\alpha x^q,0) : \lambda,x\in\mathbb{F}_{q^3}\setminus\{0\}\}$. Let I be any non-empty subset of $\mathbb{F}_q\setminus\{0,1\}$ and put

$$\mathcal{A}'(q;I)=\bigcup_{a\in I}\gamma_a\bigcup_{b\in\mathbb{F}_q\setminus(I\cup\{0\})}Z_b\cup A_1\cup A_2'\cup\{\mathbf{0}\}.$$

Up to an endomorphism of $V \otimes V$ viewed as the vector space $V(9,q)$, the image of set $\mathcal{A}'(q;I)$ under $\nu \circ \phi$ is a non-linear $(3,3,q;1)$-MRD code [8, Proposition 3.8].

Lemma 25. *Let θ be the semilinear transformation of $V(3,q^3)$ defined by*

$$\theta : \begin{array}{ccc} v_1 & \mapsto & v_3 \\ v_2 & \mapsto & v_1 \\ v_3 & \mapsto & v_2 \end{array}$$

with associated automorphism $x \mapsto x^{q^2}$. Then θ maps γ_a into $\pi_{a^{-1}}$ and Z_a into $J_{a^{-1}}$, for any nonzero element a of $\mathbb{F}_q$.

Proof. Every element $x \in \mathbb{F}_{q^3}$ with $N(x) = a$ can be written as $x = \alpha t^{q-1}$ for some $t \in \mathbb{F}_{q^3}$ and α a fixed element in $\mathbb{F}_{q^3}$ such that $N(\alpha) = a$. By straightforward calculations, we may write $\gamma_a = \{(\lambda x, \lambda\alpha^{q+1}x^q, \lambda\alpha^q x^{q^2}) : \lambda, x \in \mathbb{F}_{q^3}\}$. Then, we get $\theta(\gamma_a) = \{(\lambda x, \lambda(\alpha^{-1})^{q^2}x^q, \lambda(\alpha^{-1})^{(q^2+1)}x^{q^2}) : \lambda, x \in \mathbb{F}_{q^3}\} = \pi_{a^{-1}}$ as $N(\alpha^{-q^2}) = N(\alpha^{-1}) = a^{-1}$.

The last part of the statement follows from straightforward calculations. □

Corollary 26. *Let I be any non-empty subset I of $\mathbb{F}_q \setminus \{0,1\}$ and put $I^{-1} = \{a^{-1} : a \in I\}$. Then, up to the endomorphism θ of $V(3,q^3)$ and the changing of basis in $V(3,q^3) \otimes V(3,q^3)$ from $u_{(i,j)}$ to $v_{(i,j)}$, the Cossidente-Marino-Pavese family of non-linear MRD codes is the set $\mathcal{F}_{3,q,I^{-1}}$.*

Let L be any line of $\mathrm{PG}(2,q^3)$ disjoint from a subgeometry $\mathrm{PG}(2,q)$. The set of points of L that lie on some proper subspace spanned by points of $\mathrm{PG}(2,q)$ is called the *exterior splash* of $\mathrm{PG}(2,q)$ on L [25].

Proposition 27. *[10] The exterior splash of the subgeometry $[\pi_a]$ on the line $[W]$ is the set $[J_b]$ with $b = a^{m-1}$.*

Proof. First we note that $[W]$ is disjoint from $[\pi_1]$. The $\mathbb{F}_{q^m}$-span of some hyperplane in the cyclic model of V is a hyperplane of $\widehat{V}$ with equation $\sum_{i=1}^m \alpha^{q^{i-1}} X_i = 0$, for some nonzero$\alpha \in \mathbb{F}_{q^m}$. As the Singer cycle σ acts on the hyperplanes of V by mapping the hyperplane with equation $\sum_{i=1}^m \alpha^{q^{i-1}} X^{q^{i-1}} = 0$ to the hyperplane with equation $\sum_{i=1}^m (\mu\alpha)^{q^{i-1}} X^{q^{i-1}} = 0$, then σ maps the hyperplane of $\widehat{V}$ with equation $\sum_{i=1}^m \alpha^{q^{i-1}} X_i = 0$ into the hyperplane with equation $\sum_{i=1}^m (\mu\alpha)^{q^{i-1}} X_i = 0$. Note that σ fixes W.

The hyperplane $\sum_{i=1}^m X_i = 0$ of $\widehat{V}$ meets W in the $\mathbb{F}_{q^m}$-subspace spanned by $v_1 - v_m$. By looking at the action of the Singer cyclic group $S = \langle\sigma\rangle$ on W, we see that the exterior splash of $[\pi_1]$ on $[W]$ is the set $[J_1]$. By using he map τ_α defined above with $N(\alpha) = a$, we get the result. □

Remark 28. Let U be the $\mathbb{F}_{q^m}$-span of v_1 and v_2 in $\widehat{V}$. It is evident that the semilinear transformation θ maps the exterior splash of $[\gamma_a]$ on $[U]$ into the exterior splash of $[\pi_{a^{-1}}]$ on $[W]$.

The exterior splash of $[\gamma_a]$ on $[U]$ is

$$[\gamma_a] = \{[(1,x,0)] : x \in \mathbb{F}_{q^3}, N(x) = -a^2\}.$$

In [8], the splash of $[\gamma_a]$ was erroneusly given as the set $[Z_a]$. Note that, $[Z_a]$ never coincides with $[\gamma_a]$, unless $a = 1$.

References

[1] D. Augot, P. Loidreau, G. Robert, Rank metric and Gabidulin codes in characteristic zero, *Proceedings ISIT 2013*, 509–513.

[2] L. Bader, G. Lunardon, Some remarks on the Spin Module Representation of $\mathrm{Sp}_6(2^e)$, *Discrete Math.* **339** (2016), 1265–1273.

[3] R.H. Bruck, Construction problems of finite projective planes, in: Proc. Conf. on Combinatorics, University of North Carolina at Chapell Hill, April 10–14, 1967, University of North Carolina Press, Chapel Hill, 1969, pp. 426–514.

[4] R.H. Bruck, Circle geometry in higher dimensions. II. *Geometriae Dedicata* **2** (1973), 133–188.

[5] R.H. Bruck, The automorphism group of a circle geometry, *J. Combin. Theory Ser. A* **32** (1982), 256–263.

[6] L. Carliz, A Note on the Betti-Mathieu group, *Portugaliae mathematica* **22 (3)** (1963), 121–125.

[7] B.N. Cooperstein, External flats to varieties in $\mathrm{PG}(M_{n,n}\mathrm{GF}(q))$, *Linear Algebra Appl.* **267** (1997), 175–186.

[8] A. Cossidente, G. Marino, F. Pavese, Non-linear maximum rank distance codes, *Des. Codes Cryptogr.*, **79 (3)** (2016), 597–609.

[9] J. de la Cruz, M. Kiermaier, A. Wassermann, W. Willems, Algebraic structures of MRD Codes, *Adv. Math. Commun.* **10** (2016), 499–510.

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

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

[12] P. Dembowski, Finite Geometries. *Springer 1968.*

[13] G. Donati, N. Durante, Scattered linear sets generated by collineations between pencils of lines, *J. Algebraic Combin.* **40** (2014), 1121–1134.

[14] R.H. Dye, Spreads and classes of maximum subgroups of $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$ and $\mathrm{PSL}_n(q)$, *Ann. Mat. Pura Appl. (4)* **158** (1991), 33–50.

[15] G. Faina, G. Kiss, S. Marcugini, F. Pambianco, The cyclic model for $\mathrm{PG}(n, q)$ and a construction of arcs, *European J. Combin.* **23** (2002), 31–35.

[16] E.M. Gabidulin, Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii* **21** (1985), 3–16.

[17] E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, Ideals over a noncommutative ring and their application in cryptology, Advances in cryptology, EUROCRYPT '91, *Lecture Notes in Comput. Sci.* **547** (1991), 482–489.

[18] E.M. Gabidulin, A.V. Paramonov, O.V. Tretjakov, Rank errors and rank erasures correction, Proceedings of the 4th International Colloquium on Coding Theory, Dilijan, Armenia, Yerevan, 1992, pp. 11–19.

[19] J.W.P. Hirschfeld, Projective Geometries Over Finite Fields, 2nd edn, Clarendon Press, Oxford, 1998.

[20] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*, Oxford University Press, New York, 1991.

[21] A. Kshevetskiy and E. M. Gabidulin, The new construction of rank codes, Proc. IEEE Int. Symp. on Information Theory,pp. 2105–2108, Sept. 2005.

[22] R. Kötter, F. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inform. Theory* **54** (2008), 3579–3591.

[23] M. Lavrauw, J. Sheekey, C. Zanella, On embeddings of minimum dimension of $\mathrm{PG}(n,q) \otimes \mathrm{PG}(n,q)$, *Des. Codes Cryptogr.* **74** (2015), 427–440.

[24] M. Lavrauw, G. Van de Voorde, Scattered linear sets and pseudoreguli, *Electron. J. Combin.* **20**(1) (2013), #P15.

[25] M. Lavrauw, C. Zanella, Subgeometries and linear sets on a projective line, *Finite Fields Appl.* **34** (2015), 95–106.

[26] R. Lidl, H. Niederreiter, Finite fields. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

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

[28] G. Lunardon, R. Trombetti, Y. Zhou, Generalized twisted Gabidulin codes, preprint, arXiv:1507.07855.

[29] G. Marino, O. Polverino, R. Trombetti, Maximum scattered linear sets of pseudoregulus type and the Segre variety $\mathcal{S}_{n,n}$, *J. Algebraic Combin.* **39** (2014), no. 4, 807–831.

[30] T.G. Ostrom, Hyper-reguli, *J. Geom.* **48** (1993), 157–166.

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

[32] A. Ravagnani, Rank-metric codes and their duality theory, *Des. Codes Cryptogr.* **80** (2016), 197–216.

[33] S. Roman, Field theory. Graduate Texts in Mathematics, 158. Springer, New York, 2006.

[34] B. Segre, Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane, *Ann. Mat. Pura Appl.* **64** (1964), 1–76.

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

[36] D. Silva, F.R. Kschischang, Universal Secure Network Coding via Rank-Metric Codes, *IEEE Trans. Inform. Theory* **57** (2011), 1124–1135.

[37] D. Silva, F.R. Kschischang, R. Kötter, A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory* **54** (2008), 3951–3967.

[38] V. Tarokh, N. Seshadri, A.R. Calderbank, Space-time codes for high data rate wireless communication: performance criterion and code construction, *IEEE Trans. Inform. Theory 44 (1998)*, 744–765.

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