On a family of MRD codes with parameters $[n \times n, 2n, n-1]_q$, n even

Olga Polverino[1], Marco Timpanella[2], Giovanni Zini[3], and Ferdinando Zullo[1]

[1] Università degli Studi della Campania "Luigi Vanvitelli",
Dipartimento di Matematica e Fisica,
Viale Lincoln 5, 81100 Caserta, Italy
{olga.polverino,ferdinando.zullo}@unicampania.it
[2] Università degli Studi di Perugia,
Dipartimento di Matematica e Informatica,
Via Vanvitelli 1, 06123 Perugia, Italy
marco.timpanella@unipg.it
[3] Università degli Studi di Modena e Reggio Emilia,
Dipartimento di Scienze Fisiche, Informatiche e Matematiche,
Via Campi 213/b, 41125 Modena, Italy
giovanni.zini@unimore.it

Abstract. We consider a family $\mathcal{F}$ of $2n$-dimensional $\mathbb{F}_q$-linear rank metric codes in $\mathbb{F}_q^{n\times n}$ arising from the polynomial $x^{q^s}+\delta x^{q^{n/2+s}} \in \mathbb{F}_{q^n}[x]$, where n is even and $\gcd(n/2,s)=1$. We address the problem of characterizing those codes in $\mathcal{F}$ that are MRD, which has already been solved when $n \leq 6$. We give the solution whenever n is big enough with respect to s (e.g. $n \geq 10$ if $s=1$), and also when $n=8$ if q is odd and big enough. To this aim, we translate the problem into the study of some algebraic varieties with small degree with respect to $q^{n/2}$, and we apply techniques from algebraic geometry over finite fields. The results rely on the papers [8, 16].

Keywords: MRD code, linearized polynomial, algebraic variety

1 Introduction

Let $\mathbb{F}_q^{m\times n}$ be the set of $m \times n$ matrices over the finite field $\mathbb{F}_q$, endowed with the rank distance $d(A,B) := \operatorname{rank}(A-B)$. An $\mathbb{F}_q$-*linear rank metric code* $\mathcal{C}$ is a metric subspace of $\mathbb{F}_q^{m\times n}$, which is also a k-dimensional $\mathbb{F}_q$-subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^{m\times n}$. The elements of $\mathcal{C}$ are called codewords. The minimum distance d of $\mathcal{C}$ is the minimum distance between two distinct codewords, and coincides with the minimum rank of a non-zero codeword. The parameters of such a code $\mathcal{C}$ are denoted by $[m\times n, k, d]_q$, and satisfy the Singleton-like bound $k \leq \max\{m,n\}(\min\{m,n\}+1-d)$. If equality holds in this bound, then $\mathcal{C}$ is called *maximum rank distance*, MRD for short. The first nontrivial MRD codes were constructed by Delsarte [5] and later independently by Gabidulin [6], after

whom they are nowadays called Gabidulin codes; several other families have been constructed in recent years. MRD codes are of interest because of the optimality of their parameters, but also because of the connections they have with other mathematical objects. We refer to [7, 14] for a detailed introduction to rank metric codes.

We consider the square case $m = n$, for which we have a natural isomorphism of $\mathbb{F}_q$-algebras between $\mathbb{F}_q^{n\times n}$ and the $\mathbb{F}_q$-algebra $\mathcal{L}_{n,q}$ of $\mathbb{F}_q$-linear map over $\mathbb{F}_{q^n}$, whose elements can be identified (via the associated polynomial map) with $\mathbb{F}_q$-linearized polynomials $\sum_{i=0}^{n-1} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$ of degree smaller than q^n, with composition modulo $x^{q^n} - x$. Therefore we consider rank metric codes in $\mathcal{L}_{n,q}$, with the rank distance $d(f, g) = \mathrm{rank}(f, g)$. We focus on $\mathbb{F}_q$-linear $[n \times n, 2n, d]_q$ rank metric codes of the shape

$$\mathcal{C}_f := \langle x, f(x)\rangle_{\mathbb{F}_{q^n}} = \{ax + bf(x)\colon a, b \in \mathbb{F}_{q^n}\}, \tag{1}$$

for some $f(x) \in \mathcal{L}_{n,q}$. Notice that, if $\mathcal{C}$ is an $\mathbb{F}_q$-linear $[n \times n, 2n, n-1]_q$ MRD code such that $L(\mathcal{C}) := \{g \in \mathcal{L}_{n,q}\colon g \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}$ has maximum order q^n, then up to a suitable equivalence $\mathcal{C} = \mathcal{C}_f$ for some $f \in \mathcal{L}_{n,q}$; see [11]. Indeed, many families of linear MRD codes known in the literature are of the shape $\mathcal{C}_f$.

Notice that $\mathcal{C}_f$ is MRD if and only if the kernel of g has $\mathbb{F}_q$-dimension at most 1 for all non-zero $g \in \mathcal{C}_f$, and this is equivalent to require that

$$\frac{f(x_0)}{x_0} = \frac{f(y_0)}{y_0} \implies \frac{y_0}{x_0} \in \mathbb{F}_q$$

for all $x_0, y_0 \in \mathbb{F}_{q^n}^*$, that is, $f(x)$ is *scattered*; see [13].

In the paper [9], rank metric codes $\mathcal{C}_{\delta,s} := \mathcal{C}_{f_{\delta,s}}$ as in (1) were investigated when n is an even positive integer and

$$f_{\delta,s}(x) := x^{q^s} + \delta x^{q^{\frac{n}{2}+s}} \in \mathcal{L}_{n,q},$$

where $\delta \in \mathbb{F}_{q^n} \setminus \{0\}$, $0 < s < n$ and $\gcd(s, n/2) = 1$. The goal was to provide codes $\mathcal{C}_{\delta,s}$ that are MRD. To this aim, the following is known.

- If $\delta^{1+q^{n/2}} = \tilde{\delta}^{1+q^{n/2}}$, then $\mathcal{C}_{\delta,s}$ is MRD if and only if $\mathcal{C}_{\tilde{\delta},s}$ is MRD; see [9, Section 5].
- If $\delta^{1+q^{n/2}} = 1$, then $\mathcal{C}_{\delta,s}$ is not MRD; see [9, Section 4].
- If $\delta^{1+q^{n/2}} \neq 1$, then $\dim_{\mathbb{F}_q} \ker(f) \leq 2$ for all non-zero $f \in \mathcal{C}_{\delta,s}$; see [9, Proposition 4.1].
- If $n = 2$, then $\mathcal{C}_{\delta,s} = \mathbb{F}_q^{2\times 2}$ is MRD.
- If $n = 4$, then $\mathcal{C}_{\delta,s}$ is MRD if and only if $\delta^{1+q+q^2+q^3} \neq 1$; see [13].
- If $n = 6$, then $\mathcal{C}_{\delta,s}$ is MRD for exactly $\lceil (q^2+q+1)(q-2) \rceil$ values of δ^{1+q^3}, which are characterized; see [1] and also [12, Theorem 7.3].
- If $n = 8$, q is odd and $\delta^{1+q^4} = -1$, then $\mathcal{C}_{\delta,s}$ is MRD; see [9, Theorem 7.2].

We prove the following result concerning the open cases.

Theorem 1. *Let $n \geq 8$.*

(i) [8, Theorem 4.5] *If*

$$n \geq \begin{cases} 8s+4 & \text{if } q=3 \text{ and } s>1, \text{ or } q=2 \text{ and } s>2, \\ 8s+2 & \text{otherwise,} \end{cases}$$

then $\mathcal{C}_{\delta,s}$ is not MRD.

(ii) [16, Theorem 1.1] *If $n=8$, q is odd and $q \geq 1039891$, then $\mathcal{C}_{\delta,s}$ is MRD if and only if $\delta^{1+q^4} = -1$.*

Notice that for $s=1$, if q is odd and big enough, then Theorem 1 completes the characterization of MRD codes $\mathcal{C}_{\delta,s}$ for any n.

The proof is based on the investigation of rational points of certain algebraic varieties over finite fields; we refer to [10] and [15] for the preliminaries on this topic. A key tool is the Hasse-Weil lower bound

$$N_\ell \geq \ell + 1 - 2g\sqrt{\ell} \tag{2}$$

on the number N_ℓ of rational places of an absolutely irreducible curve of genus g defined over $\mathbb{F}_\ell$; see [15, Theorem 5.2.3]. An approach that has been used in the literature (see e.g. [2]) relies on the application of the Hasse-Weil lower bound to an $\mathbb{F}_{q^n}$ absolutely irreducible component of the curve $\mathcal{Z}_f$ with affine equation $\frac{f(X)Y - f(Y)X}{X^qY - XY^q} = 0$. This approach may be useful when the degree of $f(x)$, and hence the genus of $\mathcal{Z}_f$, is small enough with the order q^n of the field, but this is not the case for the polynomials $f_{\delta,s}$.

Therefore, we translate the property for $\mathcal{C}_{\delta,s}$ of being MRD into the investigation of another suitable algebraic curve which turns out to be absolutely irreducible, and whose genus is small enough to get the desired result when $n \geq 10$. In order to deal with the case $n=8$ when q is odd, we move from this curve to the investigation of a higher-dimensional $\mathbb{F}_q$-rational variety, whose degree equals 16. For large q, this degree is small enough to apply a Lang-Weil (Hasse-Weil-type) lower bound on the number of rational points and conclude the proof.

2 An auxiliary algebraic curve

Let $n \geq 8$ be even, $\gcd(s, n/2) = 1$ and $f_{\delta,s} = x^{q^s} + \delta x^{q^{\frac{n}{2}+s}} \in \mathcal{L}_{n,q}$ with $\delta \neq 0$. For any finite field extension $\mathbb{F}_{\ell^m}/\mathbb{F}_\ell$, denote by $\mathrm{N}_{\ell^m/\ell} : \mathbb{F}_{\ell^m} \to \mathbb{F}_\ell$ the norm function $x \mapsto x^{1+\ell+\cdots+\ell^{m-1}}$; in particular, $\mathrm{N}_{q^n/q^{n/2}}(x) = x^{1+q^{n/2}}$.

Lemma 1. *$\mathcal{C}_{\delta,s}$ is MRD if and only if*

$$\mathrm{N}_{q^n/q^{n/2}}(\delta) \neq \mathrm{N}_{q^n/q^{n/2}}\left(\frac{\xi^{q^{s+n/2}} - \xi^{q^{n/2}}}{\xi^{q^{n/2}} - \xi^{q^s}}\right) \tag{3}$$

for all $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^{n/2}}$.

Proof. The code $\mathcal{C}_{\delta,s}$ is not MRD if and only if there exist $x_0, y_0 \in \mathbb{F}_{q^n}^*$ such that $y_0/x_0 \notin \mathbb{F}_q$ and $(x_0^{q^s} + \delta x_0^{q^{n/2+s}})/x_0 = (y_0^{q^s} + \delta y_0^{q^{n/2+s}})/y_0$, that is $\delta(y_0 x_0^{q^{n/2+s}} - x_0 y_0^{q^{n/2+s}}) = x_0 y_0^{q^s} - y_0 x_0^{q^s}$. The coefficient $y_0 x_0^{q^{n/2+s}} - x_0 y_0^{q^{n/2+s}}$ of δ is not zero, otherwise it follows that $y_0/x_0 \in \mathbb{F}_{q^n} \cap \mathbb{F}_{q^{n/2+s}} = \mathbb{F}_q$, a contradiction. Then, writing $\eta := y_0/x_0, \xi := \eta^{q^n} \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$, one gets

$$\delta = \frac{1}{x_0^{q^{n/2+s}-q^s}} \cdot \frac{\xi^{q^{s+n/2}} - \xi^{q^{n/2}}}{\xi^{q^{n/2}} - \xi^{q^s}}.$$

Since $(1/x_0^{q^{n/2+s}-q^s})^{1+q^{n/2}} = 1$, $\mathcal{C}_{\delta,s}$ is MRD if and only if (3) holds for all $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q$. It is easily seen that $\xi \in \mathbb{F}_{q^n}$ satisfies $\frac{\xi^{q^{s+n/2}} - \xi^{q^{n/2}}}{\xi^{q^{n/2}} - \xi^{q^s}} = -1$ if and only if $\xi \in \mathbb{F}_{q^{n/2}}$, and $\mathcal{C}_{\delta,s}$ is not MRD when $\mathrm{N}_{q^n/q^{n/2}}(\delta) = \mathrm{N}_{q^n/q^{n/2}}(-1) = 1$. The claim of the lemma follows.

We have therefore proved that, if $\alpha \in \mathbb{F}_{q^{n/2}} \setminus \{0,1\}$ satisfies $\mathrm{N}_{q^n/q^{n/2}}(\delta) = \alpha$ and $\mathrm{N}_{q^n/q^{n/2}}\left(\frac{\xi^{q^{s+n/2}} - \xi^{q^{n/2}}}{\xi^{q^{n/2}} - \xi^{q^s}}\right) = \alpha$ for some $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^{n/2}}$, then $\mathcal{C}_{\delta,s}$ is not MRD.

If $T, S, A, B \in \mathbb{F}_{q^{n/2}}$ are such that $\mathrm{N}_{q^n/q^{n/2}}(\xi) = -T$, $\mathrm{Tr}_{q^n/q^{n/2}}(\xi) := \xi + \xi^{q^{n/2}} = S$, and $\xi^{q^s} = A + B\xi$, then Lemma 1 yields the following result.

Proposition 1. [8, Theorem 3.6] *Let $\delta \in \mathbb{F}_{q^n}$ satisfy $\mathrm{N}_{q^n/q^{n/2}}(\delta) = \alpha \in \mathbb{F}_{q^{n/2}} \setminus \{0,1\}$. Then $\mathcal{C}_{\delta,s}$ is MRD if and only if there exist $T, S, A, B \in \mathbb{F}_{q^{n/2}}$ such that*

1. $(1-\alpha)(T + T^{q^s})\alpha S^{q^s-1} + (1+\alpha)(AS - 2BT) = 0$,
2. $x^2 - Sx - T \in \mathbb{F}_{q^{n/2}}[x]$ *is irreducible over* $\mathbb{F}_{q^{n/2}}$,
3. $S^{q^s} = 2A + BS$,
4. $-T^{q^s} = A^2 + B(AS - BT)$.

The conditions in Proposition 1 can be made more explicit by considering separately the cases q odd and q even. For q odd, Condition 2. is equivalent to $S^2 + 4T = \eta Z^2$ for some $\eta, Z \in \mathbb{F}_{q^{n/2}}^*$ with η a non-square in $\mathbb{F}_{q^{n/2}}$. For q even, Condition 2. is equivalent to $S \neq 0$ and $\mathrm{Tr}_{q^{n/2}/2}(T/S^2) = 1$, where $\mathrm{Tr}_{q^{n/2}/2}$ is the absolute trace on $\mathbb{F}_{q^{n/2}}$. After some computation, the following characterization is obtained from Proposition 1.

Corollary 1. (see [8, Section 3.1] for q odd, [8, Section 3.2] for q even)

– *Let q be odd, and suppose that $\alpha := \mathrm{N}_{q^n/q^{n/2}}(\delta) \notin \{0,1\}$. Fix $\mu \in \{1,-1\}$ and define $\beta := \mu\frac{\alpha+1}{1-\alpha} \in \mathbb{F}_{q^{n/2}} \setminus \{1,-1\}$. Then $\mathcal{C}_{\delta,s}$ is MRD if and only if, for any non-square η of $\mathbb{F}_{q^{n/2}}$, there exist no $S, T, Z \in \mathbb{F}_{q^{n/2}}$ such that $Z \neq 0$ and*

$$\begin{cases} T = \frac{\eta Z^2 - S^2}{4}, \\ -(S^{q^s} - S)^2 + \eta Z^2 + \eta^{q^s} Z^{2q^s} - 2\beta\eta^{\frac{q^s+1}{2}} Z^{q^s+1} = 0. \end{cases} \tag{4}$$

– *Let q be even, and suppose that $\alpha := \mathrm{N}_{q^n/q^{n/2}}(\delta) \notin \{0,1\}$. Define $\beta := \frac{\alpha}{1+\alpha} \in \mathbb{F}_{q^{n/2}} \setminus \{0,1\}$. Then $\mathcal{C}_{\delta,s}$ is MRD if and only if, for any $\epsilon \in \mathbb{F}_{q^{n/2}}$ with $\mathrm{Tr}_{q^{n/2}/2}(\epsilon) = 1$, there exist no $S,T,Y,Z \in \mathbb{F}_{q^{n/2}}$ such that $S \neq 0$ and*

$$\begin{cases} T = S^2(Z^2 + Z + \epsilon), \\ Z^2 + Z + \epsilon = Y, \\ (S^{2(q^s-1)}Y^{q^s} + S^{q^s-1}(\beta + \mathrm{Tr}_{q^s/2}(Y)) + Y)\cdot \\ \qquad (S^{2(q^s-1)}Y^{q^s} + S^{q^s-1}(1 + \beta + \mathrm{Tr}_{q^s/2}(Y)) + Y) = 0. \end{cases} \tag{5}$$

Equations (4) and (5) define affine models of $\mathbb{F}_{q^{n/2}}$-rational algebraic curves, so that the characterization can be stated as follows.

– For q odd: $\mathcal{C}_{\delta,s}$ is MRD if and only if, for any non-square η of $\mathbb{F}_{q^{n/2}}$, the curve $\mathcal{X}_{\delta,s}$ in (4) has no affine $\mathbb{F}_{q^{n/2}}$-rational points $(\bar{s},\bar{t},\bar{z})$ with $\bar{z} \neq 0$.
– For q even: $\mathcal{C}_{\delta,s}$ is MRD if and only if, for any $\epsilon \in \mathbb{F}_{q^{n/2}}$ with $\mathrm{Tr}_{q^{n/2}/2}(\epsilon) = 1$, the curve in (5) has no affine $\mathbb{F}_{q^{n/2}}$-rational points $(\bar{s},\bar{t},\bar{y},\bar{z})$ with $\bar{s} \neq 0$.

For q odd, we study $\mathcal{X}_{\delta,s}$ by means of tools from function field theory; in particular, we show that $\mathcal{X}_{\delta,s}$ is a generalized Artin-Schreier cover of degree q^s of a quadratic Kummer cover of the projective line in Z.

For q even, we consider the following component of the curve in (5):

$$\mathcal{Y}_{\delta,s} : \begin{cases} T = S^2(Z^2 + Z + \epsilon), \\ Z^2 + Z + \epsilon = Y, \\ S^{2(q^s-1)}Y^{q^s} + S^{q^s-1}(\beta + \mathrm{Tr}_{q^s/2}(Y)) + Y = 0. \end{cases}$$

Also for the study of $\mathcal{Y}_{\delta,s}$ we apply tools from function field theory. The following result is obtained.

Theorem 2. [8, Theorems 3.7 and 3.12]

– *The curves $\mathcal{X}_{\delta,s}$ and $\mathcal{Y}_{\delta,s}$ are absolutely irreducible, and both of them have genus $q^{2s} - q^s - 1$.*
– *The number of rational places of $\mathcal{X}_{\delta,s}$ which are not centered at an affine $\mathbb{F}_{q^{n/2}}$-rational point $(\bar{s},\bar{t},\bar{z})$ with $\bar{t} \neq 0$ is at most 4.*
– *The number of rational places of $\mathcal{Y}_{\delta,s}$ which are not centered at an affine $\mathbb{F}_{q^{n/2}}$-rational point $(\bar{s},\bar{t},\bar{y},\bar{z})$ with $\bar{s} \neq 0$ is at most $2q^s + 2$.*

Once that the absolutely irreducibility of $\mathcal{X}_{\delta,s}, \mathcal{Y}_{\delta,s}$ has been proved and the number of their "bad" rational places has been upper bounded, we can apply Hasse-Weil lower bound (2) on their number N of rational places over $\mathbb{F}_{q^{n/2}}$. For n big enough, i.e. under the conditions in Theorem 1 *(i)*, Hasse-Weil bound implies that N is positive and the curves $\mathcal{X}_{\delta,s}$ and $\mathcal{Y}_{\delta,s}$ have "good" rational places, that is, places centered at an affine $\mathbb{F}_{q^{n/2}}$-rational point P such that we have we have $P = (\bar{s},\bar{t},\bar{z})$ with $\bar{z} \neq 0$ for q odd, and $P = (\bar{s},\bar{t},\bar{y},\bar{z})$ with $\bar{s} \neq 0$ for q even. Therefore, Theorem 1 *(i)* is proved.

3 An auxiliary higher-dimensional algebraic variety

Let $n = 8$. For $q \leq 11$, it was shown computationally in [9, Remark 7.4] that: for q odd, $\mathcal{C}_{\delta,s}$ is MRD if and only if $\mathrm{N}_{q^8/q^4}(\delta) = -1$; for q even, $\mathcal{C}_{\delta,s}$ is never MRD. We look at higher values of q, and notice that the Hasse-Weil lower bound $q^4 + 1 - 2(q^{2s} - q^s - 1)q^2 < 0$ applied to $\mathcal{X}_{\delta,s}$ and $\mathcal{Y}_{\delta,s}$ does not guarantee a positive number of suitable $\mathbb{F}_{q^4}$-rational points. We restrict to the case q odd and start from the case $s = 1$.

Let ξ be a normal element of $\mathbb{F}_{q^4}$ over $\mathbb{F}_q$, so that $\mathcal{B} = \{\xi, \xi^q, \xi^{q^2}, \xi^{q^3}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^4}$ over $\mathbb{F}_q$. Write two elements $S, Z \in \mathbb{F}_{q^4}$ as

$$S = S_0\xi + S_1\xi^q + S_2\xi^{q^2} + S_3\xi^{q^3}, \quad Z = Z_0\xi + Z_1\xi^q + Z_2\xi^{q^2} + Z_3\xi^{q^3}, \tag{6}$$

with $S_i, Z_i \in \mathbb{F}_q$. Now replace (6) in the equation

$$-(S^q - S)^2 + \eta Z^2 + \eta^q Z^{2q} - 2\beta\eta^{\frac{q+1}{2}} Z^{q+1} = 0 \tag{7}$$

of $\mathcal{X}_{\delta,1}$ and write it as an $\mathbb{F}_q$-linear combination

$$F_0\xi + F_1\xi^q + F_2\xi^{q^2} + F_3\xi^{q^3} = 0.$$

Since the left-hand side of (7) is a quadratic form over $\mathbb{F}_q$ in S, Z, the coefficients F_i are homogeneous quadratic polynomials over $\mathbb{F}_q$ in the S_i, Z_i's. Therefore,

$$\mathcal{V}_\delta\colon \begin{cases} F_0(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0 \\ F_1(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0 \\ F_2(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0 \\ F_3(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0 \end{cases}$$

is an $\mathbb{F}_q$-rational projective algebraic variety in the 7-dimensional projective space $\mathbb{P}^7$, obtained as the intersection of four quadrics. Since $\mathcal{B}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^4}$, there is a one-to-one correspondece between the affine $\mathbb{F}_{q^4}$-rational points of $\mathcal{X}_{\delta,1}$ different from $(0, 0, 0)$, and the $\mathbb{F}_q$-rational points of $\mathcal{V}_\delta$.

Our goal is then to show that $\mathcal{V}_\delta$ has an $\mathbb{F}_q$-rational point whose S_i-coordinates are not all zero. To this aim, it is enough to show that $\mathcal{V}_\delta$ has an absolutely irreducible component defined over $\mathbb{F}_q$ whose degree is small enough with respect to q, and then to apply the following Lang-Weil lower bound, which is the analogous of the Hasse-Weil bound for higher-dimensional varieties.

Theorem 3. (Lang-Weil lower bound, see [3, Theorem 7.1]) *Let $\mathcal{V} \subseteq \mathbb{P}^N$ be an absolutely irreducible variety defined over $\mathbb{F}_q$, of dimension m and degree d. If $q > 2(m+1)d^2$, then the number A_q of affine $\mathbb{F}_q$-rational points of $\mathcal{V}$ satisfies*

$$A_q \geq q^m - (d-1)(d-2)q^{m-\frac{1}{2}} - 5d^{\frac{13}{3}}q^{m-1}.$$

We will show that either $\mathcal{V}_\delta$ is absolutely irreducible, or has only one absolutely irreducible component of given dimension and degree. In both cases we then

obtain an absolutely irreducible component defined over $\mathbb{F}_q$: this follows from the fact that the q-Frobenius map $(S_0, \ldots, Z_3) \mapsto (S_0^q, \ldots, Z_3^q)$ fixes globally each $\mathbb{F}_q$-rational absolutely irreducible component of $\mathcal{V}_\delta$, and preserves dimension and degree of the components.

In order to investigate the components of $\mathcal{V}_\delta$ we consider another variety $\mathcal{W}_\delta$ which is easier to handle and $\mathbb{F}_{q^4}$-projectively equivalent to $\mathcal{V}_\delta$. Indeed, projective equivalence preserves both the dimension and the degree of an absolutely irreducible component.

Consider the Moore matrix

$$M = \begin{pmatrix} \xi & \xi^q & \xi^{q^2} & \xi^{q^3} \\ \xi^q & \xi^{q^2} & \xi^{q^3} & \xi \\ \xi^{q^2} & \xi^{q^3} & \xi & \xi^q \\ \xi^{q^3} & \xi & \xi^q & \xi^{q^2} \end{pmatrix},$$

which has non-zero determinant because $\mathcal{B}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^4}$. Then

$$\varphi\colon (S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) \mapsto (S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) \cdot \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}$$

is an $\mathbb{F}_{q^4}$-rational invertible projectivity of $\mathbb{P}^7$. Let $(X_0, X_1, X_2, X_3, Y_0, Y_1, Y_2, Y_3) = \varphi(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3)$. Whenever the coordinates S_i, Z_i of a point $P \in \mathbb{P}^7$ are in $\mathbb{F}_q$ and S, Z are defined as in (6), the coordinates X_i, Y_i of $\varphi(P)$ satisfy $X_i = S^{q^i}$ and $Y_i = Z^{q^i}$. Thus, the equations defining the image $\mathcal{W}_\delta$ of $\mathcal{V}_\delta$ under φ are obtained by applying the q^j-power to Equation (7), $j = 0, \ldots, 3$, and replacing S^{q^i}, Z^{q^i} with X_i, Y_i. One gets

$$\mathcal{W}_\delta : \begin{cases} (X_1 - X_0)^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta \eta^{\frac{q+1}{2}} Y_0 Y_1, \\ (X_2 - X_1)^2 = \eta^q Y_1^2 + \eta^{q^2} Y_2^2 - 2\beta^q \eta^{\frac{q^2+q}{2}} Y_1 Y_2, \\ (X_3 - X_2)^2 = \eta^{q^2} Y_2^2 + \eta^{q^3} Y_3^2 - 2\beta^{q^2} \eta^{\frac{q^3+q^2}{2}} Y_2 Y_3, \\ (X_0 - X_3)^2 = \eta^{q^3} Y_3^2 + \eta Y_0^2 - 2\beta^{q^3} \eta^{\frac{1+q^3}{2}} Y_3 Y_0. \end{cases}$$

As shown in [16, Lemma 3.1], $\mathcal{W}_\delta$ has dimension 3 and degree 16. About the absolutely irreducible components the following can be proved.

- Suppose $\beta^{2q} - \beta^2 \neq 0$. Then, for some non-square η of $\mathbb{F}_{q^4}$, there exists a hyperplane Π of $\mathbb{P}^7$ such that $\mathcal{W}_\delta$ is not contained in $\mathbb{P}$ and $\mathcal{W}_\delta \cap \Pi$ is an absolutely irreducible surface; see [16, Lemma 3.2]. This implies that $\mathcal{W}_\delta$ has a unique absolutely irreducible component $\mathcal{U}$ of maximal dimension 3, and $\mathcal{U}$ has degree 16; see [16, Proposition 3.3].
- Suppose $\beta^{2q} - \beta^2 = 0$ with $\beta \neq \pm 1$, and suppose also $\beta \neq 0$. Then $\mathcal{W}_\delta$ has exactly three absolutely irreducible components $\mathcal{W}_1$, $\mathcal{W}_2$ and $\mathcal{U}$ of maximal dimension 3, whose degree is respectively 4, 4 and 8; see [16, Lemma 3.4] and [16, Section 5] for an explicit description of the three components.

Among the absolutely irreducible components of $\mathcal{V}_\delta$, consider the component $\varphi^{-1}(\mathcal{U})$, which has the same degree and dimension of $\mathcal{U}$. As explained above, $\varphi(\mathcal{U})$ is defined over $\mathbb{F}_q$, and we can apply Theorem 3 to it. When $q \geq 1039891$, this guarantees the existence of an $\mathbb{F}_q$-rational point of $\mathcal{V}_\delta$ with the S_i-coordinates not all zero; see [16, Theorem 3.5]. This shows that $\mathcal{C}_{\delta,1}$ is not MRD whenever $\beta \neq 0$, that is, whenever $\delta \in \mathbb{F}_{q^8}^*$ satisfies $\mathrm{N}_{q^8/q^4}(\delta) \neq -1$; see [16, Proposition 3.6]. We have then proved Theorem 1 for $s = 1$.

3.1 The other values of s

For $n = 8$ and $q \geq 1039891$ odd, we still have to consider the cases $s = 3$, $s = 5$ and $s = 7$ in Theorem 1.

We make use of an equivalence result from [9]. Two codes $\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ are said to be equivalent if $\mathcal{C}' = \{f_1 \circ f^\rho \circ f_2 \colon f \in \mathcal{C} \circ\}$ for some invertible polynomials $f_1, f_2 \in \mathcal{L}_{n,q}$ and field automorphism $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$. Code equivalence preserves the parameters, and in particular preserves the property of being MRD.

Given a rank metric code of the shape $\mathcal{C}_f \subseteq \mathcal{L}_{n,q}$, define the $\mathbb{F}_q$-linear space

$$U_f := \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}.$$

Proposition 2. [13, Theorem 8] *Let $\mathcal{C}_f, \mathcal{C}_g \subseteq \mathcal{L}_{n,q}$ be MRD codes. Then $\mathcal{C}_f$ and $\mathcal{C}_g$ are equivalent if and only if U_f and U_g are $\Gamma L(2, q^n)$-equivalent.*

Proposition 3. [9, Proposition 5.1] *With the same notation as above, let $\delta, \tilde{\delta} \in \mathbb{F}_{q^n}^*$ be such that $\mathrm{N}_{q^n/q^{n/2}}(\delta) \neq 1$ and $\mathrm{N}_{q^n/q^{n/2}}(\tilde{\delta}) \neq 1$, and let $s, \tilde{s} \in \{1, \ldots, n/2-1\}$ be such that $\gcd(n/2, s) = \gcd(n/2, \tilde{s}) = 1$. Then $U_{f_{\delta,s}}$ and $U_{f_{\tilde{\delta},\tilde{s}}}$ are $\Gamma\mathrm{L}(2, q^n)$-equivalent if and only if one of the following cases occurs for some automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^{n/2}})$:*

- *$\tilde{s} = s$ and $\mathrm{N}_{q^n/q^{n/2}}(\tilde{\delta}) = \mathrm{N}_{q^n/q^{n/2}}(\delta)^\sigma$;*
- *$\tilde{s} = n/2 - s$ and $\mathrm{N}_{q^n/q^{n/2}}(\tilde{\delta}) = 1/\mathrm{N}_{q^n/q^{n/2}}(\delta)^\sigma$.*

By Propositions 2 and 3, $\mathcal{C}_{\delta,3}$ is equivalent to $\mathcal{C}_{\tilde{\delta},1}$ for some $\tilde{\delta} \in \mathbb{F}_{q^8}$ such that $\mathrm{N}_{q^8/q^4}(\tilde{\delta}) = -1$ if and only if $\mathrm{N}_{q^8/q^4}(\delta) = -1$. Therefore Theorem 1 holds for $s = 3$.

For $s = 5$ we have $f_{\delta,5}(x) = \delta f_{1/\delta,1}(x)$ and hence $\mathcal{C}_{\delta,5} = \mathcal{C}_{1/\delta,1}$, while for $s = 7$ we have $f_{\delta,7}(x) = \delta f_{1/\delta,3}(x)$ and hence $\mathcal{C}_{\delta,7} = \mathcal{C}_{1/\delta,3}$. Since $\mathrm{N}_{q^8/q^4}(\delta) = -1$ if and only if $\mathrm{N}_{q^8/q^4}(1/\delta) = -1$, it follows that Theorem 1 holds also for $s = 5$ and $s = 7$.

References

1. D. Bartoli, B. Csajbók and M. Montanucci: On a conjecture about maximum scattered subspaces in $\mathbb{F}_{q^6} \times \mathbb{F}_{q^6}$, *Linear Algebra Appl.* **631** (2021), 111–135.
2. D. Bartoli and Y. Zhou: Exceptional scattered polynomials, *J. Algebra* **509** (2018), 507–534.

3. A. Cafure and G. Matera: Improved explicit estimates on the number of solutions of equations over a finite field, *Finite Fields Appl.* **12** (2006), 155–185.
4. B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in PG$(1, q^n)$, *J. Combin. Theory Ser. A* **157** (2018), 402–426.
5. P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory Ser. A* **25** (1978), 226–241.
6. E. M. Gabidulin: Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii* **21 (1)** (1985), 3–16.
7. E. Gorla and A. Ravagnani: Codes endowed with the rank metric, *Network coding and subspace designs*, 3–23, Signals Commun. Technol., Springer, Cham (2018).
8. O. Polverino, G. Zini and F. Zullo: On certain linearized polynomials with high degree and kernel of small dimension, *J. Pure Appl. Algebra* **225 (2)** (2021), 106491.
9. B. Csajbók, G. Marino, O. Polverino and C. Zanella: A new family of MRD-codes, *Linear Algebra Appl.* **548** (2018), 203–220.
10. J.W.P. Hirschfeld, G. Korchmáros and F. Torres: *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton (2008).
11. G. Lunardon, R. Trombetti and Y. Zhou: On kernels and nuclei of rank metric codes, *J. Algebraic Combin.* **46 (2)** (2017), 313–340.
12. O. Polverino and F. Zullo: On the number of roots of some linearized polynomials, *Linear Algebra Appl.* **601** (2020), 189–218.
13. J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* **10 (3)** (2016), 475–488.
14. J. Sheekey: MRD codes: constructions and connections, *Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications*, Radon Series on Computational and Applied Mathematics **23** (2019).
15. H. Stichtenoth: *Algebraic Function Fields and Codes*, 2nd edition, Graduate Texts in Mathematics, vol 254, Springer, Berlin (2009).
16. M. Timpanella and G. Zini: On a family of linear MRD codes with parameters $[8 \times 8, 16, 7]_q$. Submitted. ArXiv:210813082.