ON A FAMILY OF LINEAR MRD CODES WITH PARAMETERS $[8 \times 8, 16, 7]_q$

MARCO TIMPANELLA AND GIOVANNI ZINI

ABSTRACT. In this paper 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 polynomials of the form $x^{q^s} + \delta x^{q^{\frac{n}{2}+s}} \in \mathbb{F}_{q^n}[x]$. The family $\mathcal{F}$ was introduced by Csajbók, Marino, Polverino and Zanella (2018) as a potential source for maximum rank distance (MRD) codes. Indeed, they showed that $\mathcal{F}$ contains MRD codes for $n = 8$, and other subsequent partial results have been provided in the literature towards the classification of MRD codes in $\mathcal{F}$ for any n. In particular, the classification has been reached when n is smaller than 8, and also for n greater than 8 provided that s is small enough with respect to n. In this paper we deal with the open case $n = 8$, providing a classification for any large enough odd prime power q. The techniques are from algebraic geometry over finite fields, since our strategy requires the analysis of certain 3-dimensional $\mathbb{F}_q$-rational algebraic varieties in a 7-dimensional projective space. We also show that the MRD codes in $\mathcal{F}$ are not equivalent to any other MRD codes known so far.

1. INTRODUCTION

Rank metric codes over finite fields were introduced by Delsarte in its seminal paper [7] in 1978, and increasingly studied since then. The interest is mainly boosted by their applications in information theory, such as crisscross error correction [21], code-based cryptography [9] and linear network coding [25], but also by the connections with other mathematical objects, such as semifields [23] and linear sets [27].

An $\mathbb{F}_q$-*linear rank metric code* $\mathcal{C}$ is an $\mathbb{F}_q$-vector subspace of the space $\mathbb{F}_q^{m \times n}$ of $m \times n$ matrices over the finite field $\mathbb{F}_q$, equipped with the rank distance $d(A, B) := \operatorname{rank}(A - B)$. We denote the main parameters of $\mathcal{C}$ by $[m \times n, k, d]_q$, where k is the $\mathbb{F}_q$-dimension of $\mathcal{C}$ and d is the minimum distance of $\mathcal{C}$, i.e. the minimum rank distance between two distinct elements of $\mathcal{C}$. The Singleton-like bound $k \leq \max\{m, n\}(\min\{m, n\} - d + 1)$ holds; see [7]. When equality holds, $\mathcal{C}$ is called *maximum rank distance* (MRD for short). Codes of this sort have particular interest because of the optimality of their parameters. The first examples of MRD codes were constructed by Delsarte [7] and independently by Gabidulin [8], and are known as *Gabidulin codes*.

We are interested in the square case $m = n$. In this case, we can identify $\mathbb{F}_q^{n \times n}$ with the $\mathbb{F}_q$-algebra $\mathcal{L}_{n,q}$ of q-polynomials over $\mathbb{F}_{q^n}$ of degree smaller than q^n, with composition modulo $x^{q^n} - x$; see [19]. Thus, $\mathbb{F}_q$-linear $[n \times n, k, d]_q$ rank metric codes $\mathcal{C}$ can be seen as k-dimensional $\mathbb{F}_q$-vector subspaces of $\mathcal{L}_{n,q}$ with minimum rank distance d. If in addition $\mathcal{C}$ is an $\mathbb{F}_{q^n}$-vector subspace of $\mathcal{L}_{n,q}$, we say that $\mathcal{C}$ is $\mathbb{F}_{q^n}$-linear.

Most of the known families of $\mathbb{F}_q$-linear MRD codes are indeed $[n \times n, 2n, d]_q$ $\mathbb{F}_{q^n}$-linear codes $\mathcal{C}_f$ for some q-polynomial $f(x) \in \mathcal{L}_{n,q}$, where

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

see e.g. [17] and the references therein. Such codes are strictly connected with so-called linear sets of the projective line $\mathrm{PG}(1, q^n)$ over $\mathbb{F}_{q^n}$. When $\mathcal{C}_f$ is MRD, the polynomial $f(x)$ is said to be *scattered* and defines a *scattered linear set* in $\mathrm{PG}(1, q^n)$; see [19].

Csajbók et al. [4] introduced for n even the family of rank metric codes $\mathcal{C}_{\delta,s} := \mathcal{C}_{f_{\delta,s}}$ with

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

where $\delta \in \mathbb{F}_{q^n}$, $\delta \neq 0$, and $s \in \{1, \ldots, n-1\}$ is coprime with $n/2$. Whenever $\delta^{1+q^{n/2}} \neq 1$, the minimum distance of $\mathcal{C}_{\delta,s}$ is large: either $d = n-1$, i.e. $\mathcal{C}_{\delta,s}$ is MRD; or $d = n-2$, i.e. $\mathcal{C}_{\delta,s}$ is as close as possible to being MRD. In the latter case $\mathcal{C}_{\delta,s}$ is called Almost MRD, in analogy with Almost MDS codes in the Hamming metric; see [6, Definition 3.1].

Several papers have provided partial results towards the classification of MRD codes of type $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{n,q}$. A sufficient condition was given in the same paper [4] when $n = 8$ and q is odd: if $\delta^{1+q^4} = -1$, then $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$ is MRD. For smaller values of n, a characterization of MRD codes $\mathcal{C}_{\delta,s}$ is known; the case $n = 6$ has been dealt with in [2] and [20]. For higher values of n, a characterization of MRD codes $\mathcal{C}_{\delta,s}$ has been obtained in [18] when n is large enough, namely when

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

For instance, this rules out any $n \geq 10$ when $s = 1$.

In this paper, we focus on the open case $n = 8$. Our main result is the characterization of the MRD codes of type $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$ under the assumption that q is odd and large enough. We also show that such MRD codes are not equivalent to any other known ones. Our results are summarized as follows (the notions of equivalence and idealisers will be given in Section 2).

Theorem 1.1. *Let* $q \geq 1039891$ *be odd,* $\delta \in \mathbb{F}_{q^8}^*$, $s \in \{1, 3, 5, 7\}$, *and* $f_{\delta,s} = x^{q^s} + \delta x^{q^{4+s}} \in \mathcal{L}_{8,q}$. *Then*

$$\mathcal{C}_{\delta,s} = \langle x, \, f_{\delta,s}(x) \rangle_{\mathbb{F}_{q^8}} \subseteq \mathcal{L}_{8,q}$$

is MRD if and only if $\delta^{1+q^4} = -1$.

The $[8 \times 8, 16, 7]_q$ *MRD codes* $\mathcal{C}_{\delta,s}$ *have left idealiser isomorphic to* $\mathbb{F}_{q^8}$, *right idealiser isomorphic to* $\mathbb{F}_{q^4}$, *and are not equivalent to the other MRD codes known so far in the literature.*

Notice that Theorem 1.1 is a partial answer to Conjecture 4.6 in [18]. The techniques that we use to prove the first part of Theorem 1.1 are from algebraic geometry over finite fields. In particular, our starting point is an $\mathbb{F}_{q^{n/2}}$-rational plane curve $\mathcal{X}_{\delta,s}$ introduced in [18]; see Equation (2) below. For $n \geq 10$, the degree of $\mathcal{X}_{\delta,s}$ is low with respect to the size of $\mathbb{F}_{q^{n/2}}$, and hence the Hasse-Weil lower bound on the number of $\mathbb{F}_{q^{n/2}}$-rational points of $\mathcal{X}_{\delta,s}$ was enough in [18] to deduce results on the MRD property for $\mathcal{C}_{\delta,s}$. For $n = 8$ this is not sufficient. We then translate the MRD property for $\mathcal{C}_{\delta,s}$ into the estimate of the number of $\mathbb{F}_q$-rational points of another $\mathbb{F}_q$-rational algebraic variety $\mathcal{W}$ of low degree. We investigate the absolutely irreducible components of $\mathcal{W}$ and apply the Lang-Weil lower bound. In the study of MRD codes $\mathcal{C}_f$, similar algebraic geometric arguments have been already used in the literature, but only to deal with algebraic curves or hypersurfaces; see for instance [15]. On the contrary, $\mathcal{W}$ turns out to be a 3-dimensional variety in a 7-dimensional projective space.

The paper is organized as follows. Section 2 contains some preliminary results: after some generalities on algebraic varieties (Section 2.1) and codes (Section 2.2), we present what is known about codes $\mathcal{C}_{\delta,s}$ (Section 2.3) and the curves $\mathcal{X}_{\delta,s}$ (Section 2.4). Section 3 proves the first part of Theorem 1.1 about the characterization of MRD codes $\mathcal{C}_{\delta,s}$; the proof of some technical lemmas is postponed to Section 5. Section 4 completes the proof of Theorem 1.1 with the investigation of parameters and equivalences. Finally, we list in 6 some open problems on codes $\mathcal{C}_{\delta,s}$.

2. Preliminaries

For the rest of the paper, q is an odd prime power.

2.1. **Algebraic varieties.** We recall some basic facts on algebraic varieties, and refer the reader to [22] and [26] for a detailed introduction to varieties and function fields. A good reference for the applications of algebraic geometric techniques to polynomials over finite field is [1].

We denote by $\mathbb{K} = \overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$, and by $\mathbb{P}^N = \mathbb{P}^N(\mathbb{K})$ the N-dimensional projective space over $\mathbb{K}$. We will be interested in determining *dimension* and *degree* of *varieties* $\mathcal{V}$, i.e. of projective, possibly reducible, algebraic varieties $\mathcal{V} \subseteq \mathbb{P}^N$. A variety $\mathcal{V}$ which is irreducible over $\mathbb{K}$, is said to be *absolutely irreducible*, and can be studied through its *function field* $\mathbb{K}(\mathcal{V})$ over $\mathbb{K}$. If the ideal of $\mathcal{V}$ is generated by polynomials over $\mathbb{F}_q$, we say that $\mathcal{V}$ is *defined over* $\mathbb{F}_q$, or simply $\mathbb{F}_q$-*rational*. When $\mathcal{V}$ is both $\mathbb{F}_q$-rational and absolutely irreducible, $\mathbb{F}_q(\mathcal{V})$ is its function field over $\mathbb{F}_q$.

The following proposition recalls some elementary facts on the dimension of a variety.

Proposition 2.1. *Let* $\mathcal{V}, \mathcal{V}_1, \mathcal{V}_2$ *be algebraic varieties in* $\mathbb{P}^N$.
  (i) [22, Sec. 6.2, Cor. 5] *If* $\mathcal{V}$ *is defined by* r *equations, then the dimension of* $\mathcal{V}$ *is at least* $N - r$.
  (ii) [22, Sec. 6.2, Cor. 4] *If* s *is the maximum dimension of a linear space of* $\mathbb{P}^N$ *disjoint from* $\mathcal{V}$, *then the dimension of* $\mathcal{V}$ *is* $N - s - 1$.
  (iii) [22, Sec. 6.2, Th. 6] *If* $\mathcal{V}_1$ *and* $\mathcal{V}_2$ *are absolutely irreducible and have dimension* m_1 *and* m_2 *respectively, then any non-empty component of* $\mathcal{V}_1 \cap \mathcal{V}_2$ *has dimension at least* $m_1 + m_2 - N$.

An estimate for the number of $\mathbb{F}_q$-rational points of an $\mathbb{F}_q$-rational absolutely irreducible variety is provided by the Lang-Weil bound, which is a generalization to higher dimension of the Hasse-Weil bound for curves. We will use the Lang-Weil bound in the following improved version, due to Cafure and Matera.

Proposition 2.2. [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. *Let* A_q *be the number of* $\mathbb{F}_q$-*rational affine points of* $\mathcal{V}$. *If* $q > 2(m+1)d^2$, *then*

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

2.2. **q-polynomials and rank metric codes.** We now recall some preliminary results on q-polynomials and rank metric codes; for a detailed introduction to this topic we refer the reader to [24] and [19].

Let $\mathcal{L}_{n,q} = \left\{ \sum_{i=0}^{n-1} a_i x^{q^i} : a_i \in \mathbb{F}_{q^n} \right\}$ be the set of q-polynomials over $\mathbb{F}_{q^n}$ of q-degree smaller than n. Then $\mathcal{L}_{n,q}$ is an n-dimensional $\mathbb{F}_q$-vector space with the usual sum and scalar multiplication, and also an $\mathbb{F}_q$-algebra with the composition modulo $x^{q^n} - x$. We identify polynomials in $\mathcal{L}_{n,q}$ with the associated $\mathbb{F}_q$-linear polynomial maps over $\mathbb{F}_q$, so that we can consider the rank and the kernel of polynomials in $\mathcal{L}_{n,q}$. This identification is an isomorphism of $\mathbb{F}_q$-algebras between $\mathcal{L}_{n,q}$ and the space of $\mathbb{F}_q$-endomorphisms of $\mathbb{F}_{q^n}$. Therefore, via the choice of an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$, $\mathcal{L}_{n,q}$ is isomorphic as an $\mathbb{F}_q$-algebra to the space $\mathbb{F}_q^{n \times n}$ of $n \times n$ matrices over $\mathbb{F}_q$. In this correspondence, the rank of a matrix equals the rank of the associated q-polynomial. Therefore, $\mathcal{L}_{n,q}$ is a metric space with the rank metric $d(f,g) := \text{rank}(f - g)$, and $\mathbb{F}_q$-linear $[n \times n, k, d]_q$ rank metric codes $\mathcal{C}$ are k-dimensional $\mathbb{F}_q$-linear subspaces of $\mathcal{L}_{n,q}$ with minimum rank distance d between two distinct elements of $\mathcal{C}$. Since $\mathcal{C}$ is $\mathbb{F}_q$-linear, d equals the minimum rank of a non-zero element of $\mathcal{C}$. The Singleton-like bound $k \le n(n - d + 1)$ holds; see [7]. The code $\mathcal{C}$ is *maximum rank distance* (MRD for short) when it attains equality in the Singleton-like bound.

The following equivalence between rank metric codes preserves the parameters of a code; see [23].

Definition 2.3. *Two* $\mathbb{F}_q$-*linear* $[n \times n, k, d]_q$-*codes* $\mathcal{C}, \mathcal{C}'$ *are* equivalent *if there exist two invertible polynomials* $f_1(x), f_2(x) \in \mathcal{L}_{n,q}$ *and a field automorphism* $\varphi \in \text{Aut}(\mathbb{F}_{q^n})$ *such that*

$$\mathcal{C}' = f_1 \circ \mathcal{C}^\varphi \circ f_2 = \{f_1 \circ f^\varphi \circ f_2 : f \in \mathcal{C}\},$$

where $f^\varphi(x)$ *is obtained from* $f(x)$ *by applying* φ *to its coefficients.*

Related to the equivalence issue for rank metric codes is the tool of idealisers, as defined in [13].

Definition 2.4. *The* left idealiser $L(\mathcal{C})$ *and* right idealiser $R(\mathcal{C})$ *of an* $\mathbb{F}_q$-*linear rank metric code* $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ *are the following* $\mathbb{F}_q$-*algebras:*

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

Idealisers are invariant under equivalence.

Proposition 2.5. [14, Proposition 4.1] *If $\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ are equivalent codes, then $L(\mathcal{C}) \cong L(\mathcal{C}')$ and $R(\mathcal{C}) \cong R(\mathcal{C}')$ as $\mathbb{F}_q$-algebras.*

More structural information is known for idealisers of MRD codes.

Proposition 2.6. [14, Section 5] *If $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ is an MRD code, then $L(\mathcal{C})$ and $R(\mathcal{C})$ are both finite fields. Also, $|L(\mathcal{C})| = q^\ell$ and $|R(\mathcal{C})| = q^m$ for some divisors ℓ and m of n.*

2.3. **Codes $\mathcal{C}_f$ and $\mathcal{C}_{\delta,s}$.** For any $f(x) \in \mathcal{L}_{n,q}$ of degree greater than 1, define the $\mathbb{F}_q$-linear code $\mathcal{C}_f$ and the $\mathbb{F}_q$-linear space U_f by

$$\mathcal{C}_f := \langle x, f(x)\rangle_{\mathbb{F}_{q^n}} = \{ax + bf(x): a, b \in \mathbb{F}_{q^n}\} \subseteq \mathcal{L}_{n,q}, \qquad U_f := \{(x, f(x)): x \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}.$$

Since $\mathcal{C}_f$ has dimension 2 over $\mathbb{F}_{q^n}$, the MRD property for $\mathcal{C}_f$ reads as follows.

Remark 2.7. *$\mathcal{C}_f$ is MRD if and only if $\dim_{\mathbb{F}_q} \ker(g(x)) \leq 1$ for any non-zero $g(x) \in \mathcal{C}_f$.*

Clearly, $\{\alpha x \colon \alpha \in \mathbb{F}_{q^n}\} \subseteq L(\mathcal{C}_f)$, and by Proposition 2.6 equality holds if $\mathcal{C}_f$ is MRD. Indeed, Proposition 2.8 shows that the parameters and the maximum size of the left idealiser are enough to characterize up to equivalence the family of codes $\mathcal{C}_f$ with scattered polynomials $f(x)$.

Proposition 2.8. [4, Proposition 6.1] *If $\mathcal{C} \subseteq \mathcal{L}_{n,q}$ is an $[n \times n, 2n, n-1]_q$ MRD code with $L(\mathcal{C}) \cong \mathbb{F}_{q^n}$, then $\mathcal{C}$ is equivalent to $\mathcal{C}_f$ for some scattered polynomial $f(x) \in \mathcal{L}_{n,q}$.*

Let n be an even positive integer, $s \in \{1, \ldots, n-1\}$ be coprime with $n/2$, and $\delta \in \mathbb{F}_{q^n}^*$. Define

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

Denote by $\mathrm{N}_{q^n/q^{\frac{n}{2}}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^{\frac{n}{2}}}$ the norm function $x \mapsto x^{1+q^{n/2}}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_{q^{\frac{n}{2}}}$.

- If $\mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta) = \mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta')$, then $\mathcal{C}_{\delta,s}$ is MRD if and only if $\mathcal{C}_{\delta',s}$ is MRD; see [4, Section 5].
- If $\mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta) = 1$ and $n > 2$, then $\dim_{\mathbb{F}_q} \ker(f_{\delta,s}(x)) > 1$ and $\mathcal{C}_{\delta,s}$ is not MRD.
- If $\mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta) \neq 1$, then the rank of any non-zero element of $\mathcal{C}_{\delta,s}$ is at least $n-2$, and hence $\mathcal{C}_{\delta,s}$ is either Almost MRD or MRD; see [4, Proposition 4.1].
- If $n = 2$, then $\mathcal{C}_{\delta,s} = \mathcal{L}_{2,q}$ is trivially MRD.
- If $n = 4$, then $\mathcal{C}_{\delta,s}$ is equivalent to a so-called twisted Gabidulin code, and is MRD if and only if $\delta^{1+q+q^2+q^3} \neq 1$; see [23].
- If $n = 6$, then there are exactly $\lceil (q^2 + q + 1)(q-2) \rceil$ values of $\mathrm{N}_{q^6/q^3}(\delta)$ for which $\mathcal{C}_{\delta,s}$ is MRD, and a characterization of such values of $\mathrm{N}_{q^6/q^3}(\delta)$ is known; see [20, Theorem 7.3] and [2].
- If $n = 8$, q is odd and $\mathrm{N}_{q^8/q^4}(\delta) = -1$, then $\mathcal{C}_{\delta,s}$ is MRD; see [4, Theorem 7.2].
- If $n = 8$, q is odd and $q \leq 11$, then $\mathcal{C}_{\delta,s}$ is MRD if and only if $\mathrm{N}_{q^8/q^4}(\delta) = -1$; see [4, Remark 7.4].
- If $n \geq 10$ and
$$n \geq \begin{cases} 8s + 4 & \text{if } q = 3 \text{ and } s > 1, \text{ or } q = 2 \text{ and } s > 2, \\ 8s + 2 & \text{otherwise}, \end{cases}$$
  then $\mathcal{C}_{\delta,s}$ is not MRD; see [18, Theorem 4.5].

Remark 2.9. *We have defined the codes $\mathcal{C}_{\delta,s}$ only when $\delta \neq 0$, which is the case under investigation in this paper. For completeness we mention here what happens when $\delta = 0$: the code $\langle x, x^{q^s}\rangle_{\mathbb{F}_{q^n}} \subseteq \mathcal{L}_{n,q}$ is MRD if and only if s is coprime with n. In this case, $\langle x, x^{q^s}\rangle_{\mathbb{F}_{q^n}}$ is a so-called generalized Gabidulin code; see [12].*

Recall that two subsets S_1, S_2 of $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ are $\Gamma\mathrm{L}(2, q^n)$-equivalent if $S_2 = \Sigma(S_1)$ for some invertible semilinear map $\Sigma \in \Gamma\mathrm{L}(2, q^n)$, that is, $\Sigma = L \circ \varphi$ where $L \in \mathrm{GL}(2, q^n)$ and φ acts elementwise as a field automorphism of $\mathbb{F}_{q^n}$.

For MRD codes, equivalence of codes $\mathcal{C}_f$ corresponds to $\Gamma\mathrm{L}$-equivalence of subspaces U_f.

Theorem 2.10. [23, Theorem 8] *Let* $f(x), g(x) \in \mathcal{L}_{n,q}$ *be such that* $\mathcal{C}_f, \mathcal{C}_g \subseteq \mathcal{L}_{n,q}$ *are MRD codes. Then the* $\mathbb{F}_q$-*vector subspaces* U_f *and* U_g *of* $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ *are* $\Gamma\mathrm{L}(2, q^n)$-*equivalent if and only if* $\mathcal{C}_f$ *and* $\mathcal{C}_g$ *are equivalent.*

The $\Gamma\mathrm{L}$-equivalence between subspaces $U_{\delta,s}$ has been determined in [4].

Proposition 2.11. [4, Proposition 5.1] *Let* $n \geq 4$ *be even,* $1 \leq s, s' < \frac{n}{2}$ *be such that* $\gcd(s, \frac{n}{2}) = \gcd(s', \frac{n}{2}) = 1$, *and* $\delta, \delta' \in \mathbb{F}_{q^n}^*$ *satisfy* $\mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta) \neq 1$, $\mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta') \neq 1$. *Then* $U_{\delta,s}$ *and* $U_{\delta',s'}$ *are* $\Gamma\mathrm{L}(2, q^n)$-*equivalent if and only if one of the following cases occurs for some automorphism* $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^{n/2}})$:

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

2.4. **An algebraic curve attached to** $\mathcal{C}_{\delta,s}$**.** We report here a characterization of MRD codes $\mathcal{C}_{\delta,s}$ provided in [18], which is our starting point for Section 3. The discussion in [18] is in terms of kernels of the q-polynomials in $\mathcal{C}_{\delta,s}$; we report it in terms of the MRD property for $\mathcal{C}_{\delta,s}$, by means of Remark 2.7.

Theorem 2.12 is a sufficient condition for $\mathcal{C}_{\delta,s}$ not being MRD.

Theorem 2.12. [18, Theorem 3.6] *Let* $\delta \in \mathbb{F}_{q^n}^*$ *be such that* $\alpha := \mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta) \in \mathbb{F}_{q^{n/2}}^*$ *satisfies* $\alpha \neq 1$, *and* $s \in \{1, \ldots, n-1\}$ *be coprime with* $n/2$. *If there exist* $T, S, A, B \in \mathbb{F}_{q^{n/2}}$ *such that*

- (i) $(1 - \alpha)(T + T^{q^s}) - \alpha S^{q^s+1} + (1 + \alpha)(AS - 2BT) = 0$,
- (ii) $X^2 - SX - T \in \mathbb{F}_{q^{n/2}}[X]$ *is irreducible over* $\mathbb{F}_{q^{n/2}}$,
- (iii) $S^{q^s} = 2A + BS$,
- (iv) $-T^{q^s} = A^2 + B(AS - BT)$,

then $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{n,q}$ *is not MRD.*

We will now translate the existence of T, S, A, B satisfying the assumptions of Theorem 2.12 into the existence of a suitable point of an $\mathbb{F}_{q^{n/2}}$-rational algebraic curve. The equation of this curve is obtained through arithmetic manipulations which depend on q being even or odd. We will give the resulting equation only in the case when q is odd, because this is the case that will be developed in the next sections. Therefore, assume in the rest of the section that q is odd.

Let T, S, A, B be as in the assumptions of Theorem 2.12. From Conditions (iii) and (iv) it follows that

$$B = \epsilon \Delta^{\frac{q^s-1}{2}}, \quad A = \frac{1}{2}(S^{q^s} - \epsilon S \Delta^{\frac{q^s-1}{2}}),$$

where $\Delta = S^2 + 4T$ and ϵ is either 1 or -1. Write $\beta := \epsilon \frac{\alpha+1}{1-\alpha}$, and choose any non-square element η of $\mathbb{F}_{q^{n/2}}$. The irreducibility condition (ii) in Theorem 2.12 is equivalent to the existence of an element $Z \in \mathbb{F}_{q^{n/2}}^*$ such that $\Delta = \eta Z^2$. Now, using $T = \frac{\eta Z^2 - S^2}{4}$ together with Condition (iv), we obtain the following equation from Condition (i):

$$(1) \qquad\qquad (S^{q^s} - S)^2 = \eta Z^2 + \eta^{q^s} Z^{2q^s} - 2\beta \eta^{\frac{q^s+1}{2}} Z^{q^s+1}.$$

Viceversa, suppose that $\beta = \epsilon \frac{\alpha+1}{1-\alpha}$ with $\epsilon \in \{1, -1\}$, and that Equation (1) is satisfied for some $S, Z \in \mathbb{F}_{q^{n/2}}$ with $Z \neq 0$ and some non-square η of $\mathbb{F}_{q^{n/2}}$. Then clearly there exist T, S, A, B satisfying the assumptions of Theorem 2.12.

In terms of the algebraic plane curve $\mathcal{X}_{\delta,s}$ with affine equation

$$(2) \qquad\qquad \mathcal{X}_{\delta,s}: \quad -(S^{q^s} - S)^2 + \eta Z^2 + \eta^{q^s} Z^{2q^s} - 2\beta \eta^{\frac{q^s+1}{2}} Z^{q^s+1} = 0,$$

the discussion above proves the following proposition.

Proposition 2.13. [18, Section 3.1] *Let* η *be a non-square in* $\mathbb{F}_{q^{n/2}}$, *Let* $\delta \in \mathbb{F}_{q^n}^*$, *s be coprime with* $n/2$, $\alpha = \mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta)$ *with* $\alpha \neq 1$, $\epsilon \in \{1, -1\}$ *and* $\beta := \epsilon \frac{\alpha+1}{1-\alpha}$. *If for some non-square* η *of* $\mathbb{F}_{q^{n/2}}$ *the curve* $\mathcal{X}_{\delta,s}$ *has an* $\mathbb{F}_{q^{n/2}}$-*rational affine point* $(\bar{s}, \bar{z})$ *with* $\bar{z} \neq 0$, *then the code* $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{n,q}$ *is not MRD.*

With the same notation as above, notice that $\beta \neq 1$ and $\beta \neq -1$, because $\delta \neq 0$; see Remark 2.9. Moreover, if $\beta = 0$ then $\mathrm{N}_{q^n/q^{\frac{n}{2}}}(\delta) = -1$; when $n = 8$, this condition on δ yields MRD codes $\mathcal{C}_{\delta,s}$, see Section 2.3. Therefore, for $n = 8$ we can assume in our investigation that $\beta \notin \{0, 1, -1\}$, and the following theorem follows from Proposition 2.13.

Theorem 2.14. *Let q be an odd prime power and $s \in \{1, 3, 5, 7\}$. Suppose that for any $\beta \in \mathbb{F}_{q^4} \setminus \{0, 1, -1\}$ there exists a non-square η of $\mathbb{F}_{q^4}$ such that the curve $\mathcal{X}_{\delta,s}$ with equation (2) has an $\mathbb{F}_{q^4}$-rational affine point $(\bar{s}, \bar{z})$ with $\bar{z} \neq 0$. Then $\mathcal{C}_{\delta,s}$ is MRD if and only if $\delta \in \mathbb{F}_{q^8}^*$ satisfies $\mathrm{N}_{q^8/q^4}(\delta) = -1$.*

Theorem 2.14 will be the key tool for the proof of the first part of Theorem 1.1 in the next section. For the sake of completeness, we now describe how Proposition 2.13 was used in [18] to study the MRD property for $\mathcal{C}_{\delta,s}$ for larger values of n.

If $\beta \notin \{1, -1\}$, then the curve $\mathcal{X}_{\delta,s}$ is absolutely irreducible, and has genus $g(\mathcal{X}_{\delta,s}) = q^{2s} - q^s - 1$; see [18, Theorem 3.7]. Thus, the Hasse-Weil lower bound

$$(3) \qquad N_{q^{n/2}} \geq q^{n/2} + 1 - 2(q^{2s} - q^s - 1)\sqrt{q^{n/2}}$$

holds for the number $N_{q^{n/2}}$ of rational places of the $\mathbb{F}_{q^{n/2}}$-rational curve $\mathcal{X}_{\delta,s}$. If

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

then the condition (3) implies that $N_{q^{n/2}}$ is positive and large enough, so that $\mathcal{X}_{\delta,s}$ has an $\mathbb{F}_{q^{n/2}}$-rational affine point $(\bar{s}, \bar{z})$ with $\bar{z} \neq 0$; see [18, Proposition 3.8]. By Proposition 2.13, this shows for any $\delta \in \mathbb{F}_{q^n}^*$ that under the condition (4) the code $\mathcal{C}_{\delta,s}$ is not MRD; this is the statement of [18, Theorem 1.1] for q odd.

In this way the question on the MRD property for $\mathcal{C}_{\delta,s}$ is completely answered when n is large enough with respect to s; for instance, when $s = 1$ and $n \geq 10$. On the contrary, the right-hand side of (4) is negative when $n = 8$, and a different approach to the curve $\mathcal{X}_{\delta,s}$ is required. This is the object of Section 3.

3. Characterization of MRD codes $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$

In this section we prove the first part of Theorem 1.1, namely Proposition 3.10. Through the whole section the prime power q is always assumed to be odd, so that we can consider the curve $\mathcal{X}_{\delta,s}$ in (2) and try to apply Theorem 2.14.

We start by showing that we can restrict to the case $s = 1$.

Proposition 3.1. *Let $\delta \in \mathbb{F}_{q^8}^*$ with $\mathrm{N}_{q^8/q^4}(\delta) \neq 1$. For any $s \in \{1, 3, 5, 7\}$, the code $\mathcal{C}_{\delta,s}$ 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 $\mathrm{N}_{q^8/q^4}(\delta) = -1$.*

Proof. For $s = 1$ or $s = 3$, the claim follows from Theorem 2.10 and Proposition 2.11, as $\sigma(-1) = -1$ for any $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^4})$.

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 $\mathrm{N}_{q^8/q^4}(1/\delta) = -1$, and the claim holds for $s = 1$ and $s = 3$, it follows that the claim holds also for $s = 5$ and $s = 7$. $\qquad\square$

We can then assume from now on that $s = 1$, so that the curve to be considered has equation

$$(5) \qquad \mathcal{X}_{\delta,1}: \quad -(S^q - S)^2 + \eta Z^2 + \eta^q Z^{2q} - 2\beta \eta^{\frac{q+1}{2}} Z^{q+1} = 0,$$

where $\beta \in \mathbb{F}_{q^4} \setminus \{0, 1, -1\}$ and η is a non-square in $\mathbb{F}_{q^4}$.

Let ξ be a normal element of $\mathbb{F}_{q^4}$ over $\mathbb{F}_q$, and write

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

Since $\mathcal{B} = \{\xi, \xi^q, \xi^{q^2}, \xi^{q^3}\}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^4}$, Equation 6 gives a one-to-one correspondence $(S, Z) \mapsto (S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3)$ between $\mathbb{F}_{q^4}^2$ and $\mathbb{F}_q^8$.

Now plug $S, Z \in \mathbb{F}_{q^4}$ from Equation (6) into (5) and write it as a zero $\mathbb{F}_q$-linear combination

$$f_0 \xi + f_1 \xi^q + f_2 \xi^{q^2} + f_3 \xi^{q^3} = 0$$

in the basis $\mathcal{B}$. Since the left-hand side of (5) is a quadratic form over $\mathbb{F}_q$, the coefficients f_i are homogeneous quadratic polynomials over $\mathbb{F}_q$ in the 8 indeterminates S_i, Z_i. Thus, the equations

$$\mathcal{W}: \begin{cases} f_0(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0, \\ f_1(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0, \\ f_2(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0, \\ f_3(S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) = 0 \end{cases}$$

define an $\mathbb{F}_q$-rational projective variety $\mathcal{W}$ in $\mathbb{P}^7$. We have shown that the $\mathbb{F}_q$-rational points of $\mathcal{W}$ give information on the $\mathbb{F}_{q^4}$-rational points of $\mathcal{X}_{\delta,1}$, as follows.

Lemma 3.2. *If $\mathcal{W}$ has an $\mathbb{F}_q$-rational point $(S_0 : S_1 : S_2 : S_3 : Z_0 : Z_1 : Z_2 : Z_3)$ with $Z_3 \neq 0$, then $\mathcal{X}_{\delta,1}$ has an $\mathbb{F}_{q^4}$-rational affine point (S, Z) with $Z \neq 0$, given by Equation (6).*

By Theorem 2.14 and Lemma 3.2, it is enough to show that $\mathcal{W}$ has an $\mathbb{F}_q$-rational point for any $\beta \notin \{0, 1, -1\}$ and for some non-square η of $\mathbb{F}_{q^4}$. To do this, we will prove that $\mathcal{W}$ has an $\mathbb{F}_q$-rational absolutely irreducible component. To this aim, we will study the absolutely irreducible components of another variety $\mathcal{V}$ which is projectively equivalent to $\mathcal{W}$.

Consider the Moore matrix

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

over $\mathbb{F}_{q^4}$. Since $\mathcal{B}$ is an $\mathbb{F}_q$-basis of $\mathbb{F}_{q^4}$, we have $\det(M) \neq 0$; see [16]. Thus the map φ defined by

$$(S_0 : S_1 : S_2 : S_3 : Z_0 : Z_1 : Z_2 : Z_3) \mapsto (X_0 : X_1 : X_2 : X_3 : Y_0 : Y_1 : Y_2 : Y_3) := (S_0, S_1, S_2, S_3, Z_0, Z_1, Z_2, Z_3) \cdot \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix}$$

is an $\mathbb{F}_{q^4}$-rational projectivity of $\mathbb{P}^7$.

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 $Y_i = Z^{q^i}$. Therefore, the equations defining the image $\varphi(\mathcal{W})$ are obtained by applying the q^j-power to Equation (5) with $j = 0, \ldots, 3$, and replacing S^{q^i}, Z^{q^i} with X_i, Y_i. One gets

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

Clearly $\varphi(\mathcal{W})$ is defined over $\mathbb{F}_{q^4}$, since φ is $\mathbb{F}_{q^4}$-rational and $\mathcal{W}$ is defined over $\mathbb{F}_q$.

Let $\psi : \mathbb{P}^7 \to \mathbb{P}^7$ be the $\mathbb{F}_q$-rational projectivity defined by

$$(X_0 : X_1 : X_2 : X_3 : Y_0 : Y_1 : Y_2 : Y_3) \mapsto (W_0 = X_1 - X_0 : W_1 = X_2 - X_1 : W_2 = X_3 - X_2 : X_3 : Y_0 : Y_1 : Y_2 : Y_3).$$

Then the variety $\mathcal{V} := \psi(\varphi(\mathcal{W}))$ is defined over $\mathbb{F}_{q^4}$ and has equations

(7)
$$\mathcal{V} : \begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}} Y_0 Y_1, \\ W_1^2 = \eta^q Y_1^2 + \eta^{q^2} Y_2^2 - 2\beta^q \eta^{\frac{q^2+q}{2}} Y_1 Y_2, \\ W_2^2 = \eta^{q^2} Y_2^2 + \eta^{q^3} Y_3^2 - 2\beta^{q^2} \eta^{\frac{q^3+q^2}{2}} Y_2 Y_3, \\ (W_0 + W_1 + W_2)^2 = \eta^{q^3} Y_3^2 + \eta Y_0^2 - 2\beta^{q^3} \eta^{\frac{1+q^3}{2}} Y_3 Y_0. \end{cases}$$

Note that $\mathcal{V}$ is a cone with vertex the point $(0:0:0:1:0:0:0:0)$.

We will use the following lemma to get information on $\mathcal{W}$ from the components of $\mathcal{V}$.

Lemma 3.3. *Suppose that $\mathcal{V}$ has an absolutely irreducible component $\mathcal{V}'$ of dimension m and degree d, such that no other absolutely irreducible component of $\mathcal{V}$ has dimension m and degree d. Then $\mathcal{W}$ has an absolutely irreducible component $\mathcal{W}'$ which is defined over $\mathbb{F}_q$ and has dimension m and degree d.*

Proof. Recall that projectivities between varieties preserve absolute irreducibility, dimension and degree of the components. Since $\mathcal{W}$ is projectively equivalent to $\mathcal{V}$ through the projectivity $\pi := (\psi \circ \varphi)^{-1}$, the variety $\mathcal{W}' := \pi(\mathcal{V}')$ is the only absolutely irreducible component of $\mathcal{W}$ with dimension m and degree d.

Let $\Phi_q : P \mapsto P^q$ be the q-Frobenius map, which raises the coordinates of a point to power q. Since $\mathcal{W}$ is defined over $\mathbb{F}_q$, Φ_q preserves $\mathcal{W}$. Being a collineation, Φ_q maps absolutely irreducible components of $\mathcal{W}$ to absolutely irreducible components of $\mathcal{W}$ with the same dimension and degree. Since $\mathcal{W}'$ is the only absolutely irreducible component of $\mathcal{W}$ with dimension d and degree m, Φ_q preserves $\mathcal{W}'$. Therefore, $\mathcal{W}'$ is defined over $\mathbb{F}_q$. $\qquad\square$

The dimension and degree of $\mathcal{V}$ are given in Lemma 3.4, whose proof is postponed to Section 5.1.

Lemma 3.4. *The variety $\mathcal{V} \subset \mathbb{P}^7$ has dimension 3 and degree 16.*

We first consider the case $\beta^{2q} \neq \beta^2$, starting by the intersection of $\mathcal{V}$ with a suitable hyperplane. The proof of Lemma 3.5 is postponed to Section 5.2.

Lemma 3.5. *Let $\beta \in \mathbb{F}_{q^4}$ be such that $\beta^{2q} \neq \beta^2$. For some non-square η of $\mathbb{F}_{q^4}$ and infinitely many elements $k \in \mathbb{K}$, the intersection between $\mathcal{V}$ and the hyperplane Π with affine equation $Y_2 = Y_1 + k$ is a non-repeated absolutely irreducible surface $\mathcal{S}$.*

Lemma 3.5 allows us to find in Proposition 3.6 a suitable component of $\mathcal{V}$.

Proposition 3.6. *Let $\beta \in \mathbb{F}_{q^4}$ be such that $\beta^{2q} \neq \beta^2$. For some non-square η of $\mathbb{F}_{q^4}$, $\mathcal{V}$ contains a unique absolutely irreducible component $\mathcal{V}'$ of dimension 3 and degree 16.*

Proof. Let η, k and Π be as in the claim of Lemma 3.5, so that $\mathcal{S} := \mathcal{V} \cap \Pi$ is a non-repeated absolutely irreducible surface. Suppose by contradiction that $\mathcal{V}$ has more than one absolutely irreducible component of dimension 3, and let $\mathcal{V}_1$ and $\mathcal{V}_2$ be two of them. By Proposition 2.1(iii), both $\Pi \cap \mathcal{V}_1$ and $\Pi \cap \mathcal{V}_2$ have dimension at least 2, and hence $\mathcal{S} = \Pi \cap \mathcal{V} \supseteq (\Pi \cap \mathcal{V}_1) \cup (\Pi \cap \mathcal{V}_2)$ contains two distinct components of dimension 2, or a repeated component of dimension 2. This is a contradiction to $\mathcal{S}$ being non-repeated and absolutely irreducible. Therefore $\mathcal{V}$ has a unique absolutely irreducible component $\mathcal{V}'$ of dimension 3. Being the unique component of maximal dimension, $\mathcal{V}'$ has the same degree 16 as $\mathcal{V}$. $\qquad\square$

The remaining cases for β are considered in Lemma 3.7, whose proof is postponed to Section 5.3.

Lemma 3.7. *Let $\beta \in \mathbb{F}_{q^4} \setminus \{0, 1, -1\}$ be such that $\beta^{2q} = \beta^2$. Then, for some non-square η of $\mathbb{F}_{q^4}$, $\mathcal{V}$ has exactly 3 irreducible components of dimension 3, and only one of them, say $\mathcal{V}'$, has degree 8.*

We can now show that $\mathcal{W}$ has $\mathbb{F}_q$-rational points when q is big enough.

Theorem 3.8. *Let $q \geq 1039891$ be an odd prime power, and $\beta \in \mathbb{F}_{q^4} \setminus \{0, 1, -1\}$. Then, for some non-square η of $\mathbb{F}_{q^4}$, $\mathcal{W}$ has an $\mathbb{F}_q$-rational point.*

Proof. If $\beta^{2q} \neq \beta^2$ then $\mathcal{W}$ has an $\mathbb{F}_q$-rational absolutely irreducible 3-dimensional component $\mathcal{W}'$ of degree 16, by Proposition 3.6 and Lemma 3.3. If $\beta^{2q} = \beta^2$ then $\mathcal{W}$ has an $\mathbb{F}_q$-rational absolutely irreducible 3-dimensional component $\mathcal{W}'$ of degree 8, by Lemma 3.7 and Lemma 3.3. In both cases we can apply Theorem 2.2 to $\mathcal{W}'$, with $m = 3$ and $d \leq 16$. Here, we choose the affine points of $\mathcal{W}'$ by dehomogenizing with respect to a Z_i-coordinate, say Z_3. Whenever $q \geq 2 \cdot (3+1) \cdot 16^2 = 2048$, this yields

$$A_q \geq q^3 - 15 \cdot 14 \cdot q^{5/2} - 5 \cdot 16^{13/3} \cdot q^2.$$

For $q \geq 1039891$, this implies $A_q > 0$. Therefore $\mathcal{W}'$ has an $\mathbb{F}_q$-rational point with $Z_3 \neq 0$, and the claim is proved. $\square$

By Theorem 3.8 and Lemma 3.2, the hypothesis of Theorem 2.14 holds when q is big enough. Therefore, by Theorem 2.14, the following is proved.

Proposition 3.9. *If $q \geq 1039891$ is an odd prime power and $\delta \in \mathbb{F}_{q^8}^*$, then $\mathcal{C}_{\delta,1} \subseteq \mathcal{L}_{8,q}$ is MRD if and only if $\mathrm{N}_{q^8/q^4}(\delta) = -1$.*

By Proposition 3.1, the claim of Proposition 3.9 holds also for any $s \in \{1, 3, 5, 7\}$.

Proposition 3.10. *If $q \geq 1039891$ is an odd prime power, $\delta \in \mathbb{F}_{q^8}^*$ and $s \in \{1, 3, 5, 7\}$, then $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$ is MRD if and only if $\mathrm{N}_{q^8/q^4}(\delta) = -1$.*

4. Parameters and equivalences for MRD codes $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$

In this section, we prove the second part of Theorem 1.1. Thus, we assume through the whole section that the prime power q is odd. We start from the parameters of $\mathcal{C}_{\delta,s}$.

Lemma 4.1. *For any $\delta \in \mathbb{F}_{q^8}$ with $\mathrm{N}_{q^8/q^4}(\delta) = -1$, $\mathcal{C}_{\delta,s}$ has parameters $[8 \times 8, 16, 7]_q$ and left idealiser $\{\lambda x : \lambda \in \mathbb{F}_{q^8}\} \cong \mathbb{F}_{q^8}$.*

Proof. The size 8×8 is clear from $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$. The $\mathbb{F}_q$-dimension of $\mathcal{C}_{\delta,s}$ is 16 because $\mathcal{C}_{\delta,s}$ is generated over $\mathbb{F}_{q^8}$ by the independent elements x and $f_{\delta,s}(x)$. The minimum distance of $\mathcal{C}_{\delta,s}$ is 7 since $\mathcal{C}_{\delta,s}$ is MRD with size 8×8 and $\mathbb{F}_q$-dimension 16. The left idealiser $L(\mathcal{C}_{\delta,s})$ contains the finite field $\{\tau_\lambda(x) = \lambda x : \lambda \in \mathbb{F}_{q^8}\} \cong \mathbb{F}_{q^8}$ and cannot be larger by Proposition 2.6. $\square$

The remaining parameter to be determined is the right idealiser.

Proposition 4.2. *For any $\delta \in \mathbb{F}_{q^8}$ with $\mathrm{N}_{q^8/q^4}(\delta) = -1$, $\mathcal{C}_{\delta,s}$ has right idealiser $\{\lambda x : \lambda \in \mathbb{F}_{q^4}\} \cong \mathbb{F}_{q^4}$.*

Proof. For any $\mu \in \mathbb{F}_{q^4}$, the polynomial $\tau_\mu(x) = \mu x$ satisfies $x \circ \tau_\mu(x) = \tau_\mu \circ x$ and $f_{\delta,s} \circ \tau_\mu(x) = \tau_{\mu^{q^s}} \circ f_{\delta,s}(x)$. As $\tau_\mu(x), \tau_{\mu^{q^s}}(x) \in L(\mathcal{C}_{\delta,s})$, this implies $\{\tau_\mu(x) : \mu \in \mathbb{F}_{q^4}\} \subseteq R(\mathcal{C}_{\delta,s})$. Then, by Proposition 2.6, either $R(\mathcal{C}_{\delta,s}) = \{\tau_\mu(x) : \mu \in \mathbb{F}_{q^4}\} \cong \mathbb{F}_{q^4}$ and the claim is proved, or $R(\mathcal{C}_{\delta,s}) \cong \mathbb{F}_{q^8}$.

Suppose that the latter case holds, so that both $L(\mathcal{C}_{\delta,s})$ and $R(\mathcal{C}_{\delta,s})$ are isomorphic to $\mathbb{F}_{q^8}$. Then, by [5, Theorem 2.2], $\mathcal{C}_{\delta,s}$ is equivalent to $\langle x, x^{q^t} \rangle_{\mathbb{F}_{q^8}}$ for some t. As $\mathcal{C}_{\delta,s}$ is MRD, t is coprime with n. Therefore, by Theorem 2.10, $U_{\delta,s}$ is $\Gamma L(2, q^8)$-equivalent to $U_{x^{q^t}}$. This is a contradiction to [4, Theorem 6.3]. $\square$

We now turn to the equivalence issue. Up to our knowledge, every $\mathbb{F}_q$-linear MRD code $\mathcal{C}$ in $\mathcal{L}_{8,q}$ with left idealiser isomorphic to $\mathbb{F}_{q^8}$ known so far in the literature is equivalent to one of the following.

(i) $\mathcal{C}_{\delta,s} = \langle x, x^{q^s} + \delta x^{q^{4+s}} \rangle_{\mathbb{F}_{q^8}}$ with $s \in \{1, 3, 5, 7\}$ and $\mathrm{N}_{q^8/q^4}(\delta) = -1$.

(ii) $\mathcal{C}_{G(r)} := \langle x, x^{q^r} \rangle_{\mathbb{F}_{q^8}}$ with $r \in \{1, 3, 5, 7\}$, so-called generalized Gabidulin codes; see [12].

(iii) $\mathcal{C}_{T(\epsilon,r)} := \langle x, \epsilon x^{q^r} + x^{q^{8-r}} \rangle_{\mathbb{F}_{q^8}}$ with $r \in \{1, 3, 5, 7\}$ and $\mathrm{N}_{q^8/q}(\epsilon) \notin \{0, 1\}$, so-called generalized twisted Gabidulin codes; see [23, Remark 8].

(iv) $\mathcal{C}_{Q(h,r)} := \langle x, \psi_{h,r}(x) \rangle_{\mathbb{F}_{q^8}}$, where $\psi_{h,r}(x)$ is the quadrinomial $x^{q^r} + x^{q^{3r}} + h^{q^r+1} x^{q^{5r}} + h^{1-q^{7r}} x^{q^{7r}}$, with $r \in \{1, 3, 5, 7\}$ and $\mathrm{N}_{q^8/q^4}(h) = -1$; see [17].

To complete the proof of Theorem 1.1, we show that $\mathcal{C}_{\delta,s}$ is not equivalent to any code in (ii), (iii) or (iv).

Proposition 4.3. *Let $s \in \{1, 3, 5, 7\}$ and $\delta \in \mathbb{F}_{q^8}$ be such that $\mathrm{N}_{q^8/q^4}(\delta) = -1$. For any $r \in \{1, 3, 5, 7\}$ and $\epsilon \in \mathbb{F}_{q^8}$ such that $\mathrm{N}_{q^8/q}(\epsilon) \notin \{0, 1\}$, $\mathcal{C}_{\delta,s}$ is not equivalent to $\mathcal{C}_{G(r)}$ nor to $\mathcal{C}_{T(\epsilon,r)}$.*

Proof. By Theorem 2.10, the claim is equivalent to $U_{\delta,s}$ being non-$\Gamma\mathrm{L}(2, q^8)$-equivalent to $U_{x^{q^r}}$ or $U_{\epsilon x^{q^r}+x^{q^{8-r}}}$. This was already proved in [4, Theorem 6.3]. □

We now consider the codes $\mathcal{C}_{Q(h,r)}$ in (iv). Let $t = n/2$. Theorem 4.6 in [17] provides an equivalence between $\mathcal{C}_{Q(h,r)}$ and $\mathcal{C}_{Q(\bar{h},1)}$ for some $\bar{h} \in \mathbb{F}_{q^{2t}}$ with $\mathrm{N}_{q^{2t}/q^t}(\bar{h}) = -1$, under the assuption $t \geq 5$. Yet, the arguments used in the proof of [17, Theorem 4.6] still hold when $t = 4$ (see also [10, Theorem 3.2 (ii)]), hence proving Lemma 4.4.

Lemma 4.4. *(see the proof of [17, Theorem 4.6]) Let $r \in \{1, 3, 5, 7\}$ and $h \in \mathbb{F}_{q^8}$ with $\mathrm{N}_{q^8/q^4}(h) = -1$. Then there exists $\bar{h} \in \mathbb{F}_{q^8}$ with $\mathrm{N}_{q^8/q^4}(\bar{h}) = -1$ such that $\mathcal{C}_{Q(h,r)}$ is equivalent to $\mathcal{C}_{Q(\bar{h},1)}$.*

Therefore we only have to consider the equivalence issue between $\mathcal{C}_{\delta,s}$ and $\mathcal{C}_{Q(h,1)}$. We start from $s = 1$.

Proposition 4.5. *For any $s \in \{1, 3, 5, 7\}$ and $\delta, h \in \mathbb{F}_{q^8}$ with $\mathrm{N}_{q^8/q^4}(\delta) = \mathrm{N}_{q^8/q^4}(h) = -1$, the codes $\mathcal{C}_{\delta,s}$ and $\mathcal{C}_{Q(h,1)}$ are not equivalent.*

Proof. By Theorem 2.10, it is enough to prove that $U_{\delta,s}$ and $U_{\psi_{h,1}}$ are not $\Gamma\mathrm{L}(2, q^8)$-equivalent. Assume by contradiction that there exist $\varphi \in \mathrm{Aut}(\mathbb{F}_{q^8})$ and $a, b, c, d \in \mathbb{F}_{q^8}$ such that $ad - bc \neq 0$ and the following holds: for every $y \in \mathbb{F}_{q^8}$, there exists $z \in \mathbb{F}_{q^8}$ satisfying

$$(8) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} y^\varphi \\ \psi_{h,1}(y)^\varphi \end{pmatrix} = \begin{pmatrix} z \\ f_{\delta,s}(z) \end{pmatrix}.$$

Write the action of φ on $\mathbb{F}_{q^8}$ as $\lambda \mapsto (\lambda^{p^i})^{q^j}$, with $1 \leq p^i < q$ and $0 \leq j < 8$. The map $(\mu, \rho) \mapsto (\mu^{q^j}, \rho^{q^j})$ is $\mathbb{F}_q$-linear on $\mathbb{F}_{q^8} \times \mathbb{F}_{q^8}$ and hence is in $\mathrm{GL}(2, q^8)$. Thus, up to changing a, b, c, d, we can assume that $j = 0$.

The condition (8) is equivalent to require that, for every $y \in \mathbb{F}_{q^8}$,

$$cy^\varphi + d\psi_{h,1}(y)^\varphi - f_{\delta,s}(ay^\varphi + b\psi_{h,1}(y)^\varphi) = 0.$$

Suppose $s = 1$. Then every element of $\mathbb{F}_{q^8}$ is a root of the following polynomial:

$$P(x) = \left(c - b^q h^{(q-1)p^i} - \delta b^{q^5}\right) x^{p^i} + (d - a^q) x^{qp^i} - \left(b^q + \delta b^{q^5} h^{(q^6+q^5)p^i}\right) x^{q^2 p^i} + dx^{q^3 p^i}$$

$$- \left(b^q + \delta b^{q^5} h^{(q^5-q^4)p^i}\right) x^{q^4 p^i} + \left(dh^{(q+1)p^i} - \delta a^{q^5}\right) x^{q^5 p^i} - \left(b^q h^{(q^2+q)p^i} + \delta b^{q^5}\right) x^{q^6 p^i} + dh^{(1-q^7)p^i} x^{q^7 p^i}.$$

Since the degree of $P(x)$ is smaller than q^8, this implies that $P(x)$ is the zero polynomial. The vanishing of its coefficients yields

$$(9) \qquad \begin{cases} a = d = 0, \\ c = b^q h^{(q-1)p^i} + \delta b^{q^5}, \\ b^q h^{(q^2+q)p^i} + \delta b^{q^5} = 0, \\ b^q + \delta b^{q^5} h^{(q^6+q^5)p^i} = 0, \\ b^q + \delta b^{q^5} h^{(q^5-q^4)p^i} = 0. \end{cases}$$

Since $\delta \neq 0$ and $b \neq 0$ (as $ad - bc \neq 0$), the last two equations in System (9) yield $h^{q^2+1} = 1$. Since 4 does not divide $q^2 + 1$, this yields a contradiction to $\mathrm{N}_{q^8/q^4}(h) = -1$. This proves the claim for $s = 1$, and hence for any $s \in \{1, 3, 5, 7\}$ by Proposition 3.1. □

Therefore, for any $\delta \in \mathbb{F}_{q^8}^*$ with $\mathrm{N}_{q^8/q^4} = -1$ and any $s \in \{1, 3, 5, 7\}$, the MRD code $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$ is not equivalent to a code $\mathcal{C}_{G(r)}$ or $\mathcal{C}_{T(\epsilon,r)}$ (Proposition 4.3), neither to a code $\mathcal{C}_{Q(h,r)}$ (Lemma 4.4 and Proposition 4.5). The proof of Theorem 1.1 is now complete.

5. Proof of Lemmas 3.4, 3.5, 3.7

In this section we prove three technical lemmas which were stated and applied in Section 3. The proofs of Lemmas 3.5 and 3.7 use arguments from the theory of algebraic function fields and their finite extensions, for which we refer the reader to the monograph [26]. In particular, we will show that certain quadratic equations $X^2 = u$ define Kummer extensions (see [26, Proposition 3.7.3]) of an algebraic function field L, by showing that u is not a square in L. To this aim, we will make use of Laurent series expansions with respect to local parameters at certain places (see [26, Theorem 4.2.6]).

5.1. Proof of Lemma 3.4.

By Proposition 2.1(i), the dimension of $\mathcal{V}$ is at least 3. To prove the equality, it is enough to provide a linear subspace $\mathcal{L}$ of $\mathbb{P}^7$ of dimension 3 such that $\mathcal{V} \cap \mathcal{L} = \emptyset$; see Proposition 2.1(ii). Let $\mathcal{L}$ be the 3-dimensional linear space defined by the equations

$$X_3 = 0, \quad Y_0 = 0, \quad Y_1 = 0, \quad Y_2 + Y_3 = 0.$$

If $\mathcal{V} \cap \mathcal{L} \neq \emptyset$, then any point $P = (\bar{w}_0 : \bar{w}_1 : \bar{w}_2 : \bar{x}_3 : \bar{y}_0 : \bar{y}_1 : \bar{y}_2 : \bar{y}_3)$ in $\mathcal{V} \cap \mathcal{L}$ satisfies

$$\bar{w}_0 = \bar{x}_3 = \bar{y}_0 = \bar{y}_1 = 0, \quad \bar{w}_1^2 = \eta^{q^2}\bar{y}_2^2, \quad \bar{w}_2^2 = (\eta^{q^2} + \eta^{q^3} + 2\beta^{q^2}\eta^{\frac{q^3+q^2}{2}})\bar{y}_2^2, \quad (\bar{w}_1 + \bar{w}_2)^2 = \eta^{q^3}\bar{y}_2^2.$$

This implies

$$2(\eta^{q^2} + \beta^{q^2}\eta^{\frac{q^3+q^2}{2}})\bar{y}_2^2 = -2\bar{w}_1\bar{w}_2,$$

whence

$$4(\eta^{q^2} + \beta^{q^2}\eta^{\frac{q^3+q^2}{2}})^2\bar{y}_2^4 = 4\bar{w}_1^2\bar{w}_2^2 = 4 \cdot \eta^{q^2}\bar{y}_2^2 \cdot (\eta^{q^2} + \eta^{q^3} + 2\beta^{q^2}\eta^{\frac{q^3+q^2}{2}})\bar{y}_2^2$$

and thus

$$4\eta^{q^3+q^2}(\beta^{2q^2} - 1)\bar{y}_2^4 = 0.$$

The case $\bar{y}_2 = 0$ cannot occur by the equations of $\mathcal{V}$ and $\mathcal{L}$, therefore $\beta^{2q^2} - 1 = 0$, a contradiction to $\beta \neq \pm 1$.

Finally, since $\mathcal{V} \subset \mathbb{P}^7$ has dimension 3 and its ideal is generated by 4 polynomials, $\mathcal{V}$ is a complete intersection. Thus, $\mathcal{V}$ has degree $2 \cdot 2 \cdot 2 \cdot 2 = 16$.

5.2. Proof of Lemma 3.5.

Note that the homogeneous equations of $\mathcal{V}$ can be dehomogenized with respect to the hyperplane at infinity $\mathcal{H}_0 \colon Y_0 = 0$, since it is easily seen that $\mathcal{V} \cap \mathcal{H}_0$ has dimension strictly smaller than 3. Thus, given $k \in \mathbb{K} = \overline{\mathbb{F}_{q^4}}$ and the hyperplane $\Pi \colon Y_2 = Y_1 + k$, $\mathcal{V} \cap \Pi$ has affine equations

$$\mathcal{V} \cap \Pi : \begin{cases} W_0^2 = \eta + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_1, \\ W_1^2 = \eta^q Y_1^2 + \eta^{q^2}(Y_1 + k)^2 - 2\beta^q\eta^{\frac{q^2+q}{2}}Y_1(Y_1 + k), \\ W_2^2 = \eta^{q^2}(Y_1 + k)^2 + \eta^{q^3}Y_3^2 - 2\beta^{q^2}\eta^{\frac{q^3+q^2}{2}}(Y_1 + k)Y_3, \\ (W_0 + W_1 + W_2)^2 = \eta^{q^3}Y_3^2 + \eta - 2\beta^{q^3}\eta^{\frac{1+q^3}{2}}Y_3 \end{cases}.$$

Therefore, given a transcendental y_1 over $\mathbb{K}$, if we prove that the equations

(10)
$$\begin{cases} w_0^2 = \eta + \eta^q y_1^2 - 2\beta\eta^{\frac{q+1}{2}}y_1, \\ w_1^2 = \eta^q y_1^2 + \eta^{q^2}(y_1 + k)^2 - 2\beta^q\eta^{\frac{q^2+q}{2}}y_1(y_1 + k), \\ w_2^2 = \eta^{q^2}(y_1 + k)^2 + \eta^{q^3}y_3^2 - 2\beta^{q^2}\eta^{\frac{q^3+q^2}{2}}(y_1 + k)y_3, \\ (w_0 + w_1 + w_2)^2 = \eta^{q^3}y_3^2 + \eta - 2\beta^{q^3}\eta^{\frac{1+q^3}{2}}y_3 \end{cases}$$

define an algebraic function field $\mathbb{K}(y_1, y_3, w_0, w_1, w_2, x_3)/\mathbb{K}$ of transcendence degree 2, then $\mathbb{K}(y_1, y_3, w_0, w_1, w_2, x_3)$ is the function field of a non-repeated absolutely irreducible surface $\mathcal{S} = \mathcal{V} \cap \Pi$ and Lemma 3.5 is proved. Note that x_3 does not appear in Equations (10), and hence is transcendental over $\mathbb{K}(y_1, y_3, w_0, w_1, w_2)$ (indeed, $\mathcal{V} \cap \Pi$ is a cone with vertex $(0 : 0 : 0 : 1 : 0 : 0 : 0 : 0)$). Thus, in order to prove Lemma 3.5 it is enough to show that Equations (10) define an algebraic function field $\mathbb{K}(y_1, y_3, w_0, w_1, w_2)/\mathbb{K}$ of transcendence degree 1.

After eliminating y_3 using the third and fourth equation of Equations (10), we obtain the following equivalent system:

(11)
$$\begin{cases} w_0^2 = \eta + \eta^q y_1^2 - 2\beta\eta^{\frac{q+1}{2}}y_1, \\ w_1^2 = \eta^q y_1^2 + \eta^{q^2}(y_1+k)^2 - 2\beta^q\eta^{\frac{q^2+q}{2}}y_1(y_1+k), \\ aw_2^2 + bw_2 + c = 0, \\ y_3 = \frac{\eta^q y_1^2 + \eta^{q^2}(y_1+k)^2 - \beta\eta^{\frac{q+1}{2}}y_1 - \beta^q\eta^{\frac{q^2+q}{2}}y_1(y_1+k) + w_0w_1 + w_1w_2 + w_0w_2}{\beta^{q^2}\eta^{\frac{q^3+q^2}{2}}(y_1+k) - \beta^{q^3}\eta^{\frac{q^3+1}{2}}}, \end{cases}$$

where

$$a = 2w_0w_1 + \left(-2\beta^q\eta^{\frac{q^2+q}{2}} - \beta^{2q^2}\eta^{q^2} + 2\eta^q + \eta^{q^2}\right)y_1^2 + 2\left(-\beta\eta^{\frac{q+1}{2}} - \beta^q\eta^{\frac{q^2+q}{2}}k - \beta^{2q^2}\eta^{q^2}k + \beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}}\right.$$
$$\left. + \eta^{q^2}k\right)y_1 - \beta^{2q^2}\eta^{q^2}k^2 + 2\beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}}k - \beta^{2q^3}\eta + \eta + \eta^{q^2}k^2,$$

$$b = \beta^q\eta^{\frac{q^2+q}{2}}(-6w_0 - 2w_1)y_1^2 - 2\beta^{2q^2}\eta^{q^2}(w_0+w_1)y_1^2 + 4\eta^q(w_0+w_1)y_1^2 + \eta^{q^2}(4w_0+2w_1)y_1^2$$
$$+ \beta\eta^{\frac{q+1}{2}}(-2w_0-6w_1)y_1 + \beta^q\eta^{\frac{q^2+q}{2}}k(-6w_0-2w_1)y_1 - 4\beta^{2q^2}\eta^{q^2}k(w_0+w_1)y_1 + 2\beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}}(w_0+w_1)y_1$$
$$+ \eta^{q^2}k(8w_0+4w_1)y_1 - 2\beta^{2q^2}\eta^{q^2}k^2(w_0+w_1) + 2\beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}}k(w_0+w_1) + \eta^{q^2}k^2(4w_0+2w_1) + 2\eta w_1,$$

$$c = 2w_0w_1\left[\left(-\beta^q\eta^{\frac{q^2+q}{2}} - \beta^{2q^2}\eta^{q^2} + \eta^q + \eta^{q^2}\right)y_1^2 + \left(-\beta\eta^{\frac{q+1}{2}} - \beta^q\eta^{\frac{q^2+q}{2}}k - 2\beta^{2q^2}\eta^{q^2}k + \beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}} + 2\eta^{q^2}k\right)y_1\right.$$
$$\left. - \beta^{2q^2}\eta^{q^2}k^2 + \beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}}k + \eta^{q^2}k^2\right] + \left(\beta^{2q}\eta^{q^2+q} + 2\beta^{2q^2+q}\eta^{\frac{3q^2+q}{2}} - 4\beta^q\eta^{\frac{q^2+3q}{2}} - 2\beta^q\eta^{3q^2+q} - 2\beta^{2q^2}\eta^{q^2+q}\right.$$
$$- \beta^{2q^2}\eta^{2q^2} + 2\eta^{2q} + 3\eta^{q^2+q} + \eta^{2q^2}\bigg)y_1^4 + 2\left(3\beta^{q+1}\eta^{\frac{q^2+2q+1}{2}} + \beta^{2q^2+1}\eta^{\frac{2q^2+q+1}{2}} - 2\beta\eta^{\frac{3q+1}{2}} - 2\beta\eta^{\frac{2q^2+q+1}{2}}\right.$$
$$+ \beta^{2q}\eta^{q^2+q}k + 3\beta^{2q^2+q}\eta^{\frac{3q^2}{2}}k - \beta^{q^3+q^2+q}\eta^{\frac{2q^2+q+1}{2}} - 2\beta^q\eta^{\frac{q^2+3q}{2}}k - 3\beta^q\eta^{\frac{3q^2+q}{2}}k - 2\beta^{2q^2}\eta^{q^2+q}k - 2\beta^{2q^2}\eta^{2q^2}k$$
$$+ \beta^{q^3+q^2}\eta^{\frac{q^2+2q+1}{2}} + 3\eta^{q^2+q}k + 2\eta^{2q^2}k\bigg)y_1^3 + \left(\beta^2\eta^{q+1} + 6\beta^{q+1}\eta^{\frac{q^2+2q+1}{2}}k + 4\beta^{2q^2+1}\eta^{\frac{2q^2+q+1}{2}}k\right.$$
$$- 2\beta^{q^3+q^2+1}\eta^{\frac{q^2+q+2}{2}} - 8\beta\eta^{\frac{2q^2+q+1}{2}}k + \beta^{2q}\eta^{q^2+q}k^2 + 6\beta^{2q^2+q}\eta^{\frac{3q^2+q}{2}}k^2 - 4\beta^{q^3+q^2+q}\eta^{\frac{2q^2+q+1}{2}}k - 2\beta^q\eta^{\frac{q^2+q+2}{2}}$$
$$- 6\beta^q\eta^{\frac{3q^2+q}{2}}k^2 - 2\beta^{2q^2}\eta^{q^2+q}k^2 - 6\beta^{2q^2}\eta^{2q^2}k^2 + 2\beta^{q^3+q^2}\eta^{\frac{q^2+2q+1}{2}}k + \beta^{2q^3}\eta^{q^2+1} + \eta^{q+1} + \eta^{q^2+1} + 3\eta^{q^2+q}k^2$$
$$+ 6\eta^{2q^2}k^2\bigg)y_1^2 + 2\left(\beta^{2q^2+1}\eta^{\frac{2q^2+q+1}{2}}k^2 - \beta^{q^3+q^2+1}\eta^{\frac{q^2+q+2}{2}}k - 2\beta\eta^{\frac{2q^2+q+1}{2}}k^2 + \beta^{2q^2+q}\eta^{\frac{3q^2+q}{2}}k^3\right.$$
$$- \beta^{q^3+q^2+q}\eta^{\frac{2q^2+q+1}{2}}k^2 - \beta^q\eta^{\frac{q^2+q+2}{2}}k - \beta^q\eta^{\frac{3q^2+q}{2}}k^3 - 2\beta^{2q^2}\eta^{q^2}k^3 + \beta^{2q^3}\eta^{q^2+1}k + \eta^{q^2+1}k + 2\eta^{2q^2}k^3\bigg)y_1$$
$$- \beta^{2q^2}\eta^{2q^2}k^4 + \beta^{2q^3}\eta^{q^2+1}k^2 + \eta^{q^2+1}k^2 + \eta^{2q^2}k^4.$$

Since the fourth equation of (11) is linear in y_3, it is enough to prove that the first, second and third equation of (11) define an algebraic function field $\mathbb{K}(y_1, w_0, w_1, w_2)/\mathbb{K}$ of transcendence degree 1 to have that $y_3 \in \mathbb{K}(y_1, w_0, w_1, w_2)$ and Lemma 3.5 is proved.

5.2.1. *The function field* $\mathbb{K}(y_1, w_0)$. Define the polynomial

$$F_0(Y) := \eta^q Y^2 - 2\beta\eta^{\frac{q+1}{2}}Y + \eta = \eta^q(Y - \lambda_1)(Y - \lambda_2) \in \mathbb{K}[Y],$$

having distinct roots

$$\lambda_1 = \eta^{\frac{1-q}{2}}(\beta - \sqrt{\beta^2 - 1}), \quad \lambda_2 = \eta^{\frac{1-q}{2}}(\beta + \sqrt{\beta^2 - 1}).$$

Then the first equation $w_0^2 = F_0(y_1)$ of (11) defines a Kummer extension $\mathbb{K}(y_1, w_0)/\mathbb{K}(y_1)$ of degree 2 with exactly two ramified places, namely the zeros of $y_1 - \lambda_1$ and $y_1 - \lambda_2$.

5.2.2. *The function field $\mathbb{K}(y_1, w_0, w_1)$.* Define the polynomial

$$F_1(Y) := \left(\eta^q - 2\beta\eta^{\frac{q+1}{2}} + \eta\right)^q Y^2 - 2k\left(\beta\eta^{\frac{q+1}{2}} - \eta^q\right)^q Y + k^2\eta^{q^2} \in \mathbb{K}[Y].$$

Up to this point, the only require on η is that it is a non-square in $\mathbb{F}_{q^4}$, and hence we have $(q^4-1)/2$ choices for η. The coefficient of Y^2 in $F_1(Y)$ vanishes for at most q values of η. Since $q < (q^4-1)/2$, we can choose η as a non-square $\mathbb{F}_{q^4}$ such that the coefficient of Y^2 in $F_1(Y)$ does not vanish. Now, choose $k \neq 0$. Then $F_1(Y)$ has distinct roots

$$\mu_1 = k \cdot \left(\frac{-\eta^q + \eta^{\frac{q+1}{2}}(\beta - \sqrt{\beta^2 - 1})}{\eta^q - 2\beta\eta^{\frac{q+1}{2}} + \eta}\right)^q, \qquad \mu_2 = k \cdot \left(\frac{-\eta^q + \eta^{\frac{q+1}{2}}(\beta + \sqrt{\beta^2 - 1})}{\eta^q - 2\beta\eta^{\frac{q+1}{2}} + \eta}\right)^q.$$

Up to excluding four values of $k \in \mathbb{K}$, we have $\{\lambda_1, \lambda_2\} \cap \{\mu_1, \mu_2\} = \emptyset$. Thus, $F_1(y_1)$ has four simple zeros in $\mathbb{K}(y_1, w_0)$, namely the zeros of $y_1 - \mu_1$ and $y_1 - \mu_2$. Then the second equation $w_1^2 = F_1(y_1)$ of (11) defines a Kummer extension $\mathbb{K}(y_1, w_0, w_1)/\mathbb{K}(y_1, w_0)$ of degree 2, in which the ramified places are the zeros of $y_1 - \mu_1$ and $y_1 - \mu_2$.

Note that the ramified places in $\mathbb{K}(y_1, w_0, w_1)/\mathbb{K}(y_1)$ are the 8 zeros of $y_1 - \lambda_1$, $y_1 - \lambda_2$, $y_1 - \mu_1$ and $y_1 - \mu_2$, all of them with ramification index 2.

5.2.3. *The function field $\mathbb{K}(y_1, w_0, w_1, w_2)$.* Define $u_2 = w_2 + \frac{b}{2a}$. Then the third equation of (11) reads

$$u_2^2 = \frac{(b/2)^2 - ac}{a^2}$$

$$= \left(\frac{\beta^{q^3}\sqrt{\eta} - \beta^{q^2}\sqrt{\eta}^{q^2}(y_1 + k)}{a}\right)^2 \left(w_0 w_1 + A - \eta^{\frac{q^2+1}{2}}\gamma(y_1 + k)\right)\left(w_0 w_1 + A + \eta^{\frac{q^2+1}{2}}\gamma(y_1 + k)\right)$$

where

$$A = -\beta\eta^{\frac{q+1}{2}}y_1 + \beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}}(y_1 + k) + \eta^q y_1^2 - \beta^q\eta^{\frac{q^2+q}{2}}y_1(y_1 + k), \qquad \gamma^2 = (\beta^{2q^3} - 1)(\beta^{2q^2} - 1).$$

Write $u_2^2 = \chi^2 \cdot \xi \cdot \zeta$, where

$$\xi = w_0 w_1 + A - \eta^{\frac{q^2+1}{2}}\gamma(y_1 + k) =: w_0 w_1 + \bar{a}y_1^2 + \bar{b}y_1 + \bar{c},$$

$$\zeta = \xi + 2\eta^{\frac{q^2+1}{2}}\gamma(y_1 + k) = w_0 w_1 + A + \eta^{\frac{q^2+1}{2}}\gamma(y_1 + k) = w_0 w_1 + \bar{a}y_1^2 + (\bar{b} + 2\eta^{\frac{q^2+1}{2}}\gamma)y_1 + \bar{c} + 2\eta^{\frac{q^2+1}{2}}\gamma k,$$

with

$$\bar{a} = \eta^q - \beta^q\eta^{\frac{q^2+q}{2}}, \quad \bar{b} = -\beta^q\eta^{\frac{q^2+q}{2}}k - \beta\eta^{\frac{q+1}{2}} + \beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}} - \eta^{\frac{q^2+1}{2}}\gamma, \quad \bar{c} = k(\beta^{q^3+q^2}\eta^{\frac{q^2+1}{2}} - \eta^{\frac{q^2+1}{2}}\gamma).$$

In order to prove that the third equation of (11) defines a Kummer extension $\mathbb{K}(y_1, w_0, w_1, w_2)/\mathbb{K}(y_1, w_0, w_1)$ of degree 2, we show that $\xi \cdot \zeta$ is not a square in $\mathbb{K}(y_1, w_0, w_1)$.

Define $\theta := w_0 w_1 - (\bar{a}y_1^2 + \bar{b}y_1 + \bar{c})$.

(i) We prove that the functions ξ, ζ, θ have exactly four poles with valuation -2 at each of them, and therefore have exactly eight zeros, counted with multiplicity. In fact, the poles of ξ, ζ, θ are among the four simple poles P_∞^i of y_1 in $\mathbb{K}(y_1, w_0, w_1)$. Clearly $1/y_1$ is a local parameter at P_∞^i. By Sections 5.2.1 and 5.2.2, the first term of the Laurent series expansion of $w_0 w_1$ at P_∞^i with respect to $1/y_1$ is ρy_1^2, where $\rho^2 = \eta^q(\eta^{q^2} - 2\beta^q\eta^{\frac{q^2+q}{2}} + \eta^q)$. If $\rho = \bar{a}$ or $\rho = -\bar{a}$, then $\rho^2 = \bar{a}^2$ which implies $\beta^{2q} = 1$, a contradiction.

(ii) We prove that, up to excluding a finite number of $k \in \mathbb{K}$, the zeros of $\xi \cdot \theta$ in $\mathbb{K}(y_1, w_0, w_1)$ are unramified over $\mathbb{K}(y_1)$. Suppose by contradiction that a zero P of $\xi \cdot \theta$ is also a zero of $y_1 - \lambda_1$ or $y_1 - \lambda_2$. Then $w_0(P) = 0$, and the resultant $R(k)$ between $F_0(Y)$ and $\bar{a}Y^2 + \bar{b}Y + \bar{c}$ with respect

to Y vanishes. $R(k)$ is a polynomial in the variable k whose coefficients must vanish, otherwise it is enough to exclude $\deg_k R(k)$ values of $k \in \mathbb{K}$ to get a contradiction. This gives

$$2\gamma\beta^{q+1}-2\gamma\beta^{q^3+q^2}+2\beta^{q+2}\eta^{\frac{q-q^2}{2}}-\beta^2\eta^{q-q^2}-2\beta^{q^3+q^2+q+1}+\beta^q-2\beta^q\eta^{\frac{q-q^2}{2}}+2\beta^{2q^3+2q^2}-\beta^{2q^2}-\beta^{2q^3}+\eta^{q-q^2}+1 = 0,$$

$$2\gamma\beta^{q+1} - 2\gamma\beta^{q^3+q^2} - 2\beta^{q^3+q^2+q+1} + \beta^{2q} + 2\beta^{2q^3+2q^2} - \beta^{2q^2} - \beta^{2q^3} + 1 = 0,$$

$$2\gamma\beta^{q+2}\eta^{\frac{q^2+1}{2}} - \gamma\beta^2\eta^{\frac{q+1}{2}} - 2\gamma\beta^{q^3+q^2+1}\eta^{\frac{q^2+1}{2}} + \gamma\eta^{\frac{q+1}{2}} - 2\beta^{q^3+q^2+q+2}\eta^{\frac{q^2+1}{2}} + \beta^{q^3+q^2+2}\eta^{\frac{q+1}{2}}$$
$$+\beta^{2q+1}\eta^{\frac{q^2+1}{2}} + 2\beta^{2q^3+2q^2+1}\eta^{\frac{q^2+1}{2}} - \beta^{2q^2+1}\eta^{\frac{q^2+1}{2}} - \beta^{2q^3+1}\eta^{\frac{q^2+1}{2}} + \beta\eta^{\frac{q+1}{2}} - \beta^{q^3+q^2}\eta^{\frac{q+1}{2}} = 0.$$

After eliminating γ, these two equations yield

$$\tag{12} \beta^{2q} - \beta^{2q^2} - \beta^{2q^3} + 1 = 0.$$

Equation (12), together with its conjugates

$$\beta^{2q^2} - \beta^{2q^3} - \beta^2 + 1 = 0, \qquad \beta^{2q^3} - \beta^2 - \beta^{2q} + 1 = 0, \qquad \beta^2 - \beta^{2q} - \beta^{2q^2} + 1 = 0$$

under the q-Frobenius map, provides a contradiction to $\beta \neq \pm 1$.

The case of a zero P of $\xi \cdot \theta$ being also a zero of $y_1 - \mu_1$ or $y_1 - \mu_2$ is ruled out analogously through the coefficients of the resultant between $F_1(Y)$ and $\bar{a}Y^2 + \bar{b}Y + \bar{c}$ seen as a polynomial in k, whose vanishing provides a contradiction to $\beta \neq \pm 1$.

(iii) Let $F_2(Y) \in \mathbb{K}[Y]$ be defined by

$$\xi \cdot \theta = w_0^2 w_1^2 - (\bar{a}y_1^2 + \bar{b}y_1 + \bar{c})^2 = c_4 y_1^4 + c_3 y_1^3 + c_2 y_1^2 + c_1 y_1 + c_0 =: F_2(y_1).$$

By direct computations we have

$$c_4 = -\eta^{q^2+q}(\beta^{2q} - 1),$$

$$c_3 = -2\eta^{q^2+q}[(\beta^{2q} - 1)k + \eta^{\frac{1-q}{2}}(\beta^q\gamma + \beta - \beta^{q^3+q^2+q}) + \eta^{\frac{1-q^2}{2}}(\beta^{q^3+q^2} - \beta^{q+1} - \gamma)],$$

$$c_2 = -\eta^{q^2+q}(\beta^{2q} - 1)k^2 - 2\eta^{q^2+q}[\eta^{\frac{1-q}{2}}(2\gamma\beta^q + 2\beta - 2\beta^{q^3+q^2+q}) + \eta^{\frac{1-q^2}{2}}(\beta^{q^3+q^2} - \beta^{q+1} - \gamma)]k$$
$$-\eta[2\gamma\beta\eta^{\frac{q^2+q}{2}} - 2\gamma\beta^{q^3+q^2}\eta^{q^2} + \beta^2\eta^q - 2\beta^{q^2+q^2+1}\eta^{\frac{q^2+q}{2}} + 2\beta^q\eta^{\frac{q^2+q}{2}} + 2\beta^{2q^3+2q^2}\eta^{q^2} - \beta^{2q^2}\eta^{q^2} - \beta^{2q^3}\eta^{q^2} - \eta^q],$$

$$c_1 = -2\eta^{q^2+1}k[\eta^{\frac{q-1}{2}}(\gamma\beta^q + \beta - \beta^{q^3+q^2+q})k + \eta^{\frac{q-q^2}{2}}(\gamma\beta - \beta^{q^3+q^2+1} + \beta^q) - 2\gamma\beta^{q^3+q^2} + 2\beta^{2q^3+2q^2} - \beta^{2q^2} - \beta^{2q^3}],$$

$$c_0 = -\eta^{q^2+1}(\gamma - \beta^{q^3+q^2} - 1)(\gamma - \beta^{q^3+q^2} + 1)k^2.$$

Note that $F_2(Y)$ has degree 4, since $c_4 = -\eta^{q^2+q}(\beta^{2q} - 1) \neq 0$.

We prove that, if $F_2(Y)$ is not a square in $\mathbb{K}[Y]$, then $\xi \cdot \zeta$ is not a square in $\mathbb{K}(y_1, w_0, w_1)$. In fact, if $F_2(Y)$ is not a square in $\mathbb{K}[Y]$, then $F(Y)$ has two distinct roots $\rho_1, \rho_2 \in \mathbb{K}$ with odd multiplicity. Then, for any $i = 1, 2$, ξ has two unramified zeros over ρ_i, with valuation equal to the odd multiplicity of ρ_i as a zero of $F_2(Y)$. Suppose by contradiction that $\xi \cdot \zeta$ is a square, and hence has even valuation at every place. Then ζ has zeros over ρ_1 and ρ_2, and $\zeta - \xi = 2\eta^{\frac{q^2+1}{2}}\gamma(y_1 + k)$ has zeros over ρ_1 and ρ_2, a contradiction to $\rho_1 \neq \rho_2$.

(iv) We prove that $F_2(Y)$ is not a square in $\mathbb{K}[Y]$. Suppose by contradiction that

$$F_2(Y) = (d_2 Y^2 + d_1 Y + d_0)^2$$

for some $d_i \in \mathbb{K}$, that is,

$$d_0^2 = c_0, \quad 2d_0 d_1 = c_1, \quad d_1^2 + 2d_0 d_1 = c_2, \quad 2d_1 d_2 = c_3, \quad d_2^2 = c_4.$$

This implies

$$\tag{13} 4c_0(c_2 - c_1) = c_1^2, \quad 4c_4(c_2 - c_1) = c_3^2.$$

Equation (13) provides two polynomials in k that must be identically zero, namely $p_1(k) := c_1^2 - 4c_0(c_2 - c_1)$ and $p_2(k) := c_3^2 - 4c_4(c_2 - c_1)$, otherwise a contradiction is obtained by excluding a finite number of $k \in \mathbb{K}$. By direct computation, the coefficient of k^2 in $p_2(k)$ is $\beta^q \gamma + \beta - \beta^{q^3+q^2+q}$, and hence

$$\tag{14} \beta^q \gamma + \beta - \beta^{q^3+q^2+q} = 0.$$

On the other hand, the vanishing of the coefficient of k^2 in $p_1(k)$ yields

$$\tag{15} 4\eta^{q^2+q+2}(\gamma^2 + 2\gamma\beta^{q+1} - 2\gamma\beta^{q^3+q^2} + \beta^2 - 2\beta^{q^3+q^2+q+1} + \beta^{2q} + \beta^{2q^3+2q^2} - 1) = 0.$$

The elimination of γ through the resultant between the left-hand sides in Equations (14) and (15) yields $\beta^{2q} - \beta^2 = 0$. This is a contradiction to the hypothesis of Lemma 3.5.

5.3. Proof of Lemma 3.7.

Note that $\beta^{q-1} \in \{1, -1\}$, and that $\mathcal{V}$ can be equivalently defined by the following linear combinations of the equations in (7):

$$\tag{16} \mathcal{V}: \begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}} Y_0 Y_1, \\ (W_1 - W_0)(W_1 + W_0) = -\eta(Y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}} Y_2)(Y_0 - 2\beta\eta^{\frac{q-1}{2}} Y_1 + \beta^{q-1}\eta^{\frac{q^2-1}{2}} Y_2), \\ (W_2 - W_1)(W_2 + W_1) = -\eta^q(Y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} Y_3)(Y_1 - 2\beta\eta^{\frac{q^2-q}{2}} Y_2 + \beta^{q-1}\eta^{\frac{q^3-q}{2}} Y_3), \\ (W_0 + W_1)(W_1 + W_2) = \beta\eta^{\frac{q+1}{2}}(Y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} Y_3)(Y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}} Y_2). \end{cases}$$

- First we show that the equations

$$\tag{17} \begin{cases} w_0^2 = \eta + \eta^q y_1^2 - 2\beta\eta^{\frac{q+1}{2}} y_1, \\ w_1^2 = \eta^q y_1^2 + \eta^{q^2} y_2^2 - 2\beta^q \eta^{\frac{q^2+q}{2}} y_1 y_2, \\ y_3 = -B'/A', \\ w_2 = \beta\eta^{\frac{q+1}{2}} \frac{(y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} y_3)(1 - \beta^{q-1}\eta^{\frac{q^2-1}{2}} y_2)}{w_0 + w_1} - w_1, \end{cases}$$

where

$$A' = -2\beta^{q-1}\eta^{\frac{q^3-1}{2}} w_0 w_1 + \beta^{q-1}(\beta^2 - 1)\eta^{\frac{q^3+1}{2}} + 2\beta^q\eta^{\frac{q^3+q}{2}} y_1 - 2\beta^2\eta^{\frac{q^3+q^2}{2}} y_2$$
$$- 2\beta^{q-1}\eta^{\frac{q^3+2q-1}{2}} y_1^2 + 2\beta\eta^{\frac{q^3+q^2+q-1}{2}} y_1 y_2 + \beta^{q-1}(\beta^2 - 1)\eta^{\frac{q^3+2q^2-1}{2}} y_2^2,$$

$$B' = 2(\beta - \eta^{\frac{q-1}{2}} y_1 + \beta^q\eta^{\frac{q^2-1}{2}} y_2) w_0 w_1 - (\beta^2 + 1)\eta^{\frac{q+1}{2}} y_1(1 + \eta^{q^2-1} y_2^2) + 2\beta^q\eta^{\frac{q^2+1}{2}} y_2$$
$$+ 4\beta\eta^q y_1^2 - 6\beta^{q+1}\eta^{\frac{q^2+q}{2}} y_1 y_2 + 2\beta\eta^{q^2} y_2^2 - 2\eta^{\frac{3q-1}{2}} y_1^3 + 4\beta^q\eta^{\frac{q^2+2q-1}{2}} y_1^2 y_2,$$

define an algebraic function field $\mathbb{F}_{q^4}(y_1, w_0, y_2, w_1)/\mathbb{F}_{q^4}$ of transcendence degree 2 over $\mathbb{F}_{q^4}$, with constant field $\mathbb{F}_{q^4}$; this will imply that $\mathbb{F}_{q^4}(y_1, w_0, y_2, w_1, x_3)$ is a function field of three variables over $\mathbb{F}_{q^4}$ with constant field $\mathbb{F}_{q^4}$, where x_3 is transcendent over $\mathbb{F}_{q^4}(y_1, w_0, y_2, w_1)$.

As shown in Section 5.2.1, the first equation of (17) defines a Kummer extension $\mathbb{F}_{q^4}(y_1, w_0)/\mathbb{F}_{q^4}(y_1)$ of degree 2 and transcendence degree 1 over $\mathbb{F}_{q^4}$ with constant field $\mathbb{F}_{q^4}$. Let y_2 be transcendent over $\mathbb{F}_{q^4}(y_1, w_0)$. Then, for some non-square η of $\mathbb{F}_{q^4}$, the function $\eta^q y_1^2 + \eta^{q^2} y_2^2 - 2\beta^q\eta^{\frac{q^2+q}{2}} y_1 y_2$ is not a square in $\mathbb{K}(y_1, w_0, y_2)$, because for some $k \in \mathbb{K}$ its specialization with $y_2 = y_1 + k$ is not a square in $\mathbb{K}(y_1, w_0)$ as shown in Section 5.2.2. Thus, the second equation of (17) defines a Kummer extension $\mathbb{F}_{q^4}(y_1, w_0, y_2, w_1)/\mathbb{F}_{q^4}(y_1, w_0, y_2)$ of degree 2 and transcendence degree 2 over $\mathbb{F}_{q^4}$ with constant field $\mathbb{F}_{q^4}$. The element A' is non-zero (since it has degree 1 as a polynomial in w_1 over $\mathbb{K}(y_1, w_0, y_2)$), and hence the element $y_3 \in \mathbb{F}_{q^4}(y_1, w_0, y_2, w_1)$ is well-defined by the third equation of (17). From $w_0 + w_1 \neq 0$ follows that the element $w_2 \in \mathbb{F}_{q^4}(y_1, w_0, y_2, w_1)$ is well-defined by the fourth equation of (17). The claim on the extension $\mathbb{F}_{q^4}(y_1, w_0)/\mathbb{F}_{q^4}(y_1)$ is proved.

- We show that the intersection between $\mathcal{V}$ and the hyperplane $W_0 + W_1 = 0$ contains exactly one absolutely irreducible component $\tilde{\mathcal{V}}$ of dimension 3, which is also the unique absolutely irreducible component of dimension 3 in the intersection between $\mathcal{V}$ and the hyperplane $Y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}}Y_2 = 0$. Moreover, $\tilde{\mathcal{V}}$ has degree 4.

  Indeed, suppose $W_0 + W_1 = 0$. Then either $Y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}}Y_3 = 0$ or $Y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}}Y_2 = 0$.

  – Suppose $Y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}}Y_3 = 0$. Then the solutions of (16) are given by the following systems:

$$\begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_0Y_1, \\ W_1 = -W_0, \\ Y_3 = \beta^{q-1}\eta^{\frac{q-q^3}{2}}Y_1, \\ Y_2 = \beta^{q-1}\eta^{\frac{1-q^2}{2}}Y_0, \\ W_2 = W_0; \end{cases} \qquad \begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_0Y_1, \\ W_1 = -W_0, \\ Y_3 = \beta^{q-1}\eta^{\frac{q-q^3}{2}}Y_1, \\ Y_2 = \beta^{q-1}\eta^{\frac{1-q^2}{2}}Y_0, \\ W_2 = -W_0; \end{cases}$$

$$\begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_0Y_1, \\ W_1 = -W_0, \\ Y_3 = \beta^{q-1}\eta^{\frac{q-q^3}{2}}Y_1, \\ Y_2 = -\beta^{q-1}\eta^{\frac{1-q^2}{2}}Y_0 + 2\beta^q\eta^{\frac{q-q^2}{2}}Y_1, \\ W_2 = W_0; \end{cases} \qquad \begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_0Y_1, \\ W_1 = -W_0, \\ Y_3 = \beta^{q-1}\eta^{\frac{q-q^3}{2}}Y_1, \\ Y_2 = -\beta^{q-1}\eta^{\frac{1-q^2}{2}}Y_0 + 2\beta^q\eta^{\frac{q-q^2}{2}}Y_1, \\ W_2 = -W_0. \end{cases}$$

  For each of these four systems, the following holds. The first equation defines an absolutely irreducible curve in W_0, Y_0, Y_1, as shown in Section 5.2.1. Each of the remaining four equations is linear and defines an absolutely irreducible curve with an additional indeterminate; in terms of function fields, $\mathbb{K}(w_0, y_1)$ remains the same. Since the indeterminate X_3 does not appear, the system defines an absolutely irreducible surface contained in $\mathcal{V} \subset \mathbb{P}^7$, namely a cone with vertex $(0 : 0 : 0 : 1 : 0 : 0 : 0 : 0)$; its function field is $\mathbb{K}(w_0, y_1, x_3)$, where x_3 is transcendental over $\mathbb{K}(w_0, y_1)$.

  – Suppose $Y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}}Y_2 = 0$. By direct computation, (7) reads

$$\tilde{\mathcal{V}}: \begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_0Y_1, \\ W_2^2 = \eta Y_0^2 + \eta^{q^3} Y_3^2 - 2\beta^q\eta^{\frac{q^3+1}{2}}Y_0Y_3, \\ Y_2 = \beta^{q-1}\eta^{\frac{1-q^2}{2}}Y_0, \\ W_1 = -W_0. \end{cases}$$

An argument analogous to the one used in Section 5.2 shows that $\tilde{\mathcal{V}}$ is absolutely irreducible. In fact, we have

$$\eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}}Y_0Y_1 = \eta^q(Y_1 - \lambda_1 Y_0)(Y_1 - \lambda_2 Y_0)$$

with $\lambda_1 \neq \lambda_2$. After the specialization $Y_3 = hY_1$ with $h \in \mathbb{K}$, write

$$(\eta Y_0^2 + \eta^{q^3} Y_3^2 - 2\beta^q\eta^{\frac{q^3+1}{2}}Y_0Y_3)\,|_{Y_3=hY_1} = \eta^{q^3}(Y_3 - h\mu_1 Y_0)(Y_3 - h\mu_3 Y_0).$$

For a suitable $h \in \mathbb{K}$, the values $h\mu_1$ and $h\mu_2$ are different from each other and different from λ_1 and λ_2. Therefore, recalling that the indeterminate X_3 does not appear explicitly, the intersection between $\tilde{\mathcal{V}}$ and the hyperplane $Y_3 = hY_1$ is an absolutely irreducible surface, namely a cone with vertex $(0 : 0 : 0 : 1 : 0 : 0 : 0 : 0)$, and hence $\tilde{\mathcal{V}}$ is an absolutely irreducible variety with $\dim(\tilde{\mathcal{V}}) = 3 = \dim(\mathcal{V})$. Hence, $\tilde{\mathcal{V}}$ is an absolutely irreducible component of $\mathcal{V}$, and it is readily seen that $\tilde{\mathcal{V}}$ is the unique 3-dimensional component of $\mathcal{V}$ contained in the hyperplane $Y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}}Y_2 = 0$. Clearly $\tilde{\mathcal{V}}$ is a complete intersection, whence $\deg(\tilde{\mathcal{V}}) = 4$.

- With the same arguments as in the previous point, it is easily seen that the intersection between $\mathcal{V}$ and the hyperplane $W_1 + W_2 = 0$ contains exactly one absolutely irreducible component $\hat{\mathcal{V}}$ of dimension 3, given by

$$\hat{\mathcal{V}}: \begin{cases} W_0^2 = \eta Y_0^2 + \eta^q Y_1^2 - 2\beta\eta^{\frac{q+1}{2}} Y_0 Y_1, \\ W_1^2 = \eta^q Y_1^2 + \eta^{q^2} Y_2^2 - 2\beta^q \eta^{\frac{q^2+q}{2}} Y_1 Y_2, \\ Y_3 = \beta^{q-1} \eta^{\frac{q-q^3}{2}} Y_1, \\ W_2 = -W_1, \end{cases}$$

which is also the unique absolutely irreducible component of dimension 3 in the intersection between $\mathcal{V}$ and the hyperplane $Y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} Y_3 = 0$. Moreover, $\hat{\mathcal{V}}$ has degree 4.
- We show that $\mathcal{V}$ has exactly another 3-dimensional absolutely irreducible component $\mathcal{V}'$ other than $\tilde{\mathcal{V}}$ and $\hat{\mathcal{V}}$, having degree 8.

  Indeed, by what has been shown for $\tilde{\mathcal{V}}$, we can assume that $W_0 + W_1$ does not vanish identically, so that the fourth equation of (16) yields

$$w_2 = \beta\eta^{\frac{q+1}{2}} \frac{(y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} y_3)(y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}} y_2)}{w_0 + w_1} - w_1.$$

  After replacing w_2 and deleting the denominator $w_0 + w_1$, the third equation of (16) gives

$$(y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} y_3) \cdot (A \cdot y_3 + B) = 0,$$

  where

$$A = -2\beta^{q-1}\eta^{\frac{q^3-1}{2}} w_0 w_1 + \beta^{q-1}(\beta^2 - 1)\eta^{\frac{q^3+1}{2}} y_0^2 + 2\beta^q \eta^{\frac{q^3+q}{2}} y_0 y_1 - 2\beta^2 \eta^{\frac{q^3+q^2}{2}} y_0 y_2$$
$$- 2\beta^{q-1}\eta^{\frac{q^3+2q-1}{2}} y_1^2 + 2\beta\eta^{\frac{q^3+q^2+q-1}{2}} y_1 y_2 + \beta^{q-1}(\beta^2 - 1)\eta^{\frac{q^3+2q^2-1}{2}} y_2^2,$$

$$B = 2(\beta y_0 - \eta^{\frac{q-1}{2}} y_1 + \beta^q \eta^{\frac{q^2-1}{2}} y_2)w_0 w_1 - (\beta^2 + 1)\eta^{\frac{q+1}{2}} (y_0^2 y_1 + \eta^{q^2-1} y_1 y_2^2) + 2\beta^q \eta^{\frac{q^2+1}{2}} y_0^2 y_2$$
$$+ 4\beta\eta^q y_0 y_1^2 - 6\beta^{q+1}\eta^{\frac{q^2+q}{2}} y_0 y_1 y_2 + 2\beta\eta^{q^2} y_0 y_2^2 - 2\eta^{\frac{3q-1}{2}} y_1^3 + 4\beta^q \eta^{\frac{q^2+2q-1}{2}} y_1^2 y_2.$$

By what has been shown for $\hat{\mathcal{V}}$, we can assume that $y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} y_3$ does not vanish identically, so that the third equation of (16) can be replaced by the equation $A \cdot y_3 + B = 0$. Therefore, every 3-dimensional absolutely irreducible component of $\mathcal{V}$ other than $\tilde{\mathcal{V}}$ and $\hat{\mathcal{V}}$ is contained in the variety $\mathcal{V}'$ whose function field is defined by

$$\begin{cases} w_0^2 = \eta y_0^2 + \eta^q y_1^2 - 2\beta\eta^{\frac{q+1}{2}} y_0 y_1, \\ w_1^2 = \eta^q y_1^2 + \eta^{q^2} y_2^2 - 2\beta^q \eta^{\frac{q^2+q}{2}} y_1 y_2, \\ y_3 = -B/A, \\ w_2 = \beta\eta^{\frac{q+1}{2}} \frac{(y_1 - \beta^{q-1}\eta^{\frac{q^3-q}{2}} y_3)(y_0 - \beta^{q-1}\eta^{\frac{q^2-1}{2}} y_2)}{w_0 + w_1} - w_1. \end{cases}$$

Note that the system (17) defines exactly the coordinate functions of $\mathcal{V}'$ after dehomogenizing the equations with respect to Y_0. Therefore, by what has been shown above for $\mathbb{F}_{q^4}(y_1, w_0, y_2, w_1, x_3)$, $\mathcal{V}'$ is absolutely irreducible and has dimension 3. Finally, we use the fact that the degree of $\mathcal{V}$ is the sum of the degrees if its absolutely irreducible components of maximal dimension (see [11, Proposition 7.6 (b)]) to conclude that

$$\deg(\mathcal{V}') = \deg(\mathcal{V}) - \deg(\tilde{\mathcal{V}}) - \deg(\hat{\mathcal{V}}) = 8.$$

6. Conclusions and open problems

In this paper we have considered for $n = 8$ the rank metric codes $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{n,q}$, where $\delta \in \mathbb{F}_{q^n}^*$ and s is coprime with $n/2$. We have given a partial answer to Conjecture 4.6 in [18], proving its validity under the assumption that q is odd and $q \geq 1039891$.

The following questions naturally arise, and we list them as open problems. A solution to them would complete the classification of MRD codes $\mathcal{C}_{\delta,s}$ in $\mathcal{L}_{n,q}$ for any even positive integer n and prime power q.

(1) Let $n \geq 10$, and suppose that $n < 4s + 1$, so that the assumptions of [18, Theorem 4.5] do not hold. Is it still possible to classify the codes $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{n,q}$ which are MRD?

(2) Let $n = 8$ and q be an odd prime power with $q < 1039891$. Classify the codes $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$ which are MRD: is it true that $\mathcal{C}_{\delta,s}$ is MRD if and only if $N_{q^8/q^4}(\delta) = -1$? For $q \leq 11$ this is true; see [4, Remark 7.4].

(3) Let $n = 8$ and q be an even prime power. Classify the codes $\mathcal{C}_{\delta,s} \subseteq \mathcal{L}_{8,q}$ which are MRD: is it true that $\mathcal{C}_{\delta,s}$ is never MRD? For $q \leq 8$ this is true; see [4, Remark 7.4].

In order to deal with the point (3), we have tried to apply algebraic geometric techniques, similar to the ones used in this paper. More precisely, a result analogous to Proposition 2.13 holds for q even after replacing the curve $\mathcal{X}_{\delta,s}$ in (2) with a suitable plane curve $\mathcal{X}_{\delta,s}^{even}$, as shown in [18, Section 3.2]. In analogy with Equation (6) and the variety $\mathcal{V}$ in this paper, we have then considered the q-powers of the indeterminates of $\mathcal{X}_{\delta,s}^{even}$ as the indeterminates of a higher-dimensional variety $\mathcal{V}_{even}$. However, we have not been able to decide whether $\mathcal{V}_{even}$ contains an absolutely irreducible rational component, although computational experiments for small values of q suggest that $\mathcal{V}_{even}$ may be absolutely irreducible.

7. Acknoledgements

References

[1] D. Bartoli: Hasse-Weil type theorems and relevant classes of polynomial functions. In: BCC 2021, 43–102.

[2] 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.

[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, O. Polverino and C. Zanella: A new family of MRD-codes, *Linear Algebra Appl.* **548** (2018), 203–220.

[5] B. Csajbók, G. Marino, O. Polverino and Y. Zhou: MRD codes with maximum idealizers, *Discrete Math.* **343** (2020), 111985.

[6] J. de la Cruz: On dually almost MRD codes, *Finite Fields Appl.* **53** (2018), 1–20.

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

[8] E. M. Gabidulin: Theory of codes with maximum rank distance, *Problemy Peredachi Informatsii* **21 (1)** (1985), 3–16.

[9] E. M. Gabidulin, A. Paramonov and O. Tretjakov: Ideals over a non-commutative ring and their application in cryptology, *Advances in Cryptology - EUROCRYPT'91*, LNCS **547**, Springer, Berlin (1991), 482–489.

[10] S. Gupta, G. Longobardi and R. Trombetti: On the equivalence issue of a class of 2-dimensional linear Maximum Rank Distance codes. arXiv:2208.09701.

[11] R. Hartshorne: *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer-Verlag, New York-Heidelberg (1977).

[12] A. Kshevetskiy and E. Gabidulin: The new construction of rank codes, *International Symposium on Information Theory* (2005), 2105–2108.

[13] D. Liebhold and G. Nebe: Automorphism groups of Gabidulin-like codes, *Arch. Math. (Basel)* **107 (4)** (2016), 355–366.

[14] G. Lunardon, R. Trombetti and Y. Zhou: On kernels and nuclei of rank metric codes, *J. Algebraic Combin.* **46 (2)** (2017), 313–340.

[15] M. Montanucci and C. Zanella: A class of linear sets in $\mathrm{PG}(1, q^5)$, *Finite Fields Appl.* **78** (2022), 101983.

[16] E.H. Moore, A two-fold generalization of Fermat's theorem, *Bull. Am. Math. Soc.* **2 (7)** (1986), 189–199.

[17] A. Neri, P. Santonastaso and F. Zullo: Extending two families of maximum rank distance codes, *Finite Fields Appl.* **81** (2022), 102045.

[18] 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.

[19] O. Polverino and F. Zullo: Connections between scattered linear sets and MRD-codes, *Bull. Inst. Combin. Appl.* **89** (2020), 46–74.

[20] O. Polverino and F. Zullo: On the number of roots of some linearized polynomials, *Linear Algebra Appl.* **601** (2020), 189–218.

[21] R. M. Roth: Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inform. Theory* **37 (2)** (1991), 328–336.

[22] I. R. Shafaverich: *Basic Algebraic Geometry 1: Varieties in Projective Space*, Second edition, Springer, Heidelberg (1994).

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

[24] 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).

[25] D. Silva, F. R. Kschischang and R. Koetter: A rank-metric approach to error control in random network coding, *IEEE Trans. Inform. Theory* **54 (9)** (2008), 3951–3967.

[26] H. Stichtenoth: *Algebraic function fields and codes*, Graduate Texts in Mathematics **254**, Second edition, Springer, Berlin (2009).

[27] G. Zini and F. Zullo: Scattered subspaces and related codes, *Des. Codes Cryptogr.* **89 (8)** (2021), 1853–1873.

MARCO TIMPANELLA, Università degli Studi di Perugia, Dipartimento di Matematica e Informatica, Via Vanvitelli, 1, 06123 Perugia PG, Italy

Email address: `marco.timpanella@unipg.it`

GIOVANNI ZINI, Università degli Studi di Modena e Reggio Emilia, Dipartimento di Scienze Fisiche, Informatiche e Matematiche, Via Campi, 213/b Modena MO, Italy

Email address: `giovanni.zini@unimore.it`