Combinatorica (2023) 43:681–716
https://doi.org/10.1007/s00493-023-00030-x

ORIGINAL PAPER

A Large Family of Maximum Scattered Linear Sets of PG$(1, q^n)$ and Their Associated MRD Codes

G. Longobardi[1] · Giuseppe Marino[1] · Rocco Trombetti[1] · Yue Zhou[2]

Received: 18 November 2021 / Revised: 26 September 2022 / Accepted: 1 February 2023 /
Published online: 13 June 2023

Abstract

Linear sets in projective spaces over finite fields were introduced by Lunardon (Geom Dedic 75(3):245–261, 1999) and they play a central role in the study of blocking sets, semifields, rank-metric codes, etc. A linear set with the largest possible cardinality and rank is called maximum scattered. Despite two decades of study, there are only a limited number of maximum scattered linear sets of a line $\mathrm{PG}(1, q^n)$. In this paper, we provide a large family of new maximum scattered linear sets over $\mathrm{PG}(1, q^n)$ for any even $n \geq 6$ and odd q. In particular, the relevant family contains at least

$$\begin{cases} \left\lfloor \frac{q^t+1}{8rt} \right\rfloor, & \text{if } t \not\equiv 2 \pmod 4; \\ \left\lfloor \frac{q^t+1}{4rt(q^2+1)} \right\rfloor, & \text{if } t \equiv 2 \pmod 4, \end{cases}$$

inequivalent members for given $q = p^r$ and $n = 2t > 8$, where $p = \mathrm{char}(\mathbb{F}_q)$. This is a great improvement of previous results: for given q and $n > 8$, the number of inequivalent maximum scattered linear sets of $\mathrm{PG}(1, q^n)$ in all classes known so far, is smaller than $q^2\phi(n)/2$, where ϕ denotes Euler's totient function. Moreover, we show that there are a large number of new maximum rank-distance codes arising from the constructed linear sets.

✉ Giuseppe Marino
giuseppe.marino@unina.it

G. Longobardi
giovanni.longobardi@unina.it

Rocco Trombetti
rtrombet@unina.it

Yue Zhou
yue.zhou.ovgu@gmail.com

[1] Dipartimento di Matematica e Applicazioni "Renato Caccioppoli", Università degli Studi di Napoli Federico II, Via Vicinale Cupa Cintia, 80126 Naples, Italy

[2] Department of Mathematics, National University of Defense Technology, Changsha 410073, China

Keywords Linear set · Linearized polynomial · Rank-metric code

Mathematics Subject Classification 94B05 · 51E20 · 94B27

1 Introduction

Let V be a vector space over $\mathbb{F}_{q^n}$ of dimension r and $\Omega = \mathrm{PG}(V, q^n) = \mathrm{PG}(e-1, q^n)$. A set of points L_U of Ω is called an $\mathbb{F}_q$*-linear set* of *rank* k if it consists of the points defined by the non-zero elements of an $\mathbb{F}_q$-subspace U of V of dimension k, that is,

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

The term *linear* was introduced by Lunardon [19] who considered a special kind of blocking sets. In the past two decades after this work, linear sets have been intensively investigated and applied to construct and characterize various objects in finite geometry, such as blocking sets, two-intersection sets, translation spreads of the Cayley generalized Hexagon, translation ovoids of polar spaces, semifields and rank-metric codes. We refer to [1, 16, 25–27] and the references therein.

The most interesting linear sets are those satisfying certain extremal properties. Firstly, it is clear that $|L_U| \leq \frac{q^k-1}{q-1}$. When the equality is achieved, L is called *scattered*. A scattered linear set L_U of Ω with largest possible rank k is called a *maximum scattered linear set*. In [6], it is proved that the largest possible rank is $k = en/2$ if e is even, and $(en - n)/2 \leq k \leq en/2$ if e is odd. In particular, when $e = 2$, i.e. L_U is a maximum scattered linear set over a projective line, its rank k equals n.

For a given linear set L_U of rank n of a projective line, by a suitable collineation of $\mathrm{PG}(1, q^n)$, we may always assume that the point $\langle (0, 1) \rangle_{\mathbb{F}_{q^n}}$ is not in L_U. This means

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

for a q*-polynomial* $f(x)$ over $\mathbb{F}_{q^n}$; i.e. an element of the set

$$\mathcal{L}_{n,q}[x] = \left\{ \sum_{i=0}^{n-1} c_i x^{q^i} : c_i \in \mathbb{F}_{q^n} \right\}.$$

Since polynomials in this set define $\mathbb{F}_q$-linear maps of $\mathbb{F}_{q^n}$ seen as an $\mathbb{F}_q$-vector space, they are also known in the literature as *linearized polynomials*. Given a q-polynomial f, we use L_f to denote the linear set defined by U_f. It is not difficult to show that L_f is scattered if and only if for any $z, y \in \mathbb{F}_{q^n}^*$ the condition

$$\frac{f(z)}{z} = \frac{f(y)}{y}$$

implies that z and y are $\mathbb{F}_q$-linearly dependent. Hence, a q-polynomial satisfying this condition is usually called a *scattered polynomial* (over $\mathbb{F}_{q^n}$), see [27]. The condition

Table 1 Numbers of inequivalent $\mathcal{C}_f$ and $P\Gamma L(2, q^n)$-inequivalent L_f, where f is a scattered polynomial in (i), (ii) or (iii), $q = p^r$ with $p = \mathrm{char}(\mathbb{F}_q)$ and ϕ denotes Euler's totient function

No	Families	# inequivalent $\mathcal{C}_f$	# inequivalent L_f
(i)	Pseudo-regulus	$\phi(n)/2$	1
(ii)	Lunardon–Polverino	$\le \begin{cases} \phi(n)\frac{q-2}{2} & 2 \nmid n \\ \phi(n)\frac{q^2+p-4}{4} & 2 \mid n, \end{cases}$	$\le \begin{cases} \phi(n)\frac{q-2}{2} & 2 \nmid n \\ \phi(n)\frac{q^2+p-4}{4} & 2 \mid n, \end{cases}$
(iii)	Longobardi–Zanella	$\phi(n)/2$	$\le \phi(n)/2$

for a q-polynomial $f(x)$ to be scattered can be rephrased by saying that if $f(\gamma x) = \gamma f(x)$, for x and $\gamma \in \mathbb{F}_{q^n}$ with $x \neq 0$, then $\gamma \in \mathbb{F}_q$.

Scattered polynomials are also strongly related to maximum rank-distance (MRD, for short) codes. Given a scattered polynomial f, the set of q-polynomials

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

defines a linear MRD code of minimum distance $n - 1$ over $\mathbb{F}_q$. For recent surveys on MRD codes and their relations with linear sets, we refer to [26, 28].

Up to now, there are only three families of maximum scattered linear sets in $\mathrm{PG}(1, q^n)$ for infinitely many n. We list the corresponding scattered polynomials over $\mathbb{F}_{q^n}$ below:

(i) x^{q^s}, where $1 \le s \le n - 1$ and $\gcd(s, n) = 1$; see [6].

(ii) $\delta x^{q^s} + x^{q^{n-s}}$, where $n \ge 4$, $N_{q^n/q}(\delta) \notin \{0, 1\}$, $\gcd(s, n) = 1$ and $N_{q^n/q} : x \in \mathbb{F}_{q^n} \mapsto x^{\frac{q^n-1}{q-1}} \in \mathbb{F}_q$, is the norm function of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$; see [20, 27].

(iii) $\psi^{(k)}(x)$, where $\psi(x) = \frac{1}{2}\left(x^q + x^{q^{t-1}} - x^{q^{t+1}} + x^{q^{2t-1}}\right)$, q odd, $n = 2t$ and
- t is even and $\gcd(k, t) = 1$, or
- t is odd, $\gcd(k, 2t) = 1$, and $q \equiv 1 \pmod 4$; see [18].

For $n \in \{6, 8\}$, there are other families of scattered polynomials over $\mathbb{F}_{q^n}$; see [4, 9, 10, 23, 31]. According to the asymptotic classification results of them obtained in [2, 3, 5, 13], maximum scattered linear sets in $\mathrm{PG}(1, q^n)$ seem rare.

Two linear sets L_U and $L_{U'}$ of $\mathrm{PG}(1, q^n)$ are said to be *$P\Gamma L$-equivalent* (or *projectively equivalent*) if there exists $\varphi \in P\Gamma L(2, q^n)$ such that $L_U^{\varphi} = L_{U'}$. For two given q-polynomials, it is well-known that $\mathcal{C}_f$ is equivalent to $\mathcal{C}_g$ if and only if U_f and U_g are on the same $\Gamma L(2, q^n)$-orbit (see Theorem 2.1), which further implies that L_f and L_g are $P\Gamma L$-equivalent. However, the converse statement is not true in general. For instance, if $U_f = \left\{(x, x^q) : x \in \mathbb{F}_{q^n}\right\}$ and $U_g = \left\{(x, x^{q^s}) : x \in \mathbb{F}_{q^n}\right\}$ with $s \neq 1, n - 1$ and $\gcd(s, n) = 1$, then U_f and U_g are not $\Gamma L(2, q^n)$-equivalent, but obviously $L_f = \left\{\langle(1, x^{q-1})\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\right\} = L_g$. For more results on the equivalence problems, we refer to [8, 11].

In Table 1, we list the numbers of inequivalent $\mathcal{C}_f$ and $P\Gamma L(2,q^n)$-inequivalent L_f, for a scattered polynomial f in each one of the three known families. The proof of what is stated in Table 1 will be provided in Sect. 2.

In this paper, we present a new family of maximum scattered linear sets in $\mathrm{PG}(1,q^n)$ where $q=p^r$, p is an odd prime and $n=2t\geq 6$; see Theorem 3.1. In particular, when $t>4$, this new family provides at least

$$\begin{cases} \left\lfloor \frac{q^t+1}{4rt} \right\rfloor, & \text{if } t \not\equiv 2 \pmod 4; \\ \left\lfloor \frac{q^t+1}{2rt(q^2+1)} \right\rfloor, & \text{if } t \equiv 2 \pmod 4 \end{cases}$$

inequivalent number of MRD codes (Corollary 4.3) and at least

$$\begin{cases} \left\lfloor \frac{q^t+1}{8rt} \right\rfloor, & \text{if } t \not\equiv 2 \pmod 4; \\ \left\lfloor \frac{q^t+1}{4rt(q^2+1)} \right\rfloor, & \text{if } t \equiv 2 \pmod 4 \end{cases}$$

$P\Gamma L(2,q^n)$-inequivalent maximum linear sets (Theorem 5.1). Therefore, the number of maximum scattered linear sets in $\mathrm{PG}(1,q^n)$ (and hence of MRD codes) grows exponentially with respect to n.

The remaining part of this paper is organized as follows. In Sect. 2, we introduce more results on the equivalence of maximum scattered linear sets in $\mathrm{PG}(1,q^n)$ and the associated MRD codes, and explain Table 1 in details. In Sect. 3, we exhibit a family of polynomials f over $\mathbb{F}_{q^n}$, and prove that they are scattered. The equivalence between the MRD codes $\mathcal{C}_f$ associated to the members of this family are completely determined in Sect. 4, in which we also study the MRD codes derived from the adjoint maps of our scattered polynomials. Based on these results, the $P\Gamma L$-equivalence of the associated maximum linear sets are investigated in Sect. 5.

2 Equivalence of MRD Codes and Linear Sets

A *rank-distance code* (or RD code for short) $\mathcal{C}$ is a subset of the set of $m\times n$ matrices $\mathbb{F}_q^{m\times n}$ over $\mathbb{F}_q$ endowed with the rank distance

$$d(A,B)=\mathrm{rk}(A-B)$$

for any $A,B\in\mathbb{F}_q^{m\times n}$. The *minimum distance* of an RD code $\mathcal{C}$, $|\mathcal{C}|\geq 2$, is defined as

$$d(\mathcal{C})=\min_{\substack{M,N\in\mathcal{C}\\ M\neq N}} d(M,N).$$

A rank-distance code of $\mathbb{F}_q^{m\times n}$ with minimum distance d has *parameters* $(m,n,q;d)$. If $\mathcal{C}$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m\times n}$, then $\mathcal{C}$ is called $\mathbb{F}_q$-*linear* RD code and its *dimension* $\dim_{\mathbb{F}_q}\mathcal{C}$ is defined to be the dimension of $\mathcal{C}$ as a subspace over $\mathbb{F}_q$. The

Singleton-like bound [12] for an $(m, n, q; d)$ RD-code $\mathcal{C}$ is

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

If $\mathcal{C}$ attains this size, then $\mathcal{C}$ is a called *Maximum Rank-Distance code*, MRD *code* for short. In this paper we will consider only the case in which the codewords are square matrices, i.e. $m = n$. Note that if $n = d$, then an MRD code $\mathcal{C}$ consists of q^n invertible endomorphisms of $\mathbb{F}_{q^n}$; such $\mathcal{C}$ is called *spread set* of $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$. In particular if $\mathcal{C}$ is $\mathbb{F}_q$-linear, it is called a *semifield spread set* of $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$, see [15]. Two $\mathbb{F}_q$-linear codes $\mathcal{C}$ and $\mathcal{C}'$ are called *equivalent* if there exist $A, B \in \mathrm{GL}(n, q)$ and a field automorphism σ of $\mathbb{F}_q$ such that

$$\mathcal{C}' = \{AC^{\sigma}B \colon C \in \mathcal{C}\}.$$

The aforementioned link lies in the fact that rank-distance codes can be described by means of q-polynomials over $\mathbb{F}_{q^n}$, considered modulo $x^{q^n} - x$. After fixing an ordered $\mathbb{F}_q$-basis $\{b_1, b_2, \ldots, b_n\}$ for $\mathbb{F}_{q^n}$ it is possible to give a bijection Φ which associates for each matrix $M \in \mathbb{F}_q^{n\times n}$ a unique q-polynomial $f_M \in \mathcal{L}_{n,q}[x]$. More precisely, put $\mathbf{b} = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_{q^n}^n$, then $\Phi(M) = f_M$ where for each $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ we have $f_M(\mathbf{b}\cdot\mathbf{u}) = \mathbf{b}\cdot\mathbf{u}M$.

For a scattered polynomial f, as the kernel of the $\mathbb{F}_q$-linear map $z \mapsto az+bf(z)$ is of dimension at most 1 for any $a, b \in \mathbb{F}_{q^n}$ with $(a, b) \ne (0, 0)$, the set of q-polynomials

$$\mathcal{C}_f = \left\{ax + bf(x) : a, b \in \mathbb{F}_{q^n}\right\}$$

defines a linear MRD code of minimum distance $n - 1$ over $\mathbb{F}_q$.

Given two scattered polynomials f and g over $\mathbb{F}_{q^n}$, the corresponding MRD codes $\mathcal{C}_f$ and $\mathcal{C}_g$ are equivalent if and only if there exists a triple (L_1, L_2, σ), with L_1, $L_2 \in \mathcal{L}_{n,q}[x]$ permuting $\mathbb{F}_{q^n}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ such that

$$L_1 \circ \varphi^{\sigma} \circ L_2 \in \mathcal{C}_g \text{ for all } \varphi \in \mathcal{C}_f,$$

where $\circ$ stands for the composition of maps and $\varphi^{\sigma}(x) = \sum a_i^{\sigma} x^{q^i}$ for $\varphi(x) = \sum a_i x^{q^i}$. If $f = g$, the set of the triples defined as above is a group which is called the *automorphism group* of the code $\mathcal{C}_f$ and it is denoted by $\mathrm{Aut}(\mathcal{C}_f)$.

The following result concerning the equivalence of MRD codes associated with scattered polynomials is proved in [27].

Theorem 2.1 *Let f and g be two scattered polynomials over $\mathbb{F}_{q^n}$, respectively. The MRD-codes $\mathcal{C}_f$ and $\mathcal{C}_g$ are equivalent if and only if U_f and U_g are $\Gamma L(2, q^n)$-equivalent.*

For two scattered polynomials f and g, by Theorem 2.1 and the definition of $P\Gamma L$-equivalence of linear sets, if $\mathcal{C}_f$ and $\mathcal{C}_g$ are equivalent, then L_f and L_g are also $P\Gamma L$-equivalent. The converse does not hold, see [11].

For this paper, we only need the necessary and sufficient conditions in Theorem 2.1 to interpret the equivalence problem in Sect. 4. However, in general, the equivalence problem for MRD codes could be more complicated. We refer to the surveys [26, 28] for its precise definition and related results. See [7] for the hardness of testing the equivalence between rank-distance codes. The *left idealizer* and the *right idealizer* of any given rank-distance code $\mathcal{C}$ are invariant under equivalence. These two concepts were introduced in [17], and in [21] with different names. If a rank-distance code $\mathcal{C}$ is given as a subset of $\mathcal{L}_{n,q}[x]$, then its left idealizer and right idealizer are defined as

$$I_L(\mathcal{C}) = \{\varphi \in \mathcal{L}_{n,q}[x] : \varphi \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\},$$

and

$$I_R(\mathcal{C}) = \{\varphi \in \mathcal{L}_{n,q}[x] : f \circ \varphi \in \mathcal{C} \text{ for all } f \in \mathcal{C}\},$$

respectively. When $\mathcal{C}$ is an MRD-code, it is well known that all nonzero elements in $I_L(\mathcal{C})$ and $I_R(\mathcal{C})$ are invertible and each of the idealizers must be a subfield of $\mathbb{F}_{q^n}$. In particular, if $\mathcal{C}$ is an $\mathbb{F}_{q^n}$-subspace of $\mathcal{L}_{n,q}[x]$, then $I_L(\mathcal{C})$ is isomorphic to $\mathbb{F}_{q^n}$ and $\mathcal{C}$ is said to be an *$\mathbb{F}_{q^n}$-linear MRD code*.

Obviously, for every MRD code $\mathcal{C}_f$ associated with a scattered polynomial f over $\mathbb{F}_{q^n}$, its left idealizer

$$I_L(\mathcal{C}_f) = \left\{\alpha x : x \in \mathbb{F}_{q^n}\right\}, \tag{1}$$

clearly isomorphic to $\mathbb{F}_{q^n}$.

For a q-polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ over $\mathbb{F}_{q^n}$, the *adjoint map* $\hat{f}$ of it with respect to the bilinear form $\langle x, y\rangle = \mathrm{Tr}_{q^n/q}(xy)$ is

$$\hat{f}(x) = a_0 x + \sum_{i=1}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}.$$

For a given scattered polynomial f over $\mathbb{F}_{q^n}$, its adjoint $\hat{f}$ is a scattered polynomial over $\mathbb{F}_{q^n}$ as well, and U_f and $U_{\hat{f}}$ (and hence $\mathcal{C}_f$ and $\mathcal{C}_{\hat{f}}$) are not necessarily equivalent. However, they define exactly the same linear set of $\mathrm{PG}(1, q^n)$; see [1, Lemma 2.6] and [8, Lemma 3.1]. This also implies that $\mathcal{C}_f$ and $\mathcal{C}_{\hat{f}}$ are both MRD-codes.

To investigate the $P\Gamma L$-equivalence among linear sets of a line, we need the following result

Lemma 2.2 [8, Lemma 3.6] *Let $f(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i}$ and $g(x) = \sum_{i=0}^{n-1} \beta_i x^{q^i}$ be two q-polynomials over $\mathbb{F}_{q^n}$ such that $L_f = L_g$. Then*

(a) $\alpha_0 = \beta_0$,

(b) $\alpha_k \alpha_{n-k}^{q^k} = \beta_k \beta_{n-k}^{q^k}$ *for* $k = 1, 2, \cdots, n-1$,

(c) $\alpha_1 \alpha_{k-1}^{q} \alpha_{n-k}^{q^k} + \alpha_k \alpha_{n-1}^{q} \alpha_{n-k+1}^{q^k} = \beta_1 \beta_{k-1}^{q} \beta_{n-k}^{q^k} + \beta_k \beta_{n-1}^{q} \beta_{n-k+1}^{q^k}$, *for* $k = 2, 3, \cdots, n-1$.

In the following we provide details on the estimates stated in Table 1 for the three families.

Family (i) The number of inequivalent MRD codes defined in (i) comes from the well-known results on the equivalence of Delsarte–Gabidulin codes and their generalizations; see [22, Theorem 4.4] for instance. Moreover all monomials $f(x) = x^{q^s}$ with $\gcd(s, n) = 1$, determine the same linear set in $\mathrm{PG}(1, q^n)$; in fact,

$$L_f := \left\{\left\langle\left(1, x^{q^s-1}\right)\right\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\right\};$$

the so-called linear set of pseudo-regulus type.

Family (ii) For the number of inequivalent MRD defined in (ii), we need more complicated analysis. Firstly, we state the following result which is a special case of [22, Theorem 4.4].

Proposition 2.3 *For $\theta, \eta \in \mathbb{F}_{q^n}$ such that $N_{q^n/q}(\theta), N_{q^n/q}(\eta) \notin \{0, 1\}$, with $1 \leq s, t \leq \frac{n-1}{2}$ satisfying $\gcd(s, n) = 1$, let $f(x) = \eta x^{q^s} + x^{q^{n-s}}$ and $g(x) = \theta x^{q^t} + x^{q^{n-t}}$. Then $\mathcal{C}_f$ and $\mathcal{C}_g$ are equivalent if and only if $s = t$ and*

$$\theta = \eta^\tau z^{q^{2s}-1}$$

for some $\tau \in \mathrm{Aut}(\mathbb{F}_{q^n})$ and $z \in \mathbb{F}_{q^n}^*$.

By Hilbert's Theorem 90, if $m|n$, $\{x \in \mathbb{F}_{q^n}^* : N_{q^n/q^m}(x) = 1\} = \{y^{q^m-1} : y \in \mathbb{F}_{q^n}^*\}$. As

$$\gcd(q^{2s} - 1, q^n - 1) = q^{\gcd(2s,n)} - 1 = q^{\gcd(2,n)} - 1 = \begin{cases} q^2 - 1, & 2 \mid n, \\ q - 1, & 2 \nmid n, \end{cases}$$

if $N_{q^n/q^{\gcd(2,n)}}(\theta) = N_{q^n/q^{\gcd(2,n)}}(\eta)$, then we can always find $z \in \mathbb{F}_{q^n}^*$ such that $\theta = \eta z^{q^{2s}-1}$. Hence, under the maps $\eta \mapsto \eta z^{q^{2s}-1}$ for $z \in \mathbb{F}_{q^n}^*$, the elements in $\mathbb{F}_{q^n}^*$ are partitioned into $q^{\gcd(2,n)} - 1$ orbits. Moreover, θ and η are in the same orbit under the maps $\eta \mapsto \eta^\tau z^{q^{2s}-1}$ for $z \in \mathbb{F}_{q^n}^*$ and $\tau \in \mathrm{Aut}(\mathbb{F}_{q^n})$ if and only if $N_{q^n/q^{\gcd(2,n)}}(\theta) = \left(N_{q^n/q^{\gcd(2,n)}}(\eta)\right)^{\tau'}$ for some $\tau' \in \mathrm{Aut}(\mathbb{F}_{q^{\gcd(2,n)}})$, which implies that $N_{q^n/q^{\gcd(2,n)}}(\theta)$ and $N_{q^n/q^{\gcd(2,n)}}(\eta)$ must belong either to $\mathbb{F}_p \setminus \{0, 1\}$ or to $F(m)$ for some $m \,|\, r \cdot \gcd(2, n)$, where $m > 1$ and

$$F(m) = \left\{x \in \mathbb{F}_{p^m} : x \notin \mathbb{F}_{p^k} \text{ with } k < m, k \mid m\right\}.$$

Therefore, the total number $\Theta(q, n)$ of inequivalent MRD codes in family (ii) for given $q = p^r$ and n, where $p = \mathrm{char}(\mathbb{F}_q)$, is

$$\Theta(q, n) = \left(\sum_{j|r\cdot\gcd(2,n), j\neq1} \frac{|F(j)|}{j} + (p - 2)\right) \frac{\phi(n)}{2}.$$

By computation, we have

$$\sum_{j|r\cdot\gcd(2,n),\, j\neq 1} \frac{|F(j)|}{j} + (p-2) \le \begin{cases} \sum_{j|r, j\neq 1} |F(j)| + (p-2), & 2 \nmid n, \\ \frac{1}{2}\sum_{j|2r, j\neq 1} |F(j)| + (p-2), & 2 \mid n, \end{cases}$$

$$= \begin{cases} q-2, & 2 \nmid n, \\ \frac{1}{2}\left(q^2-p\right) + p - 2, & 2 \mid n. \end{cases}$$

As a consequence, we can derive the following upper bound for $\Theta(q, n)$:

$$\Theta(q,n) \le \begin{cases} (q-2)\frac{\phi(n)}{2}, & 2 \nmid n, \\ \frac{q^2+p-4}{2}\frac{\phi(n)}{2}, & 2 \mid n. \end{cases} \tag{2}$$

One can also derive a lower bound

$$\Theta(q,n) \ge \begin{cases} \frac{q-2}{r}\frac{\phi(n)}{2}, & 2 \nmid n, \\ \frac{q^2-q}{2r}\frac{\phi(n)}{2}, & 2 \mid n. \end{cases}$$

Note that for q large most choices of θ satisfying $N_{q^n/q}(\theta) \notin \{0, 1\}$, $N_{q^n/q^{\gcd(s,n)}}(\theta)$ is not in any proper subfield of $\mathbb{F}_{q^{\gcd(s,n)}}$. Therefore, $\Theta(n, q)$ is asymptotically close to the above lower bound when q is getting large. By (2), we get an upper bound on the number of inequivalent $\mathcal{C}_f$ in family (ii) in Table 1.

Let $\Lambda(n, q)$ be the number of $P\Gamma L$-inequivalent Lunardon–Polverino linear sets over $\mathrm{PG}(1, q^n)$. Clearly, the upper bound for $\Theta(n, q)$ is an upper bound for $\Lambda(n, q)$, but, actually, this could be smaller. In [10, Section 3], $\Lambda(n, q)$ is determined for $n = 6, 8$. The precise value of $\Lambda(n, q)$ for all $n \ge 3$ can be found in a recent preprint [30, Section 4]. The value of $\Lambda(n, q)$ is approximately $\frac{q\phi(n)}{4r}$ for odd n and $\frac{q^2\phi(n)}{8r}$ for even n provided that q is large enough.

Family (iii) Regarding (iii) in Table 1, for fixed q and n, there are exactly $\phi(n)/2$ inequivalent MRD-codes derived from this family of scattered polynomials; see [18, Theorem 5.4]. The precise number of $P\Gamma L$-inequivalent linear sets provided by it is still unknown, but it is obviously smaller than or equal to $\phi(n)/2$.

3 Construction

Inspired by the results obtained in [18] where polynomials $\psi^{(k)}(x)$ defined in (iii) were introduced, and their scatteredness proven, we investigate here a similar problem for a natural generalization of these examples.

Precisely, set $n = 2t$, $t \ge 3$ and let q be an odd prime power. We consider the following q-polynomials:

$$\psi_{h,t}(x) = x^q + x^{q^{t-1}} - h^{1-q^{t+1}}x^{q^{t+1}} + h^{1-q^{2t-1}}x^{q^{2t-1}} \in \mathbb{F}_{q^n}[x] \tag{3}$$

where $h \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^t}$ and $h^{q^t+1} = -1$.

First we note that if $t = 3$ in (3), then $\psi_{h,3}(x)$ are the scattered polynomials and they are the adjoint polynomials of those constructed by Bartoli et al. in [4].

Furthermore, if we allow $h \in \mathbb{F}_{q^t}$, since $-1 = h^{q^t+1} = h^2$, then $h \in \mathbb{F}_{q^2}$. Then we may distinguish two cases:

(a) $q \equiv 1 \pmod 4$. In this case $h \in \mathbb{F}_q$ and $\psi_{h,t}(x)$ becomes

$$x^q + x^{q^{t-1}} - x^{q^{t+1}} + x^{q^{2t-1}}.$$

This polynomial was proven to be scattered for each $t \geq 3$ in [18].

(b) $q \equiv 3 \pmod 4$. In this case $h \in \mathbb{F}_{q^2}$ and $h^q = -h$; hence, t must be even and $\psi_{h,t}(x)$ becomes

$$x^q + x^{q^{t-1}} + x^{q^{t+1}} - x^{q^{2t-1}}.$$

Also, this polynomial was proven to be scattered in [18].

In this section, our goal is to prove the following main result.

Theorem 3.1 *Let $n = 2t$, $t \geq 3$ and let q be an odd prime power. For each $h \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^t}$ such that $h^{q^t+1} = -1$, the $\mathbb{F}_q$-linearized polynomial $\psi_{h,t}(x)$ is scattered.*

Now we note that polynomials described in (3) can be rewritten in the following fashion:

$$\psi_{h,t}(x) = L(x) + M(x), \tag{4}$$

where $L(x) = x^q - h^{1-q^{t+1}} x^{q^{t+1}}$ and $M(x) = x^{q^{t-1}} + h^{1-q^{2t-1}} x^{q^{2t-1}}$.

It is straightforward to see that $L(x)$ and $M(x)$ are $\mathbb{F}_{q^t}$-semilinear maps of $\mathbb{F}_{q^n}$ with companion automorphisms $x \mapsto x^q$ and $x \mapsto x^{q^{t-1}}$, respectively. Moreover, we have that

$$\ker L = \left\{ x \in \mathbb{F}_{q^n} : x - h^{q^{2t-1}-q^t} x^{q^t} = 0 \right\} \tag{5}$$

and similarly

$$\ker M = \left\{ x \in \mathbb{F}_{q^n} : x + h^{q^{t+1}-q^t} x^{q^t} = 0 \right\}. \tag{6}$$

In addition, since $h^{q^t+1} = -1$, we have

$$\begin{aligned} L(x)^{q^t} &= \left(x^q - h^{1-q^{t+1}} x^{q^{t+1}} \right)^{q^t} = x^{q^{t+1}} - h^{q^t-q} x^q \\ &= -h^{q^t-q} \left(x^q - h^{1-q^{t+1}} x^{q^{t+1}} \right) = -h^{q^t-q} L(x) \end{aligned}$$

and similarly, we may prove that $M(x)^{q^t} = h^{q^t-q^{t-1}} M(x)$. Hence, we obtain that

$$\operatorname{im} L = \left\{z \in \mathbb{F}_{q^{2t}} : z^{q^t} + h^{q^t-q} z = 0\right\} \tag{7}$$

and

$$\operatorname{im} M = \left\{z \in \mathbb{F}_{q^{2t}} : z^{q^t} - h^{q^t-q^{t-1}} z = 0\right\}. \tag{8}$$

Clearly, the sets in (5), (6), (7) and (8) are 1-dimensional $\mathbb{F}_{q^t}$-subspaces of $\mathbb{F}_{q^n}$.

Proposition 3.2 *Let $n = 2t$, $t \geq 1$ and let $h \in \mathbb{F}_{q^{2t}}$ be such that $h^{q^t+1} = -1$. Then $h^{q^2+1} \neq 1$ and $h^{q^{t-2}} \neq -h$.*

Proof First, as q is odd, $\gcd(q^2+1, q^{2t}-1) = 2$ if t is odd, and

$$\gcd\left(q^2+1, q^t+1\right) = \begin{cases} 2, & t \equiv 0 \pmod 4; \\ q^2+1, & t \equiv 2 \pmod 4. \end{cases}$$

Assume on the contrary that $h^{q^2+1} = 1$. Together with $h^{q^t+1} = -1$ and the above GCD conditions, we deduce the following results.

If t is odd, then $h^2 = 1$ which contradicts $h^{q^t+1} = -1$. If $4 \mid t$, then $h^2 = -1$ which implies $h^{q^2+1} = -1$ contradicting the assumption. If $2 \mid t$ but $4 \nmid t$, then $h^{q^t+1} = 1$ contradicting $h^{q^t+1} = -1$.

From $h^{q^t+1} = -1$ and $h^{q^2+1} \neq 1$, we finally derive $h^{q^{t-2}} \neq -h$ directly. □

Proposition 3.3 *Let $n = 2t$ with $t \geq 3$. The finite field $\mathbb{F}_{q^n}$, seen as $\mathbb{F}_{q^t}$-vector space, is both the direct sum of* $\ker L$ *and* $\ker M$*, and of* $\operatorname{im} L$ *and* $\operatorname{im} M$*.*

Proof Since $\ker L$ and $\ker M$ are 1-dimensional $\mathbb{F}_{q^t}$-subspaces of $\mathbb{F}_{q^n}$, it is enough to prove that $\ker L \cap \ker M = \{0\}$. In this regard, let $u \in \ker L \cap \ker M$. By (5) and (6), we get $h^{q^{2t-1}} = -h^{q^{t+1}}$, i.e. $(h^{q^{t-2}})^{q^{t+1}} = -h^{q^{t+1}}$. Since $h^{q^t+1} = -1$, we get $h^{q^{t-2}} = -h$, contradicting Proposition 3.2.

Taking into account (7) and (8), a similar argument shows that the additive group of $\mathbb{F}_{q^n}$, seen as $\mathbb{F}_{q^t}$-vector space, can be also written as $\operatorname{im} L \oplus \operatorname{im} M$. □

Consider now the following $\mathbb{F}_{q^t}$-linear maps of $\mathbb{F}_{q^n}$

$$R(x) = x^{q^t} + h^{q^{t-1}-q} x \quad \text{and} \quad T(x) = x^{q^t} + h^{q-q^{t-1}} x. \tag{9}$$

It is straightforward to see that $\dim_{\mathbb{F}_{q^t}} \ker R = \dim_{\mathbb{F}_{q^t}} \ker T = 1$; moreover, $\ker T = h^{q^{t-1}-q} \ker R$, moreover by the same argument that we use above, one gets that

$$\operatorname{im} R = \left\{z \in \mathbb{F}_{q^n} : z^{q^t} - h^{q-q^{t-1}} z = 0\right\}$$

and

$$\operatorname{im} T = \left\{z \in \mathbb{F}_{q^n} : z^{q^t} - h^{q^{t-1}-q} z = 0\right\},$$

obtaining that $\operatorname{im} T = h^{q-q^{t-1}} \operatorname{im} R$.

Lemma 3.4 *Let $\rho, \tau \in \mathbb{F}_{q^n}^*$, $n = 2t$ and $t \geq 3$ be such that $\rho \in \ker R$ and $\tau \in \ker T$. Then*

(i) *$\{1, \rho\}$ and $\{1, \tau\}$ are $\mathbb{F}_{q^t}$-bases of $\mathbb{F}_{q^n}$.*

(ii) *If $\tau = h^{q^{t-1}-q}\rho$ and an element $\gamma \in \mathbb{F}_{q^n}$ has components (λ_1,μ_1) in the ordered $\mathbb{F}_{q^t}$-basis $\{1, \rho\}$, then the components of γ in the ordered $\mathbb{F}_{q^t}$-basis $\{1, \tau\}$ are*

$$\left(\lambda_1 + \mu_1\rho\left(1 - h^{q^{t-1}-q}\right), \mu_1\right). \tag{10}$$

Proof (i) It is enough showing that ρ and τ are not in $\mathbb{F}_{q^t}$. We will show that $\rho \notin \mathbb{F}_{q^t}$. A similar argument can be applied to τ as well. Suppose that $\rho \in \mathbb{F}_{q^t}$, then $\rho^{q^t-1} = 1$. Then, by hypothesis,

$$1 = \rho^{q^t-1} = -h^{q^{t-1}-q}.$$

Hence $h^{q^{t-2}} = -h$ which, by Proposition 3.2, is not the case.

(ii) Let $\gamma \in \mathbb{F}_{q^n}$ and suppose that $\gamma = \lambda_1 + \mu_1\rho$ with $\lambda_1, \mu_1 \in \mathbb{F}_{q^t}$. Also, denote by λ_2 and μ_2 the components of γ in the $\mathbb{F}_{q^t}$-basis $\{1, \tau\}$. Of course, we have

$$\lambda_2 + \mu_2\tau = \lambda_1 + \mu_1\rho \tag{11}$$

Raising (11) to the q^t-th power, and taking into account that $\rho \in \ker R$ and $\tau \in \ker T$, we get the following linear system in the unknowns λ_2 and μ_2

$$\begin{cases} \lambda_2 + \mu_2\tau = \lambda_1 + \mu_1\rho \\ \lambda_2 - \mu_2 h^{q-q^{t-1}}\tau = \lambda_1 - \mu_1 h^{q^{t-1}-q}\rho. \end{cases}$$

Clearly, this linear system has a unique solution; i.e.,

$$\lambda_2 = \lambda_1 + \mu_1\rho\left(1 - h^{q^{t-1}-q}\right) \quad \text{and} \quad \mu_2 = \mu_1.$$

Hence, the assertion follows. □

Proposition 3.5 *For any nonzero vectors $u \in \ker L$, $v \in \ker M$ and any $a \in \mathbb{F}_{q^n}$, the following statements are equivalent:*

(i) *$a \in \ker R$;*

(ii) *$av \in \ker L$;*

(iii) *$aM(u) \in \operatorname{im} L$.*

Proof Clearly, if a is zero the statement is trivially verified. Suppose that $a \in \mathbb{F}_{q^n}^*$. Let ρ be a nonzero vector in $\ker R$ which means $\ker R = \langle \rho \rangle_{q^t}$.

$(i) \Rightarrow (ii)$. Let $a \in \langle \rho \rangle_{q^t}$, then there exists $\lambda \in \mathbb{F}_{q^t}$ such that $a = \lambda\rho$. Then

$$L(av) = \lambda^q L(\rho v) = \lambda^q \left((\rho v)^q - h^{1-q^{t+1}} (\rho v)^{q^{t+1}} \right).$$

Since $\rho \in \ker R$ and $v \in \ker M$, by (6) and (9), we get

$$(\lambda\rho v)^q \left(1 - h^{-q^{t+2}+1+q^t-q^2} \right).$$

Moreover, since $h^{q^t+1} = -1$, the latter expression is equal to 0; hence, $av \in \ker L$.

$(ii) \Rightarrow (iii)$ Let $v \in \ker M$. Since $av \in \ker L$,

$$0 = L(av) = (av)^q - h^{1-q^{t+1}} (av)^{q^{t+1}} = v^q \left(a^q + h^{1-q^{t+2}} a^{q^{t+1}} \right),$$

that is

$$a + h^{q^{2t-1}-q^{t+1}} a^{q^t} = 0. \tag{12}$$

We will prove that $aM(u) \in \mathrm{im} L$. So, putting $z = M(u)$, by (7), this is equivalent to prove that

$$(az)^{q^t} + h^{q^t-q}(az) = 0.$$

By Proposition 3.3, since $u \in \ker L$, $z = M(u) \neq 0$. Also, since $h^{q^t+1} = -1$, by (8), we have

$$(az)^{q^t} + h^{q^t-q}(az) = zh^{q^t-q} \cdot \left(a^{q^t} h^{q^{2t-1}-q^{t+1}} + a \right)$$

and by (12) the last expression equals 0, proving the result.

$(iii) \Rightarrow (i)$ As before, by Proposition 3.3, $z = M(u)$ is a nonzero element of $\mathrm{im}\, M$. Since $az \in \mathrm{im}\, L$, by (7) and (8), we obtain

$$\begin{aligned} 0 &= (az)^{q^t} + h^{q^t-q}(az) = z \left(a^{q^t} h^{q^t-q^{t-1}} + h^{q^t-q} a \right) \\ &= h^{q^t-q^{t-1}} z \left(a^{q^t} + h^{q^{t-1}-q} a \right), \end{aligned}$$

which implies $a^{q^t} + h^{q^{t-1}-q} a = 0$. Then, by (9), $a \in \ker R$. Finally, since $\ker R$ is a 1-dimensional $\mathbb{F}_{q^t}$-subspace of $\mathbb{F}_{q^n}$, $a = \lambda\rho$ for some $\lambda \in \mathbb{F}_{q^t}$. □

Using similar techniques as in the previous proposition we can show the following result

Proposition 3.6 *For any nonzero vectors $u \in \ker L$, $v \in \ker M$ and any $b \in \mathbb{F}_{q^n}$, the following statements are equivalent:*

(i) $b \in \ker T$;
(ii) $bu \in \ker M$;
(iii) $bL(v) \in \operatorname{im} M$.

We are now in the position to prove our main result of this section.

Proof of Theorem 3.1 Let $\psi(x) := \psi_{h,t}(x)$, we want to prove that for each $x \in \mathbb{F}^*_{q^n}$ and for each $\gamma \in \mathbb{F}_{q^n}$ such that

$$\psi(\gamma x) = \gamma\psi(x) \tag{13}$$

we get $\gamma \in \mathbb{F}_q$. Recall that

$$\psi(x) = L(x) + M(x)$$

as in (4). Also, by Proposition 3.3, any $x \in \mathbb{F}_{q^n}$ can be uniquely written as $x = x_1+x_2$, where $x_1 \in \ker L$ and $x_2 \in \ker M$. Similarly, by Lemma 3.4, if $\gamma \in \mathbb{F}_{q^n}$ there are exactly two elements $\lambda_1, \mu_1 \in \mathbb{F}_{q^t}$ and two elements $\lambda_2, \mu_2 \in \mathbb{F}_{q^t}$ such that

$$\lambda_1 + \mu_1\rho = \gamma = \lambda_2 + \mu_2\tau$$

where $\rho \in \ker R$ and $\tau = h^{q^{t-1}-q}\rho$. It has been already noted that $\tau \in \ker T$. Putting $a = \mu_1\rho$ and $b = \mu_2\tau$, which imply $a \in \ker R$ and $b \in \ker T$, Condition (13) may be re-written as follows

$$\begin{aligned} L((\lambda_1 + a)(x_1 + x_2)) + M((\lambda_2 + b)(x_1 + x_2)) = (\lambda_2 + b)L(x_1 + x_2)\\ + (\lambda_1 + a)M(x_1 + x_2). \end{aligned} \tag{14}$$

Also, since $x_1 \in \ker L$, $x_2 \in \ker M$, $L(x)$ and $M(x)$ are $\mathbb{F}_{q^t}$-semilinear maps and by (ii) of Proposition 3.5 and (ii) of Proposition 3.6, Eq. (14) is equivalent to

$$\begin{aligned} L(\lambda_1 x_2) + L(ax_1) + M(\lambda_2 x_1) + M(bx_2) = \lambda_2 L(x_2) + bL(x_2)\\ + \lambda_1 M(x_1) + aM(x_1). \end{aligned}$$

and hence

$$\begin{aligned} \lambda_1^q L(x_2) + L(ax_1) - \lambda_2 L(x_2) - aM(x_1) = bL(x_2) + \lambda_1 M(x_1)\\ - \lambda_2^{q^{t-1}} M(x_1) - M(bx_2). \end{aligned} \tag{15}$$

Now, since the image spaces of the maps $L(x)$ and $M(x)$ are $\mathbb{F}_{q^t}$-spaces, taking (iii) of Proposition 3.5 and (iii) of Proposition 3.6 into account, the expressions on left and right hand sides of (15) belong to $\operatorname{im} L$ and $\operatorname{im} M$, respectively. By Proposition 3.3, both sides of (15) must be equal to zero an hence we obtain the following system

$$\begin{cases} L(ax_1) - aM(x_1) = \left(\lambda_2 - \lambda_1^q\right)L(x_2)\\ bL(x_2) - M(bx_2) = \left(\lambda_2^{q^{t-1}} - \lambda_1\right)M(x_1). \end{cases}$$

Raising to the q-th power the second equation, we get

$$\begin{cases} L(ax_1) - aM(x_1) = \left(\lambda_2 - \lambda_1^q\right) L(x_2) \\ b^q L(x_2)^q - M(bx_2)^q = \left(\lambda_2 - \lambda_1^q\right) M(x_1)^q. \end{cases} \tag{16}$$

Since $a = \mu_1 \rho$, $b = \mu_2 \tau$ and $\tau = h^{q^{t-1}-q}\rho$, from Lemma 3.4 it follows

$$\lambda_1 + \mu_1 \rho = \mu_1 \rho \left(1 - h^{q^{t-1}-q}\right) + \mu_1 \tau = \lambda_2 + \mu_2 \tau$$

and, since $\{1, \tau\}$ is an $\mathbb{F}_{q^t}$-basis of $\mathbb{F}_{q^n}$, we get $\mu_1 = \mu_2$ and $b = h^{q^{t-1}-q} a$.

If $a = 0$, we have $\mu_1 = 0$ and hence $\gamma = \lambda_1 = \lambda_2 \in \mathbb{F}_{q^t}$. Also, from (16), if $\lambda_2 \neq \lambda_1^q$, then $L(x_2) = M(x_1) = 0$. By Proposition 3.3, $x = x_1 = x_2 = 0$, a contradiction. Then $\lambda_1 = \lambda_2 = \lambda_1^q$, which gives $\lambda_1 \in \mathbb{F}_q$, i.e. $\gamma \in \mathbb{F}_q$.

In the remainder of the proof, we are going to show that $a \neq 0$, i.e. $\gamma \in \mathbb{F}_{q^{2t}} \setminus \mathbb{F}_{q^t}$ leads to contradictions. Depending on the value of x_1 and x_2, we separate the proof into three cases.

Case 1 $x_1 = 0$. The system in (16) is reduced to

$$\begin{cases} \left(\lambda_2 - \lambda_1^q\right) L(x_2) = 0 \\ b^q L(x_2)^q - M(bx_2)^q = 0. \end{cases}$$

By the second equation, taking into that $b \in \ker T$, $x_2 \in \ker M$ and $h^{q^t+1} = -1$, we get

$$b^{q-1} = \frac{h^{q-1}}{\left(x_2\left(1 + h^{q-q^{t-1}}\right)\right)^{q^2-1}}.$$

Then, there exists $\lambda \in \mathbb{F}_q^*$ such that

$$b = \lambda \cdot \frac{h}{\left(x_2\left(1 + h^{q-q^{t-1}}\right)\right)^{q+1}}.$$

Since $b \in \ker T$, then $b^{q^t} + h^{q-q^{t-1}} b = 0$ and we get

$$\frac{h^{q^t-1}}{\left(x_2\left(1 + h^{q-q^{t-1}}\right)\right)^{q^t(q+1)}} + \frac{h^{q-q^{t-1}}}{\left(x_2\left(1 + h^{q-q^{t-1}}\right)\right)^{q+1}} = 0,$$

whence, since $x_2 \in \ker M$, $x_2^{q^t} = -h^{q^t-q^{t+1}} x_2$ and hence

$$\left(\frac{1 + h^{q-q^{t-1}}}{h^{q-1}\left(1 + h^{q^{t-1}-q}\right)}\right)^{q+1} = -h^{1+q-q^{t-1}-q^t}.$$

This is equivalent to

$$\left(\frac{h^{q^{t-1}-1}\big(1+h^{q-q^{t-1}}\big)}{h^{q-1}\big(1+h^{q^{t-1}-q}\big)}\right)^{q+1}=-1,$$

whence we have $1^{q+1}=-1$, a contradiction.

Case 2 $x_2=0$. The system in (16) is reduced to

$$\begin{cases} L(ax_1)-aM(x_1)=0\\ \big(\lambda_2-\lambda_1^q\big)M(x_1)^q=0. \end{cases}$$

By the first equation, taking into account that $a\in\ker R$, $x_1\in\ker L$ and $h^{q^t+1}=-1$, we obtain

$$a^{q-1}=\big(x_1^q\big)^{q^{t-2}-1}\cdot\frac{1+h^{1-q^{t-2}}}{1+h^{q^{t+2}-1}}=\left(x_1^q\big(1+h^{q^{t+2}-1}\big)\right)^{q^{t-2}-1}.$$

Then there exists $\lambda\in\mathbb{F}_q{}^*$ such that

$$a=\lambda\left(x_1^q\big(1+h^{q^{t+2}-1}\big)\right)^{\nu},$$

where $\nu=(q^{t-2}-1)/(q-1)$.

By (9), since $a\in\ker R$, then

$$\left(x_1^{q^{t+1}}\big(1+h^{q^2-q^t}\big)\right)^{\nu}+h^{q^{t-1}-q}\left(x_1^q\big(1+h^{q^{t+2}-1}\big)\right)^{\nu}=0.$$

Moreover, since $x_1\in\ker L$, then

$$\left(\frac{h^{q^{t+1}-1}\big(1+h^{q^2-q^t}\big)}{1+h^{q^t-q^2}}\right)^{\nu}=-h^{q^{t-1}-q}.$$

The last expression is equivalent to

$$\left(\frac{h^{q^t-q}\big(1+h^{q^2-q^t}\big)}{h^{q^2-q}\big(1+h^{q^t-q^2}\big)}\right)^{\nu}=-1,$$

whence $1^{\nu}=-1$, leading to a contradiction.

Case 3 $x_1,x_2\neq 0$. Recall that $a\in\ker R$, $b=h^{q^{t-1}-q}a$, $\lambda_2=\lambda_1+(1-h^{q^{t-1}-q})a$, $x_1\in\ker L$ and $x_2\in\ker M$. Then, by (16), a turns out to be a nonzero solution of the following linear system

$$\begin{cases} x_1^q\left(1+h^{q^t-q^2}\right)a^q-\left(M(x_1)+\left(1-h^{q^{t-1}-q}\right)L(x_2)\right)a \\ \quad =\left(\lambda_1-\lambda_1^q\right)L(x_2) \\ h^{q^t-q^2}L(x_2)^q a^q+\left(x_2^{q^t}\left(1+h^{q^{t-1}-q}\right)-\left(1-h^{q^{t-1}-q}\right)M(x_1)^q\right)a \\ \quad =\left(\lambda_1-\lambda_1^q\right)M(x_1)^q. \end{cases} \tag{17}$$

By $x_1 \in \ker L$ and $x_2 \in \ker M$, we obtain the following two equations which will be frequently used later,

$$L(x_2)=x_2^q\left(1+h^{1-q^{t+2}}\right),$$
$$M(x_1)=x_1^{q^{t-1}}\left(1+h^{1-q^{t-2}}\right).$$

- *Case 3.1* First of all, suppose that $\lambda_1 \in \mathbb{F}_q$, then System (17) becomes

$$\begin{cases} x_1^q\left(1+h^{q^t-q^2}\right)a^q-\left(M(x_1)+\left(1-h^{q^{t-1}-q}\right)L(x_2)\right)a=0 \\ h^{q^t-q^2}L(x_2)^q a^q+\left(x_2^{q^t}\left(1+h^{q^{t-1}-q}\right)-\left(1-h^{q^{t-1}-q}\right)M(x_1)^q\right)a=0. \end{cases} \tag{18}$$

and since a is a nonzero solution then

$$\begin{aligned} &x_1^q\left(1+h^{q^t-q^2}\right)\left(x_2^{q^t}\left(1+h^{q^{t-1}-q}\right)-\left(1-h^{q^{t-1}-q}\right)M(x_1)^q\right) \\ &\quad =-h^{q^t-q^2}L(x_2)^q\left(M(x_1)+\left(1-h^{q^{t-1}-q}\right)L(x_2)\right). \end{aligned} \tag{19}$$

Since $L(x_2) \neq 0 \neq M(x_1)$, from (18) we get

$$\begin{aligned} &M(x_1)^q\left(x_1^q\left(1+h^{q^t-q^2}\right)a^q-M(x_1)a\right) \\ &\quad =L(x_2)\left(h^{q^t-q^2}L(x_2)^q a^q+x_2^{q^t}\left(1+h^{q^{t-1}-q}\right)a\right) \end{aligned}$$

whence

$$\begin{aligned} &\left(x_1^q M(x_1)^q\left(1+h^{q^t-q^2}\right)-h^{q^t-q^2}L(x_2)L(x_2)^q\right)a^q \\ &\quad =\left(M(x_1)M(x_1)^q+x_2^{q^t}\left(1+h^{q^{t-1}-q}\right)L(x_2)\right)a. \end{aligned} \tag{20}$$

Next we want to show that the coefficient of a^q in (20) cannot be 0. By way of contradiction, suppose that

$$x_1^q\left(1+h^{q^t-q^2}\right)M(x_1)^q=h^{q^t-q^2}L(x_2)L(x_2)^q, \tag{21}$$

from (19) it follows

$$x_1^q x_2^{q^t}\left(1+h^{q^t-q^2}\right)\left(1+h^{q^{t-1}-q}\right)=-h^{q^t-q^2}L(x_2)^q M(x_1). \tag{22}$$

Since $x_1 \in \ker L$ and $x_2 \in \ker M$, this is equivalent to

$$x_1^{q^{t-2}-1}=-\left(x_2^q\right)^{q^{t-2}-1}\frac{\left(1+h^{q-q^{t-1}}\right)\left(1+h^{q^{t-2}-1}\right)}{\left(1+h^{1-q^{t+2}}\right)\left(1+h^{q^{2t-1}-q^{t-3}}\right)}. \tag{23}$$

This formula is equivalent to

$$x_1^{q^{t-2}-1}=-\left(x_2^q\cdot\frac{1+h^{1-q^{t+2}}}{\left(1+h^{q-q^{t-1}}\right)h^{q^{t-1}}}\right)^{q^{t-2}-1}. \tag{24}$$

Since

$$d=\gcd(2t,t-2)=\gcd(4,t-2)=\begin{cases}1, & \text{if } t \text{odd}\\ 2, & \text{if } t\equiv 0 \pmod 4\\ 4, & \text{if } t\equiv 2 \pmod 4\end{cases}$$

there exists a solution of the equation $x^{q^{t-2}-1}=-1$ for any $t\geq 3$ and $t\not\equiv 2 \pmod 4$ in $\mathbb{F}_{q^n}$. Thus, for $t\equiv 2 \pmod 4$, Eq. (24) gives a contradiction. In the remaining cases,

$$x_1=\omega x_2^q\cdot\frac{1+h^{1-q^{t+2}}}{\left(1+h^{q-q^{t-1}}\right)h^{q^{t-1}}},$$

for some $\omega\in\mathbb{F}_{q^n}^*$ satisfying $\omega^{q^{t-2}-1}=-1$. By substituting this expression in (21), since $x_1\in\ker L$, we get

$$\omega^{q+1}=-1, \tag{25}$$

and hence $\omega\in\mathbb{F}_{q^2}$.

If t is odd, since $\omega^{q^{t-2}}=-\omega$, then $\omega^q=-\omega$ and from (25), we get $\omega=\pm 1$. If $t\equiv 0 \pmod 4$, since $\omega=\omega^{q^{t-2}}=-\omega$. In both cases we get a contradiction.

Then, by (20), we get

$$\begin{aligned}a^{q-1}&=\frac{M(x_1)M(x_1)^q-h^{q^t-q^{t+1}}x_2L(x_2)(1+h^{q^{t-1}-q})}{x_1^q(1+h^{q^t-q^2})M(x_1)^q-h^{q^t-q^2}L(x_2)L(x_2)^q}\\&=h^{q-1}\cdot\frac{1+h^{q^{t-1}-q}}{1+h^{q^t-q^2}}\cdot\frac{x_1M(x_1)-x_2L(x_2)}{x_1^qM(x_1)^q-x_2^qL(x_2)^q}\\&=\left(\frac{h}{(1+h^{q^{t-1}-q})(x_1M(x_1)-x_2L(x_2))}\right)^{q-1},\end{aligned} \tag{26}$$

whence

$$a = \lambda \cdot \frac{h}{(1 + h^{q^{t-1}-q})(x_1 M(x_1) - x_2 L(x_2))}$$

for some $\lambda \in \mathbb{F}_q^*$. Since $a \in \ker R$, then

$$\frac{h^{q^t}}{\left((1 + h^{q^{t-1}-q})(x_1 M(x_1) - x_2 L(x_2))\right)^{q^t}} + h^{q^{t-1}-q} \cdot \\ \frac{h}{(1 + h^{q^{t-1}-q})(x_1 M(x_1) - x_2 L(x_2))} = 0.$$

Recalling that $x_1 \in \ker L$ and $x_2 \in \ker M$, we get

$$x_1 M(x_1) - x_2 L(x_2) = x_1^{q^{t-1}+1}\left(1 + h^{1-q^{t-2}}\right) - x_2^{q+1}\left(1 + h^{1-q^{t+2}}\right).$$

This implies that

$$-\frac{1}{h^{q^t}(1 + h^{q-q^{t-1}})} + \frac{h^{q^{t-1}-q} \cdot h}{1 + h^{q^{t-1}-q}} = 0,$$

which means $h^{q^t+1} = 1$, a contradiction. Then λ_1 may not belong to $\mathbb{F}_q$.

- *Case 3.2* Let $\lambda_1 \notin \mathbb{F}_q$ and let a be a nonzero solution of System (17). If this system admits more than one solution, then each 2×2 minor of the associated matrix of (17) is zero. In particular Eqs. (21) and (22) hold true, obtaining a contradiction as in the previous case.

Then, System (17) must admits a unique nonzero solution $(a, a^q) \in \mathbb{F}_{q^n}^2$. By computing the ratio a^{q-1} of its components, we get

$$a^{q-1} = \frac{\begin{vmatrix} L(x_2) & -M(x_1) \\ M(x_1)^q & x_2^{q^t}(1 + h^{q^{t-1}-q}) \end{vmatrix}}{\begin{vmatrix} x_1^q(1 + h^{q^t-q^2}) & L(x_2) \\ h^{q^t-q^2} L(x_2)^q & M(x_1)^q \end{vmatrix}}$$
$$= \frac{M(x_1)M(x_1)^q - h^{q^t-q^{t+1}} x_2 L(x_2)(1 + h^{q^{t-1}-q})}{x_1^q(1 + h^{q^t-q^2})M(x_1)^q - h^{q^t-q^2} L(x_2)L(x_2)^q}.$$

This is again Eq. (26). Repeating the arguments as in *Case 3.1* we get a contradiction. □

4 A New Family of MRD Codes

Let start by the following preliminary general result.

Lemma 4.1 *Let $f(x)$ be a scattered polynomial and let $\mathcal{C}_f$ denote the associated MRD code. Then* $\mathrm{Aut}(\mathcal{C}_f)$ *consists of elements* $(\alpha x^{q^m}, L_2, \sigma) \in \mathcal{L}_{n,q}[x] \times \mathcal{L}_{n,q}[x] \times \mathrm{Aut}(\mathbb{F}_q)$ *with L_2 an invertible map, $\alpha \in \mathbb{F}_{q^n}^*$ and $m \in \{0, 1, \dots, n-1\}$ such that*

$$\mathcal{C}_{f^{\sigma q^m}} \circ x^{q^m} \circ L_2 = \mathcal{C}_f.$$

Also, for any $\alpha \in \mathbb{F}_{q^n}^*$ and $m \in \{0, 1, \dots, n-1\}$, there is a bijection between each L_2 such that $(\alpha x^{q^m}, L_2, \sigma) \in \mathrm{Aut}(\mathcal{C}_f)$ and each $\mathrm{GL}(2, q^n)$*-equivalence map from U_f to $U_{f^{\sigma q^m}}$, where $U_f = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\}$. In particular, the multiplicative group $I_R(\mathcal{C}_f) \setminus \{0\}$ and the* $\mathrm{GL}(2, q^n)$*-automorphism group of U_f are isomorphic.*

Proof Suppose that $\varphi \in I_L(\mathcal{C}_f)^* := I_L(\mathcal{C}_f) \setminus \{0\}$ and $(L_1, L_2, \sigma) \in \mathrm{Aut}(\mathcal{C}_f)$ where L_1, L_2 are invertible $\mathbb{F}_q$-polynomials and $x^\sigma = x^{p^\ell}$ with $0 \leq \ell \leq r-1$. Then for any $g \in \mathcal{C}_f$, there exists an element $g' \in \mathcal{C}_f$ such that

$$\varphi \circ (L_1 \circ g^\sigma \circ L_2) = L_1 \circ g'^\sigma \circ L_2$$

which means

$$\begin{aligned} \varphi \circ (L_1 \circ x^{p^\ell} \circ g \circ x^{p^{nr-\ell}} \circ L_2) &= L_1 \circ x^{p^\ell} \circ g' \circ x^{p^{nr-\ell}} \circ L_2 \\ (L_1 \circ x^{p^\ell})^{-1} \circ \varphi \circ (L_1 \circ x^{p^\ell}) \circ g &= g' \in \mathcal{C}_f, \end{aligned}$$

and hence, $(L_1 \circ x^{p^\ell})^{-1} \circ \varphi \circ (L_1 \circ x^{p^\ell}) \in I_L(\mathcal{C}_f)$. By (1),

$$(L_1 \circ x^{p^\ell})^{-1} \circ \varphi \circ (L_1 \circ x^{p^\ell}) = \gamma x$$

for some $\gamma \in \mathbb{F}_{q^n}^*$ which is equivalent to say that $L_1^{-1} \circ \varphi \circ L_1 \in I_L(\mathcal{C}_f)^*$. Thus, L_1 is in the normalizer of $I_L(\mathcal{C}_f)^*$ in $\mathrm{GL}(n, q)$, and hence, by [17, p. 362], it is isomorphic to $(\mathbb{F}_{q^n}^*, \cdot) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. Then, $L_1(x) = \alpha x^{q^m}$ for some $\alpha \in \mathbb{F}_{q^n}^*$ and $m \in \{0, 1, \dots, n-1\}$. So any element in $\mathrm{Aut}(\mathcal{C}_f)$ is as in the statement and

$$\mathcal{C}_f = \alpha x^{q^m} \circ \mathcal{C}_f^\sigma \circ L_2 = \mathcal{C}_{f^{\sigma q^m}} \circ x^{q^m} \circ L_2.$$

This completes the first part of the proof.

As the identity map is in $\mathcal{C}_{f^{\sigma q^m}}$, $h(x) := x^{q^m} \circ L_2 \in \mathcal{C}_f$, that is $h(x) = ax + bf(x)$ for some $a, b \in \mathbb{F}_{q^n}$. Furthermore, $\mathcal{C}_{f^{\sigma q^m}} \circ h = \mathcal{C}_f$ also implies the existence of $c, d \in \mathbb{F}_{q^n}$ such that

$$cx + df(x) = f^{\sigma q^m}(ax + bf(x)), \tag{27}$$

for all $x \in \mathbb{F}_{q^n}$. By setting $y = ax + bf(x)$, (27) is equivalent to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ f(x) \end{pmatrix} = \begin{pmatrix} y \\ f^{\sigma q^m}(y) \end{pmatrix}. \tag{28}$$

Also, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible. Indeed, if there exists $\lambda \in \mathbb{F}_{q^n}^*$ such that $(c, d) = \lambda(a, b)$ then by (27) we get

$$\lambda h(x) = f^{\sigma q^m}(h(x)) = x^{\sigma q^m} \circ f \circ x^{-\sigma q^m} \circ h,$$

and hence $f(k(x)) = \mu k(x)$ where $k(x) = x^{-\sigma q^m} \circ h(x)$ and $\mu = \lambda^{-\sigma q^m} \in \mathbb{F}_{q^n}^*$. Since $k(x)$ is invertible, then $f(x) = \mu x$ contradicting the fact that L_f is scattered. This means that U_f is $\mathrm{GL}(2, q^n)$-equivalent to $U_{f^{\sigma q^m}}$. Also from (27), it can be easily seen that (c, d) is uniquely determined by (a, b). Therefore, there is a 1–1 correspondence between every L_2 and every matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mapping U_f. In particular, when $f = f^{\sigma q^m}$, all such $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ form the $\mathrm{GL}(2, q^n)$-automorphism group of U_f, denoted by G_f. As each nonzero element of $I_R(\mathcal{C}_f)$ is invertible (see [21, Corollary 5.6]), it is straightforward to see that the map described above determines an isomorphism between the groups G_f and $I_R(\mathcal{C}_f)\backslash\{0\}$. Hence, the result follows. □

Let $\psi_{h,t}$ be defined as in (3) and

$$\mathcal{C}_{h,t} = \{ax + b\psi_{h,t}(x) : a, b \in \mathbb{F}_{q^n}\}. \tag{29}$$

By the argument stated in [27, Section 5], $\mathcal{C}_{h,t}$ is an $\mathbb{F}_{q^n}$-linear MRD code.

The following result is about the equivalence among $\mathcal{C}_{h,t}$'s for different h and the automorphism group of $\mathcal{C}_{h,t}$.

Theorem 4.2 *Let $n = 2t$ with $t > 4$. For each $h, k \in \mathbb{F}_{q^n}$ satisfying $h^{q^t+1} = k^{q^t+1} = -1$, the following hold*

(a) *If $t \not\equiv 2 \pmod 4$, then $\mathcal{C}_{h,t}$ and $\mathcal{C}_{k,t}$ are equivalent if and only if $h = \pm k^\rho$ where $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$;*
(b) *If $t \equiv 2 \pmod 4$, then $\mathcal{C}_{h,t}$ and $\mathcal{C}_{k,t}$ are equivalent if and only if $h = \ell k^\rho$ where $\ell^{q^2+1} = 1$ and $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$.*

The full automorphism group $\mathrm{Aut}(\mathcal{C}_{h,t})$ is isomorphic to $(\mathbb{F}_{q^n}^*, \cdot) \times (\mathbb{F}_{q^2}^*, \cdot) \rtimes H$, where $H = \{\rho \in \mathrm{Aut}(\mathbb{F}_{q^n}) : h = \pm h^\rho\}$ if $t \not\equiv 2 \pmod 4$, and $H = \{\rho \in \mathrm{Aut}(\mathbb{F}_{q^n}) : (h^\rho/h)^{q^2+1} = 1\}$ if $t \equiv 2 \pmod 4$.

Proof Let $U_h = \{(x, \psi_{h,t}(x)) : x \in \mathbb{F}_{q^n}\}$ and $U_k = \{(x, \psi_{k,t}(x)) : x \in \mathbb{F}_{q^n}\}$. By Theorem 2.1, we only have to consider the $\Gamma L(2, q^n)$-equivalence between U_h and

U_k. Since U_k is $\mathrm{GL}(2, q^n)$-equivalent to U_{k^ρ} for any ρ in $\mathrm{Aut}(\mathbb{F}_{q^n})$, this is equivalent to study the $\mathrm{GL}(2, q^n)$-equivalence between U_h and U_{k^ρ}. This also means that, to get (a) and (b), we can replace k^ρ by k and we just need to show that a necessary and sufficient condition for that U_h is $\mathrm{GL}(2, q^n)$-equivalent to U_k is

$$h = \begin{cases} \pm k, & t \not\equiv 2 \pmod 4; \\ \ell k, & t \equiv 2 \pmod 4, \end{cases} \tag{30}$$

where $\ell \in \mathbb{F}_{q^n}$ satisfies $\ell^{q^2+1} = 1$.

Hence, we only have to consider the existence of invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over $\mathbb{F}_{q^n}$ such that for each $x \in \mathbb{F}_{q^n}$ there exists $y \in \mathbb{F}_{q^n}$ satisfying

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ \psi_{h,t}(x) \end{pmatrix} = \begin{pmatrix} y \\ \psi_{k,t}(y) \end{pmatrix}.$$

This is equivalent to

$$cx + d\psi_{h,t}(x) = \psi_{k,t}\left(ax + b\psi_{h,t}(x)\right), \tag{31}$$

for all $x \in \mathbb{F}_{q^n}$. The right-hand-side of (31) is

$$\begin{aligned}
&\left(b^q + k^{1-q^{t+1}} b^{q^{t+1}} h^{q^{t+1}-q^2}\right) x^{q^2} + \left(b^{q^{t-1}} h^{q^{t-1}-q^{t-2}} + b^{q^{2t-1}} k^{1-q^{2t-1}}\right) x^{q^{t-2}} \\
&\quad + \left(b^q + b^{q^{t-1}} - h^{q^{t+1}-q^t} k^{1-q^{t+1}} b^{q^{t+1}} - k^{1-q^{2t-1}} h^{q^{2t-1}-q^t} b^{q^{2t-1}}\right) x^{q^t} \\
&\quad + \left(b^{q^{t-1}} + k^{1-q^{2t-1}} h^{q^{2t-1}-q^{2t-2}} b^{q^{2t-1}}\right) x^{q^{2t-2}} - \left(h^{q-q^{t+2}} b^q + k^{1-q^{t+1}} b^{q^{t+1}}\right) x^{q^{t+2}} \\
&\quad + \left(b^q h^{q-1} - b^{q^{t-1}} h^{q^{t-1}-1} - k^{1-q^{t+1}} b^{q^{t+1}} + k^{1-q^{2t-1}} b^{q^{2t-1}}\right) x + \psi_{k,t}(ax).
\end{aligned}$$

As $t > 4$, it is easy to see that the coefficients of x^{q^2}, $x^{q^{t-2}}$, x^{q^t}, $x^{q^{t+2}}$ and $x^{q^{2t-2}}$ in the right-hand-side of (31) must be 0. Depending on whether the value of b equals 0 or not, we separate the proof into two cases.

Case 1 $b \neq 0$. By the coefficient of x^{q^2} (or equivalently, by the coefficient of $x^{q^{t+2}}$), we get

$$b^{q^{t+1}-q} = -k^{-q-1} h^{q^2+q}. \tag{32}$$

Similarly, by the coefficient of $x^{q^{t-2}}$ (or equivalently, by the coefficient of $x^{q^{2t-2}}$), we get

$$b^{q^{t+1}-q} = -k^{-q+q^2} h^{q-1}. \tag{33}$$

By (32) and (33), we obtain

$$h^{q^2+1} = k^{q^2+1}.$$

Let $\ell = h/k$. Then $\ell^{q^2+1} = 1$. By the assumption that $h^{q^t+1} = k^{q^t+1} = -1$, we have $\ell^{q^t+1} = 1$.

If $t \not\equiv 2 \pmod 4$, then $\ell = \pm 1$; if $t \equiv 2 \pmod 4$, then we obtain $\ell^{q^2+1} = 1$, which implies $\ell \in \mathbb{F}_{q^4}$.

Case 2 $b = 0$. If (31) holds, then $c = 0$ and

$$\begin{cases} d = a^q = a^{q^{t-1}} \\ dh^{1-q^{t+1}} = k^{1-q^{t+1}} a^{q^{t+1}} \\ dh^{1-q^{2t-1}} = k^{1-q^{2t-1}} a^{q^{2t-1}}. \end{cases} \tag{34}$$

The first equation in (34) implies that $a \in \mathbb{F}_{q^{\gcd(2t,t-2)}}$ which means $a \in \mathbb{F}_{q^{\gcd(t-2,4)}}$. Let $\ell = h/k$. The last two equations in (34) become

$$d\ell^{1-q^{t+1}} = a^{q^3} = d\ell^{1-q^{2t-1}}. \tag{35}$$

Thus $\ell^{q^{2t-1}-q^{t+1}} = 1$. This means $\ell \in \mathbb{F}_{q^{\gcd(t-2,2t)}} = \mathbb{F}_{q^{\gcd(t-2,4)}}$. By the assumption that $h^{q^t+1} = k^{q^t+1} = -1$, we have $\ell^{q^t+1} = 1$. If $\gcd(t-2,4) \in \{1,2\}$ i.e. $t \not\equiv 2 \pmod 4$, then $\ell = \pm 1$ which means $\psi_{k,t} = \psi_{h,t}$ and $\mathcal{C}_{h,t}$ and $\mathcal{C}_{k,t}$ are the same; if $\gcd(t-2,4) = 4$ i.e. $t \equiv 2 \pmod 4$, then we obtain $\ell^{q^2+1} = 1$.

Next, let us further consider the case $t \equiv 2 \pmod 4$. By (35),

$$a^{q^3-q} = \ell^{1-q^{t+1}} = \ell^{1-q^3} = \ell^{(1-q)(q^2+q+1)} = \ell^{q-q^2} = \ell^{q+1}.$$

For a given $\ell \in \mathbb{F}_{q^4}$, we can always find $a \in \mathbb{F}_{q^4}$ satisfying the above equation. Moreover, it is routine to verify that such a satisfies (34) provided that $h = \ell k$ with $\ell^{q^2+1} = 1$; note here that by (34) d depends on a. This complete the proof of equivalence between $\mathcal{C}_{h,t}$ and $\mathcal{C}_{k,t}$.

In the final part of this proof, we determine the automorphism group of $\mathcal{C}_{h,t}$. By the first part of Lemma 4.1, $\mathrm{Aut}(\mathcal{C}_{h,t})$ consists of $(\alpha x^{q^m}, L_2, \sigma) \in \mathcal{L}_{n,q}[x] \times \mathcal{L}_{n,q}[x] \times \mathrm{Aut}(\mathbb{F}_q)$ such that

$$\mathcal{C}_{h,t} = \left\{ f^{\sigma q^m} \circ x^{q^m} \circ L_2 : f \in \mathcal{C}_{h,t} \right\}.$$

Note that α can be any element in $\mathbb{F}_{q^n}^*$, because we always have $\alpha(a + b\psi_{h,t}(x)) \in \mathcal{C}_{h,t}$ for any $a, b \in \mathbb{F}_{q^n}$.

By the second part of Lemma 4.1, for a given m, there is a bijection between each L_2 and each invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that (28) holds for $f = \psi_{h,t}$. More precisely, following the proof of Lemma 4.1,

$$L_2(x) = (ax + b\psi_{h,t}(x))^{q^{n-m}}. \tag{36}$$

Write $\rho = \sigma q^m$. Consequently, we only have to determine all the $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$ and all the elements in $\mathrm{GL}(2, q^n)$ mapping U_h to U_{h^ρ}. By (a) and (b), we see that ρ must satisfy the condition $h^\rho = \pm h$ for $t \not\equiv 2 \pmod 4$, and $(h^\rho/h)^{q^2+1} = 1$ for $t \equiv 2 \pmod 4$. All such ρ form a subgroup $H \subseteq \mathrm{Aut}(\mathbb{F}_{q^n})$.

To accomplish the proof, we just need to continue the computation of the first part for $k = h$ and determine which matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ defines an equivalence map from U_h to itself. Indeed, all such maps provide a subgroup K, which is normal in $\mathrm{Aut}(C_{h,t})$, where

$$K = \left\{(\alpha x, L_2, \mathrm{id}) : \alpha \in \mathbb{F}_{q^n}^*, L_2 \in \mathcal{L}_{n,q}[x] \text{ invertible}, \mathcal{C}_{h,t} = \{\alpha f(L_2(x)) : f \in \mathcal{C}_{h,t}\}\right\}.$$

Moreover, every other element in $\mathrm{Aut}(\mathcal{C}_{h,t})$ which corresponds to a map from U_h to U_{h^ρ} with $\rho \neq \mathrm{id}$ belongs to a coset of K in $\mathrm{Aut}(\mathcal{C}_{h,t})$, and $\mathrm{Aut}(\mathcal{C}_{h,t})/K \cong H$.

Depending on whether $b = 0$ or not, we consider two cases to determine the elements in K.

When $b = 0$, we only have to let $k = h$ in (34). From there we derive that $d = a^q = a^{q^{t-1}} = a^{q^{t+1}}$. Therefore $a \in \mathbb{F}_{q^{\gcd(t,2)}}^*$.

When $b \neq 0$, by letting $k = h$, we see that the coefficient of x^{q^t} in the right-hand-side of (31) is

$$b^q + b^{q^{t-1}} - h^{1-q^t} b^{q^{t+1}} - h^{1-q^t} b^{q^{2t-1}}$$

which must be 0. Plugging (32) into it and taking into account that $h^{q^t} = -1/h$, we get

$$b^q\left(1 + h^{q^2-q^t}\right) + b^{q^{t-1}}\left(1 + h^{1-q^{t-2}}\right) = 0.$$

Raising it to the q^2-th power and plugging (32) again, we obtain

$$b^{q^3}\left(1 - h^{q^4+q^2}\right) - b^q\left(h^{q^2-1} - h^{2q^2}\right) = 0,$$

which means

$$b^q\left(h^{-1} - h^{q^2}\right) = \left(b^q\left(h^{-1} - h^{q^2}\right)\right)^{q^2}.$$

By Proposition 3.2, $h^{-1} \neq h^{q^2}$. Thus

$$b = \frac{-\delta}{h^{-q^{2t-1}} - h^q} = \frac{\delta}{h^{q^{t-1}} + h^q}$$

for some $\delta \in \mathbb{F}_{q^2}$. Substitute it into (32),

$$\frac{\delta^{q^t}}{h^{q^{2t-1}} + h^{q^{t+1}}} - h^{q+q^{t-1}} \frac{\delta}{h^{q^{t-1}} + h^q} = 0,$$

which means

$$\delta^{q^t} + \delta = 0. \tag{37}$$

When t is even, it follows that $2\delta = 0$. Thus b must be 0 which contradicts the assumption that $b \neq 0$. Thus, by (36), the assumption $m = 0$ and the above discussions for $b = 0$ and $b \neq 0$, we have determined the subgroup

$$K = \left\{(\alpha, ax, \mathrm{id}) : \alpha \in \mathbb{F}_{q^n}^*, a \in \mathbb{F}_{q^2}^*\right\}.$$

When t is odd, (37) implies $\delta^q = -\delta$. Plugging this value back into (31), we see that the coefficients of $x^{q^2}, x^{q^{t-2}}, x^{q^t}, x^{q^{t+2}}$ and $x^{q^{2t-2}}$ on the right-hand-side of (31) are all 0. Consequently, (31) becomes

$$\begin{aligned} cx + d\psi_{h,t}(x) \ = &\left(b^q h^{q-1} - b^{q^{t-1}} h^{q^{t-1}-1} - h^{1-q^{t+1}} b^{q^{t+1}} + h^{1-q^{2t-1}} b^{q^{2t-1}}\right) x \\ &+ \psi_{h,t}(ax). \end{aligned}$$

By simply setting c equal the coefficient of x in the right-hand-side of the above equation, which means c is determined by b, we only have to guarantee $d\psi_{h,t}(x) = \psi_{h,t}(ax)$. It reduces to the same computation for $b = 0$, in which we get $d = a^q = a^{q^{t-1}} = a^{q^{t+1}}$ with $a \in \mathbb{F}_q$, because $\gcd(t, 2) = 1$. The only difference is that, under the assumption that $b \neq 0$, we allow a to be 0. Therefore,

$$\begin{aligned} K = \Bigg\{&(\alpha x, ax + b\psi_{h,t}(x), \mathrm{id}) : \alpha \in \mathbb{F}_{q^n}^*, a \in \mathbb{F}_q, \\ &b = \frac{\delta}{h^{q^{t-1}} + h^q} \text{ with } \delta^q = -\delta, (a, b) \neq (0, 0)\Bigg\}. \end{aligned}$$

One may check directly that all such $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ form a cyclic group of order $q^2 - 1$, which also follows from the fact that the nonzero elements of the right idealizer

$$\begin{aligned} I_R(\mathcal{C}_{h,t}) =& \{\varphi \in \mathcal{L}_{n,q}[x] : f \circ \varphi \in \mathcal{C}_{h,t} \text{ for all } f \in \mathcal{C}_{h,t}\} \\ =& \left\{ax + b\psi_{h,t}(x) : a \in \mathbb{F}_q, b = \frac{\delta}{h^{q^{t-1}} + h^q} \text{ with } \delta^q = -\delta\right\} \end{aligned} \tag{38}$$

form the multiplicative group of a finite field.

Hence, no matter t is even or odd, K is isomorphic to $(\mathbb{F}_{q^n}^*, \cdot) \times (\mathbb{F}_{q^2}^*, \cdot)$. Therefore, $\mathrm{Aut}(\mathcal{C}_{h,t}) \cong (\mathbb{F}_{q^n}^*, \cdot) \times (\mathbb{F}_{q^2}^*, \cdot) \rtimes H$. □

Theorem 4.2 shows that our construction provides a big family of inequivalent MRD codes.

Corollary 4.3 *Let p be an odd prime number and let r, t be positive integers with $t > 4$ and $q = p^r$. The total number N of inequivalent MRD codes $\mathcal{C}_{h,t}$ is*

$$N \geq \begin{cases} \left\lfloor \frac{q^t+1}{4rt} \right\rfloor, & \textit{if } t \not\equiv 2 \pmod 4; \\ \left\lfloor \frac{q^t+1}{2rt(q^2+1)} \right\rfloor, & \textit{if } t \equiv 2 \pmod 4. \end{cases}$$

Proof In the proof of Theorem 4.2, we have obtained a necessary and sufficient condition (30) for the $\mathrm{GL}(2, q^n)$-equivalence between U_h and U_k, $n = 2t$. For a given h satisfying $h^{q^t+1} = -1$, let ξ_h denote the number of k for which U_k is $\mathrm{GL}(2, q^n)$-equivalent to U_h. The value of ξ_h is independent of h and

$$\xi_h = \begin{cases} 2, & t \not\equiv 2 \pmod 4; \\ q^2 + 1, & t \equiv 2 \pmod 4. \end{cases}$$

As there are at most $|\operatorname{Aut}(\mathbb{F}_{q^n})| = rn$ different ρ such that U_h is $\mathrm{GL}(2, q^n)$-equivalent to U_{k^σ} for a given h, there are at most $nr\xi_h$ choices of k for which U_h is $\Gamma L(2, q^n)$-equivalent to U_k. Therefore, we have obtained the lower bound for N which concludes the proof. □

By Corollary 4.3, we can prove the following result.

Theorem 4.4 *Let $n = 2t$ with $t > 4$ and let q be an odd prime power. The family of $\mathbb{F}_{q^n}$-linear MRD codes of minimum distance $n - 1$*

$$\mathcal{C}_{h,t} = \{ax + b\psi_{h,t}(x) : a, b \in \mathbb{F}_{q^n}\},$$

where $\psi_{h,t}(x) = x^q + x^{q^{t-1}} - h^{1-q^{t+1}} x^{q^{t+1}} + h^{1-q^{2t-1}} x^{q^{2t-1}} \in \mathbb{F}_{q^n}[x]$ and h is any element of $\mathbb{F}_{q^n}$ such that $h^{q^t+1} = -1$, contains examples which are not equivalent to any known ones in Table 1.

Proof As q can be any odd prime power and n can be any even integer larger than 6, by comparing Corollary 4.3 with the numbers of known inequivalent constructions of $\mathbb{F}_{q^n}$-linear MRD codes of minimum distance $n - 1$ in Table 1, our family must be new. □

Remark 4.5 In a recent paper [24], our family $\mathcal{C}_{h,t}$ of MRD codes has been generalized by Neri, Santonastaso and Zullo with an extra field automorphism σ as follows

$$\mathcal{C}_{h,t,\sigma} = \{ax + b\psi_{h,t,\sigma}(x) : a, b \in \mathbb{F}_{q^n}\}$$

with

$$\psi_{h,t,\sigma}(x) = x^\sigma + x^{\sigma^{t-1}} + h\sigma(h)x^{\sigma^{t+1}} + h\sigma^{-1}(h^{-1})x^{\sigma^{2t-1}},$$

where σ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$, $n = 2t$ with $t \geq 3$ and $h \in \mathbb{F}_{q^n}$ such that $h^{q^t+1} = -1$. If we take $\sigma(x) = x^q$, then $\mathcal{C}_{h,t,\sigma}$ coincides with $\mathcal{C}_{h,t}$. In [24, Section 4], a strengthened version of Theorem 4.4 has been proved: any member of the family $\mathcal{C}_{h,t,\sigma}$ is not equivalent to the MRD codes in family (i) for $t \geq 3$ or (ii) for $t > 4$ in Table 1. The first part of Theorem 4.2 for the members in $\mathcal{C}_{h,t,\sigma}$ has been also proved in [24, Section 4]. Instead of considering the equivalence map between subspaces U_h and U_{k^ρ} as we did in the proof of Theorem 4.2, they prove it using the rank-metric code equivalence directly. However, if we wanted to further determine the automorphism group of $\mathrm{Aut}(\mathcal{C}_{h,t})$, then we would need to find every map preserving $\mathcal{C}_{h,t}$. Nonetheless, Propositions 3.8 and 3.9 in [29] do not seem to be enough toward this aim. This is the reason why we proved Lemma 4.1 and Theorem 4.2 (the second part about automorphism groups) without checking the definition of MRD-code equivalence directly.

Finally, in [14], the authors complete the study of the equivalence issue of the MRD codes $\mathcal{C}_{h,t,\sigma}$ for $t \in \{3, 4\}$.

The following result is a direct consequence of (38) in the proof of Theorem 4.2.

Corollary 4.6 *Let $\mathcal{C}_{h,t}$ be defined as in (29), with $t > 4$. Then $I_R(\mathcal{C}_{h,t}) \cong \mathbb{F}_{q^2}$.*

Finally, let us investigate the adjoint of $\psi_{h,t}$ and the associated MRD code.

Theorem 4.7 *The $\mathbb{F}_{q^n}$-linear MRD code $\hat{\mathcal{C}}_{h,t} = \{ax + b\hat{\psi}_{h,t}(x) : a, b \in \mathbb{F}_{q^n}\}$, where $\hat{\psi}_{h,t}$ is the adjoint map of $\psi_{h,t}$ is equivalent to $\mathcal{C}_{h,t}$.*

Proof Consider the polynomial

$$g(x) := h\hat{\psi}_{h,t}(x/h) = x^q - x^{q^{t-1}} + h^{1-q^{t+1}}x^{q^{t+1}} + h^{1-q^{2t-1}}x^{q^{2t-1}},$$

we investigate the equivalence between $\mathcal{C}_g$ and $\mathcal{C}_{h,t}$.

To prove that $\mathcal{C}_g$ is equivalent to $\mathcal{C}_{h,t}$, as in the proof of Theorem 4.2, we only have to consider the existence of invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over $\mathbb{F}_{q^n}$ such that for each $x \in \mathbb{F}_{q^n}$ there exists $y \in \mathbb{F}_{q^n}$ satisfying

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ g(x) \end{pmatrix} = \begin{pmatrix} y \\ \psi_{h,t}(y) \end{pmatrix}.$$

Straightforward computation show that this happens for $a = d = 0$, $b = \left(\frac{h}{h^{q^2+1}-1}\right)^{q^{2t-1}}$ and $c = -(h^q + h^{q^{t-1}})$. □

5 Equivalence of the Associated Linear Sets

Let $\psi_{h,t}$ be the scattered polynomial over $\mathbb{F}_{q^n}$, $n = 2t$, defined in Theorem (3). Let

$$L_{h,t} := \left\{\langle(x, \psi_{h,t}(x))\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\right\}, \tag{39}$$

which is a maximum scattered linear set of $\mathrm{PG}(1, q^n)$.

In this part, we consider the $P\Gamma L$-equivalence between $L_{h,t}$ and $L_{k,t}$. Our main result shows that there is a large number of inequivalent maximum scattered linear sets associated with our family of scattered linear sets.

Theorem 5.1 *Let p be an odd prime number and let r, t be positive integers with $t > 4$ and $q = p^r$. The total number M of inequivalent maximum scattered linear sets $L_{h,t}$ of* $\mathrm{PG}(1, q^n)$*, $n = 2t$, satisfies*

$$M \geq \begin{cases} \left\lfloor \frac{q^t+1}{8rt} \right\rfloor, & \text{if } t \not\equiv 2 \pmod 4; \\ \left\lfloor \frac{q^t+1}{4rt(q^2+1)} \right\rfloor, & \text{if } t \equiv 2 \pmod 4. \end{cases}$$

Remark 5.2 We can provide an asymptotic estimation on the number of scattered linear sets we found over the number of known families. As our new family contains (iii) in Table 1 and (i) has only one member, we only have to know the number of inequivalent members of the Lunardon–Polverino family over $\mathbb{F}_{q^n}$, which has been recently determined in [30]. Let us denote this number by $\Lambda(n, q)$, whose precise value is quite complicated; see [30, Theorem 4.4]. However, for given n, the value of $\Lambda(n, q)$ is approximately $\frac{q\phi(n)}{4r}$ for odd n and $\frac{q^2\phi(n)}{8r}$ for even n provided that q is large enough. Together with Theorem 5.1, it follows that the number of our scattered linear sets over the number of known ones for given $n = 2t > 8$ is approximately at least

$$\begin{cases} \dfrac{q^{n/2-2}}{\frac{n}{2}\phi(n)}, & \frac{n}{2} \not\equiv 2 \pmod 4; \\ \dfrac{q^{n/2-4}}{\frac{n}{4}\phi(n)}, & \frac{n}{2} \equiv 2 \pmod 4, \end{cases}$$

provided that q is large enough.

To prove Theorem 5.1, we first restrict to the equivalence of linear sets under $\mathrm{PGL}(2, q^n)$ and consider two cases which will be handled in Lemmas 5.4 and 5.5, respectively. Then we will consider the $P\Gamma L(2, q^n)$-equivalence and present the proof of Theorem 5.1.

Let $f(x) = \sum_{i=0}^{n-1} \alpha_i x^{q^i}$ and $g(x) = \sum_{i=0}^{n-1} \beta_i x^{q^i}$ be two scattered polynomials over $\mathbb{F}_{q^n}$ with $\alpha_0 = \beta_0 = 0$. The associated linear sets L_f and L_g are $\mathrm{PGL}(2, q^n)$-equivalent if and only if there exists an invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over $\mathbb{F}_{q^n}$ such that

$$\left\{ \frac{f(x)}{x} : x \in \mathbb{F}_{q^n}^* \right\} = \left\{ \frac{cx + dg(x)}{ax + bg(x)} : x \in \mathbb{F}_{q^n}^* \right\}. \tag{40}$$

Remark 5.3 Note that $ax + bg(x)$ has no nonzero solution in $\mathbb{F}_{q^n}$, otherwise the linear set L_f would contain the point $\langle(0, 1)\rangle_{\mathbb{F}_{q^n}}$.

Depending on whether the value of b equals 0 or not, we may consider the equivalence in two cases.

If $b = 0$, then we can assume that $a = 1$, and (40) becomes

$$\left\{\sum_{i=0}^{n-1} \alpha_i x^{q^i-1} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{c + d\sum_{i=0}^{n-1} \beta_i x^{q^i-1} : x \in \mathbb{F}_{q^n}^*\right\},$$

i.e.

$$\left\{\sum_{i=0}^{n-1} \alpha_i x^{q^i} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{cx + d\sum_{i=0}^{n-1} \beta_i x^{q^i} : x \in \mathbb{F}_{q^n}^*\right\}.$$

By (a) of Lemma 2.2, $\alpha_0 = c + d\beta_0$. As $\alpha_0 = \beta_0 = 0$, c must be 0. Hence

$$\left\{\sum_{i=1}^{n-1} \alpha_i x^{q^i-1} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{d\sum_{i=1}^{n-1} \beta_i x^{q^i-1} : x \in \mathbb{F}_{q^n}^*\right\}. \tag{41}$$

Lemma 5.4 *Suppose $f = \psi_{h,t}$, $g = \psi_{k,t}$ with $t > 4$. If there exists d such that (41) holds, then $(h/k)^{q^2+1} = 1$ which means U_h is $\Gamma L(2, q^n)$-equivalent to U_k.*

Proof By (b) of Lemma 2.2,

$$\alpha_j \alpha_{n-j}^{q^j} = d^{q^j+1} \beta_k \beta_{n-j}^{q^j}$$

for $j = 1, 2, \cdots, n-1$. Plugging the coefficients of $\psi_{h,t}$ and $\psi_{k,t}$, we get

$$\left(h^{1-q^{2t-1}}\right)^q = d^{q+1}\left(k^{1-q^{2t-1}}\right)^q \text{ and } \left(-h^{1-q^{t+1}}\right)^{q^{t-1}} = d^{q^{t-1}+1}\left(-k^{1-q^{t+1}}\right)^{q^{t-1}}.$$

By setting $\ell = h/k$, we get

$$\begin{cases} \ell^{q-1} = d^{q+1}, \\ \ell^{q^{t-1}-1} = d^{q^{t-1}+1}. \end{cases} \tag{42}$$

From (42), we derive

$$d^{(q+1)(q^{t-2}+q^{t-3}+\cdots+1)} = \ell^{q^{t-1}-1} = d^{q^{t-1}+1},$$

which means $d^{2q(q^{t-3}+\cdots+1)} = 1$. Hence $d^{q^{t-2}-1} = d^{2(q^{t-3}+\cdots+1)\cdot\frac{q-1}{2}} = 1$. It follows that $\ell^{q^{t-1}-1} = d^{q^{t-1}+1} = d^{q+1} = \ell^{q-1}$, whence $\ell^{q^{t-2}} = \ell$.

As $h^{q^t+1} = k^{q^t+1} = -1$, $\ell^{q^t} = 1/\ell$. By $\ell^{q^{t-2}} = \ell$, we get $\ell^{q^2+1} = 1$. By Theorem 4.2, U_h is $\Gamma L(2, q^n)$-equivalent to U_k. □

Next we consider the case $b \neq 0$. Without loss of generality, we assume that $b = 1$. Then

$$\frac{cx + dg(x)}{ax + g(x)} = \frac{(c - da)x + d(ax + g(x))}{ax + g(x)} = \frac{\bar{c}x}{ax + g(x)} + d,$$

for any $x \in \mathbb{F}_{q^n}^*$, where $\bar{c} = c - da \neq 0$. Noting that $ax + g(x) = 0$ must have no nonzero solution,

$$\frac{\bar{c}x}{ax + g(x)} + d = \frac{\bar{c}\bar{g}(y)}{y} + d,$$

where $\bar{g}(y) = \sum_{i=0}^{n-1} \gamma_i y^{q^i}$ is the inverse of the map $x \mapsto ax + g(x)$.

Furthermore, (40) becomes

$$\left\{ \sum_{i=1}^{n-1} \alpha_i x^{q^i - 1} : x \in \mathbb{F}_{q^n}^* \right\} = \left\{ \bar{c} \sum_{i=1}^{n-1} \gamma_i x^{q^i - 1} + d + \bar{c}\gamma_0 : x \in \mathbb{F}_{q^n}^* \right\}.$$

By (a) of Lemma 2.2,

$$d + \bar{c}\gamma_0 = 0. \tag{43}$$

Thus

$$\left\{ \frac{1}{\bar{c}} \sum_{i=1}^{n-1} \alpha_i x^{q^i - 1} : x \in \mathbb{F}_{q^n}^* \right\} = \left\{ \sum_{i=1}^{n-1} \gamma_i x^{q^i - 1} : x \in \mathbb{F}_{q^n}^* \right\}. \tag{44}$$

Lemma 5.5 *Let $f = \psi_{h,t}$, $g = \psi_{k,t}$ with $t > 4$. Suppose that there exist a, c and d such that (44) holds.*

(a) *If t is even, then a must be* 0.
(b) *If t is odd and $a \neq 0$, then $f = g$.*

In particular, when $a = 0$, $\gamma_0 = d = 0$.

The proof of the above lemma is one of the most technical parts in this paper. Let us first give a sketch of it. The difficulty lies in the unknown coefficients γ_i for $i = 1, \ldots, n - 1$. Thus we should derive necessary conditions on them as many as possible.

First, as $f = \psi_{h,t}$, there are only four terms with nonzero coefficients in the polynomials of the left-hand-side of (44). Hence, by Lemma 2.2 (b) and (c), all the other terms with zero coefficients can provide many equations on γ_i; see (45) to (48).

Secondly, by definition, γ_i is defined by the inverse of $\psi_{k,t}$ which provides us another set of restrictions on γ_i; see (51) to (57).

By all these restrictions on γ_i and some further computation into four different cases, we can prove that $a = 0$ or a has to satisfy $\frac{1}{a^{q^t}} = -k^{q - q^{2t-1}} \frac{1}{a}$; see (59). By plugging (59) into some other necessary conditions derived from (44), we can finish the proof.

Proof By the second identity in Lemma 2.2, we know that

$$\gamma_j \gamma_{2t-j} = 0, \tag{45}$$

for $j \in \{1, 2, \cdots, 2t-1\} \setminus \{1, t-1, t+1, 2t-1\}$,

$$\gamma_1 \gamma_{2t-1}^q = \left(\frac{1}{\bar{c}}\right)^{q+1} \tau^q, \tag{46}$$

and

$$\gamma_{t-1} \gamma_{t+1}^{q^{t-1}} = \left(\frac{1}{\bar{c}}\right)^{1+q^{t-1}} \theta^{q^{t-1}}, \tag{47}$$

where $\tau = h^{1-q^{2t-1}}$ and $\theta = -h^{1-q^{t+1}} = h^{1+q}$.

By the third identity in Lemma 2.2, we have

$$\gamma_1 \gamma_{j-1}^q \gamma_{2t-j}^{q^j} + \gamma_j \gamma_{2t-1}^q \gamma_{2t-j+1}^{q^j} = 0, \tag{48}$$

for $j \in \{2, 3, \cdots, n-1\}$. Letting $j = 2$, we obtain

$$\gamma_1 \gamma_1^q \gamma_{2t-2}^{q^2} + \gamma_2 \gamma_{2t-1}^q \gamma_{2t-1}^{q^2} = 0.$$

As $\gamma_2 \gamma_{2t-2} = 0$ and $\gamma_1 \gamma_{2t-1} \neq 0$, we derive $\gamma_2 = \gamma_{2t-2} = 0$. Similarly, by letting $j = t-1$, we have

$$\gamma_1 \gamma_{t-2}^q \gamma_{t+1}^{q^{t-1}} + \gamma_{t-1} \gamma_{2t-1}^q \gamma_{t+2}^{q^{t-1}} = 0.$$

Since $\gamma_{t-2}\gamma_{t+2} = 0$ and $\gamma_1, \gamma_{t+1}, \gamma_{t-1}, \gamma_{t+1} \neq 0$, from the above equation we deduce

$$\gamma_{t-2} = \gamma_{t+2} = 0.$$

Moreover, by (45), (48) and replacing $j-1$ by j in (48),

$$\gamma_j \neq 0 \Rightarrow \gamma_{2t-j} = \gamma_{2t-j+1} = \gamma_{2t-j-1} = 0, \tag{49}$$

for $j \in \{1, 2, \cdots, 2t-1\} \setminus \{1, t-1, t+1, 2t-1\}$.

Now, we will use the fact that $\bar{g}(ax + g(x)) = x$, namely,

$$\bar{g}(ax + x^q + x^{q^{t-1}} + ux^{q^{t+1}} + vx^{q^{2t-1}}) = x, \tag{50}$$

for all $x \in \mathbb{F}_{q^n}$, where $u = -k^{1-q^{t+1}}$ and $v = k^{1-q^{2t-1}}$. The coefficient of x^{q^j} in the left-hand-side of (50) is

$$a^{q^j}\gamma_j + \gamma_{j-1} + \gamma_{j+t+1} + u^{q^{j+t-1}}\gamma_{j+t-1} + v^{q^{j+1}}\gamma_{j+1}. \tag{51}$$

By letting $j = 0, 1, 2t-1, t+1, t-1$ and t in (51) and comparing it with the right-hand-side of (50), we get

$$a\gamma_0 + \gamma_{2t-1} + \gamma_{t+1} + u^{q^{t-1}}\gamma_{t-1} + v^q\gamma_1 = 1, \tag{52}$$

$$a^q\gamma_1 + \gamma_0 = 0, \tag{53}$$

$$a^{q^{2t-1}}\gamma_{2t-1} + v\gamma_0 = 0, \tag{54}$$

$$a^{q^{t+1}}\gamma_{t+1} + u\gamma_0 = 0, \tag{55}$$

$$a^{q^{t-1}}\gamma_{t-1} + \gamma_0 = 0, \tag{56}$$

$$\gamma_{t-1} + \gamma_1 + u^{q^{2t-1}}\gamma_{2t-1} + v^{q^{t+1}}\gamma_{t+1} = 0. \tag{57}$$

Here we have used the result that $\gamma_t = \gamma_2 = \gamma_{2t-2} = \gamma_{t+2} = \gamma_{t-2} = 0$.

It is clear that if $a = 0$, then γ_0 must be 0. By (43), $d = 0$.

Assume that $a \neq 0$. By (53), (54), (55) and (56) into (52) and (57), we see that $\gamma_0 \neq 0$ is completely determined by a, and

$$-\gamma_0\left(\frac{1}{a^{q^{t-1}}} + \frac{1}{a^q} + \frac{u^{q^{2t-1}}v}{a^{q^{2t-1}}} + \frac{v^{q^{t+1}}u}{a^{q^{t+1}}}\right) = 0,$$

respectively. Recall that $u = -k^{1-q^{t+1}}$, $v = k^{1-q^{2t-1}}$ and $k^{q^t} = -1/k$, from the above equation we deduce

$$\frac{1}{a^{q^{t-1}}} + \frac{1}{a^q} + \frac{k^2}{a^{q^{2t-1}}} + \frac{k^2}{a^{q^{t+1}}} = 0.$$

Therefore

$$\frac{1}{a^{q^{t-1}}} + \frac{1}{a^q} = -k^2\left(\frac{1}{a^{q^{t-1}}} + \frac{1}{a^q}\right)^{q^t}. \tag{58}$$

Our goal of the next step is to prove

$$\frac{1}{a^{q^t}} = -k^{q-q^{2t-1}}\frac{1}{a}, \tag{59}$$

always holds.

Let $j = 2, t+2, 2t-2, t-2$ in (51), we have

$$\gamma_1 + \gamma_{t+3} + u^{q^{t+1}}\gamma_{t+1} + v^{q^3}\gamma_3 = 0, \tag{60}$$

$$\gamma_{t+1}+\gamma_3+u^q\gamma_1+v^{q^{t+3}}\gamma_{t+3}=0, \tag{61}$$

$$\gamma_{2t-3}+\gamma_{t-1}+u^{q^{t-3}}\gamma_{t-3}+v^{q^{2t-1}}\gamma_{2t-1}=0, \tag{62}$$

$$\gamma_{t-3}+\gamma_{2t-1}+u^{q^{2t-3}}\gamma_{2t-3}+v^{q^{t-1}}\gamma_{t-1}=0. \tag{63}$$

Depending on the value of γ_3, γ_{t+3}, γ_{t-3} and γ_{2t-3}, we separate the proof of (59) into four different cases.

Case (i) $\gamma_3=\gamma_{t+3}=0$. By (53), (55) and (60),

$$-\frac{u}{a^{q^{t+1}}}\gamma_0=\gamma_{t+1}=-u^q\gamma_1=\frac{u^q}{a^q}\gamma_0,$$

which means $\frac{1}{a^{q^t}}=-u^{1-q^{2t-1}}\frac{1}{a}=-k^{q-q^{2t-1}}\frac{1}{a}$.

Case (ii) $\gamma_{t-3}=\gamma_{2t-3}=0$. By a similar computation of (62) as in Case (i), we get (59) again.

Case (iii) $\gamma_3\neq 0$ and $\gamma_{t-3}\neq 0$. By (49), $\gamma_{2t-3}=\gamma_{2t-4}=\gamma_{t+3}=\gamma_{t+4}=0$. Now, (60) and (61) become

$$\gamma_1+k^{-q^2-q}\gamma_{t+1}+k^{q^3-q^2}\gamma_3=0,$$

$$\gamma_3+\gamma_{t+1}+k^{q^2+q}\gamma_1=0.$$

Canceling γ_3, we get

$$(1-k^{q^3+q})\gamma_{t+1}=-(1-k^{q^3+q})k^{q^2+q}\gamma_1.$$

By Proposition 3.2, $k^{q^2+1}\neq 1$. Hence, $\gamma_{t+1}=-k^{q^2+q}\gamma_1$. By plugging (53) and (55) into it, we derive (59).

Case (iv) $\gamma_{t+3}\neq 0$ and $\gamma_{2t-3}\neq 0$. By (49), $\gamma_{t-3}=\gamma_{t-4}=\gamma_3=\gamma_4=0$. As in Case (iii), by canceling γ_{t+3} using (60) and (61), we obtain (59) again.

By (49), we have covered all possible cases. Therefore, (59) is proved.

Now we are ready to prove (a) and (b). Our strategy is to give a precise expression for a, which is strong enough to prove (a). Then we further use (46) to get more restrictions on the value of h which leads to (b).

Plugging (59) in (58), we have

$$\frac{1}{a^{q^{t-1}}}\left(1-k^{1+q^{2t-2}}\right)+\frac{1}{a^q}\left(1-k^{1+q^2}\right)=0,$$

that is

$$\left(\frac{1}{a^q}\left(1-k^{1+q^2}\right)\right)^{q^{t-2}}-k^{-1-q^{2t-2}}\frac{1}{a^q}\left(1-k^{1+q^2}\right)=0.$$

By $k^{q^{t-2}} = -k^{-q^{2t-2}}$, we have

$$\left(\frac{k^{-1}}{a^q}\left(1-k^{1+q^2}\right)\right)^{q^{t-2}} + \frac{k^{-1}}{a^q}\left(1-k^{1+q^2}\right) = 0.$$

Therefore,

$$a = k^{-q^{2t-1}}\left(1-k^{q+q^{2t-1}}\right)\eta, \tag{64}$$

where η satisfies $\eta^{q^{t-2}} + \eta = 0$. Since $0 = (\eta^{q^{t-2}} + \eta)^{q^{t+2}} = \eta + (\eta^{q^{t-2}})^{q^4} = \eta - \eta^{q^4}$, we get $\eta \in \mathbb{F}_{q^4}$. Moreover,

$$\eta = -\eta^{q^{t-2}} = \begin{cases} -\eta^{q^3} = -\eta^q, & t \equiv 1 \pmod 4, \\ -\eta = 0, & t \equiv 2 \pmod 4, \\ -\eta^q, & t \equiv 3 \pmod 4, \\ -\eta^{q^2}, & t \equiv 0 \pmod 4. \end{cases}$$

Hence

$$\eta^{q^2-1} = \begin{cases} 1, & t \equiv 1 \pmod 4, \\ 0, & t \equiv 2 \pmod 4, \\ 1, & t \equiv 3 \pmod 4, \\ -1, & t \equiv 0 \pmod 4. \end{cases} \tag{65}$$

Substitute a in (59) by (64),

$$-k^{q-q^{2t-1}}k^{-q^{t-1}}(1-k^{q^{t+1}+q^{t-1}})\eta^{q^t} = k^{-q^{2t-1}}(1-k^{q+q^{2t-1}})\eta,$$

which equals

$$k^q(1-k^{-q-q^{2t-1}})\eta^{q^t} = k^{-q^{2t-1}}(1-k^{q+q^{2t-1}})\eta.$$

It implies

$$\eta^{q^t} = -\eta. \tag{66}$$

Together with $\eta^{q^{t-2}} + \eta = 0$, we deduce $\eta^{q^2} = \eta$. It contradicts (65) when $t \equiv 0 \pmod 4$. Therefore, when t is even, a must be 0 and (a) is proved.

Finally, let us plugging (53) and (54) into (46), we have

$$(\bar{c}\gamma_0)^{q+1} = \frac{\tau^q}{\upsilon^q}a^{q+1} = \ell^{q-1}a^{q+1}, \tag{67}$$

where $\ell = h/k$ which means $\ell^{q^t} = 1/\ell$.

Similarly, by (56) and (55) into (47)

$$(\bar{c}\gamma_0)^{q^{t-1}+1} = \frac{\theta^{q^{t-1}}}{u^{q^t-1}} a^{q^{t-1}+1} = \ell^{q^{t-1}-1} a^{q^{t-1}+1}. \tag{68}$$

Raising (67) to its $\frac{q^{t-1}+1}{2}$-th power and (68) to its $\frac{q+1}{2}$-th power and canceling $(\bar{c}\gamma_0)^{\frac{1}{2}(q+1)(q^{t-1}+1)}$ and $a^{\frac{1}{2}(q+1)(q^{t-1}+1)}$, we obtain

$$\ell^{q^{t-2}-1} = 1.$$

Again, by $\ell^{q^t+1} = 1$, we have $\ell^{q^2+1} = 1$ which means $\ell^{\gcd(q^2+1, q^t+1)} = 1$. Therefore, since t is odd, we get $\ell^2 = 1$, and (b) is proved. □

Now we are ready to prove Theorem 5.1.

Proof of Theorem 5.1 Suppose that $f = \psi_{h,t}$, $g = \psi_{k,t}$, and L_f is $P\Gamma L(2, q^n)$-equivalent to L_g. Then there exists an invertible matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over $\mathbb{F}_{q^n}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that

$$\left\{\frac{f(x)}{x} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{\frac{cx^\sigma + d(g(x))^\sigma}{ax^\sigma + b(g(x))^\sigma} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{\frac{cx + d\bar{g}(x)}{ax + b\bar{g}(x)} : x \in \mathbb{F}_{q^n}^*\right\},$$

where $\bar{g}(x) = \psi_{k^\sigma,t}(x)$.

For a given h satisfying $h^{q^t+1} = -1$, let ε_h denote the number of k for which U_k is $\Gamma L(2, q^n)$-equivalent to U_h.

Depending on the value of b, we separate the remainder part of the proof into two cases:

Case (a) $b = 0$. By Lemma 5.4, $(h/k^\sigma)^{q^2+1} = 1$ which means that U_h is $\Gamma L(2, q^n)$-equivalent to U_{k^σ}. Thus there are exactly ε_h choices of k for which $L_{k,t}$ is equivalent to $L_{h,t}$.

Case (b) $b \neq 0$. Without loss of generality, we assume $b = 1$ and $f \neq \bar{g}$. By Lemma 5.5, $d = a = 0$. Thus

$$\left\{\frac{f(x)}{x} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{\frac{cx}{\bar{g}(x)} : x \in \mathbb{F}_{q^n}^*\right\}.$$

Suppose that there is another $\tilde{g}(x) = \psi_{\tilde{k},t}(x)$ for certain $\tilde{k} \in \mathbb{F}_{q^{2t}}$ satisfying $\tilde{k}^{q^t+1} = -1$ and

$$\left\{\frac{f(x)}{x} : x \in \mathbb{F}_{q^n}^*\right\} = \left\{\frac{\tilde{c}x}{\tilde{g}(x)} : x \in \mathbb{F}_{q^n}^*\right\}$$

for some $\tilde{c} \in \mathbb{F}_{q^{2t}}$. Then

$$\left\{ \frac{\bar{g}(x)}{x} : x \in \mathbb{F}_{q^n}^* \right\} = \left\{ \frac{c}{\tilde{c}} \cdot \frac{\tilde{g}(x)}{x} : x \in \mathbb{F}_{q^n}^* \right\}.$$

By Lemma 5.4, $(\tilde{k}/k^\sigma)^{q^2+1} = 1$ which means that U_{k^σ} is $\Gamma L(2, q^n)$-equivalent to $U_{\tilde{k}}$. Hence, for the case $b \neq 0$, there are exactly $\varepsilon_{\tilde{k}}$ choices of k for which $L_{k,t}$ is equivalent to $L_{h,t}$.

Finally we combine Case (a) and Case (b), for a given $L_{h,t}$. Noting that $|\{h \in \mathbb{F}_{q^n} : h^{q^t+1} = -1\}| = q^t + 1$, there are exactly

$$M = \frac{q^t+1}{\varepsilon_h} + \frac{q^t+1}{\varepsilon_{\tilde{k}}}$$

inequivalent $L_{h,t}$ defined by (39). Recall that

$$\varepsilon_h \leq nr\xi_h = \begin{cases} 4rt, & t \not\equiv 2 \pmod 4; \\ 2(q^2+1)rt, & t \equiv 2 \pmod 4), \end{cases}$$

for every possible choice of h; see the proof of Corollary 4.3. We obtain the lower bound of M. □

Remark 5.6 By Theorem 5.1, Family (39) contains much more inequivalent elements compared with the known constructions for infinitely many n listed in Table 1. Therefore, this family must be new.

Acknowledgements The authors express their gratitude to the anonymous reviewers for their detailed and constructive comments which helped to improve the presentation of the paper. The research that led to the present paper was partially supported by a grant of the group GNSAGA of INdAM. Yue Zhou is partially supported by Training Program for Excellent Young Innovators of Changsha (No. kq2106006).

References

1. Bartoli, D., Giulietti, M., Marino, G., Polverino, O.: Maximum scattered linear sets and complete caps in Galois spaces. Combinatorica **38**(2), 255–278 (2018)
2. Bartoli, D., Giulietti, M., Zini, G.: Towards the classification of exceptional scattered polynomials. arXiv:2206.13795
3. Bartoli, D., Montanucci, M.: On the classification of exceptional scattered polynomials. J. Comb. Theory Ser. A **179**, 105386 (2021)
4. Bartoli, D., Zanella, C., Zullo, F.: A new family of maximum scattered linear sets in PG(1, q^6). Ars Math. Contemp. **19**(1), 125–145 (2020)
5. Bartoli, D., Zhou, Y.: Exceptional scattered polynomials. J. Algebra **509**, 507–534 (2018)
6. Blokhuis, A., Lavrauw, M.: Scattered spaces with respect to a spread in PG(n, q). Geom. Dedic. **81**(1), 231–243 (2000)
7. Couvreur, A., Debris-Alazard, T., Gaborit, P.: On the hardness of code equivalence problems in rank metric. [cs, math]. arXiv:2011.04611 (2020)
8. Csajbók, B., Marino, G., Polverino, O.: Classes and equivalence of linear sets in PG(1, q^n). J. Comb. Theory Ser. A **157**, 402–426 (2018)

9. Csajbók, B., Marino, G., Polverino, O., Zanella, C.: A new family of MRD-codes. Linear Algebra Appl. **548**, 203–220 (2018)
10. Csajbók, B., Marino, G., Zullo, F.: New maximum scattered linear sets of the projective line. Finite Fields Appl. **54**, 133–150 (2018)
11. Csajbók, B., Zanella, C.: On the equivalence of linear sets. Des. Codes Cryptogr. **81**(2), 269–281 (2016)
12. Delsarte, P.: Bilinear forms over the finite field, with applications to coding theory. J. Comb. Theory Ser. A **25**, 226–241 (1978)
13. Ferraguti, A., Micheli, G.: Exceptional scatteredness in prime degree. J. Algebra **565**, 691–701 (2021)
14. Gupta, S., Longobardi, G., Trombetti, R.: On the equivalence issue of a class of 2-dimensional linear Maximum Rank Distance codes. Preprint at arXiv: 2208.09701 (2022)
15. Lavrauw, M., Polverino, O.: Finite semifields and Galois geometry, chapter. In: De Beule, J., Storme, L. (eds.) Current Research Topics in Galois Geometry. NOVA Academic Publishers, Hauppauge (2011)
16. Lavrauw, M., Van de Voorde, G.: Field reduction and linear sets in finite geometry. In: Kyureghyan, G., Mullen, G., Pott, A. (eds.) Contemporary Mathematics, vol. 632, pp. 271–293. American Mathematical Society, Providence (2015)
17. Liebhold, D., Nebe, G.: Automorphism groups of Gabidulin-like codes. Arch. Math. **107**(4), 355–366 (2016)
18. Longobardi, G., Zanella, C.: Linear sets and MRD-codes arising from a class of scattered linearized polynomials. J. Algebr. Comb. **53**(3), 639–661 (2021)
19. Lunardon, G.: Normal spreads. Geom. Dedic. **75**(3), 245–261 (1999)
20. Lunardon, G., Polverino, O.: Blocking sets and derivable partial spreads. J. Algebr. Comb. **14**(1), 49–56 (2001)
21. Lunardon, G., Trombetti, R., Zhou, Y.: On kernels and nuclei of rank metric codes. J. Algebr. Comb. **46**(2), 313–340 (2017)
22. Lunardon, G., Trombetti, R., Zhou, Y.: Generalized twisted Gabidulin codes. J. Comb. Theory Ser. A **159**, 79–106 (2018)
23. Marino, G., Montanucci, M., Zullo, F.: MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$. Linear Algebra Appl. **591**, 99–114 (2020)
24. Neri, A., Santonastaso, P., Zullo, F.: Extending two families of maximum rank distance codes. Finite Fields Appl. **81**, 102045 (2022)
25. Polverino, O.: Linear sets in finite projective spaces. Discret. Math. **22**, 3096–3107 (2010)
26. Polverino, O., Zullo, F.: Connections between scattered linear sets and MRD-codes. Bull. ICA **89**, 46–74 (2020)
27. Sheekey, J.: A new family of linear maximum rank distance codes. Adv. Math. Commun. **10**(3), 475–488 (2016)
28. Sheekey, J.: MRD codes: constructions and connections. In: Schmidt, K.-U., Winterhof, A. (eds.) Combinatorics and Finite Fields. Difference Sets, Polynomials, Pseudorandomness and Applications, pp. 255–286. De Gruyter, Berlin (2019)
29. Sheekey, J., Van de Voorde, G.: Rank-metric codes, linear sets, and their duality. Des. Codes Cryptogr. **88**, 655–675 (2020)
30. Tang, W., Zhou, Y., Zullo, F.: On the automorphism groups of Lunardon–Polverino scattered linear sets. Discret. Math. **346**(5), 113313 (2023)
31. Zanella, C., Zullo, F.: Vertex properties of maximum scattered linear sets of $\mathrm{PG}(1, \mathrm{q}^{\mathrm{n}})$. Discret. Math. **343**(5), 111800 (2020)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.