Linear Algebra and its Applications 702 (2024) 143–160

Contents lists available at ScienceDirect

Linear Algebra and its Applications

journal homepage: www.elsevier.com/locate/laa

New scattered linearized quadrinomials

Valentino Smaldore [a], Corrado Zanella [a,*], Ferdinando Zullo [b]

[a] *Dipartimento di Tecnica e Gestione dei Sistemi Industriali, Università degli Studi di Padova, Stradella S. Nicola, 3, 36100 Vicenza VI, Italy*
[b] *Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", Viale Lincoln 5, 81100 Caserta CE, Italy*

ARTICLE INFO

Article history:
Received 28 February 2024
Received in revised form 10 August 2024
Accepted 10 August 2024
Available online 21 August 2024
Submitted by R.A. Brualdi

MSC:
11T71
11T06
94B05

Keywords:
Scattered polynomials
Linearized polynomials
MRD codes

ABSTRACT

Let $1 < t < n$ be integers, where t is a divisor of n. An R-q^t-partially scattered polynomial is a q-polynomial f in $\mathbb{F}_{q^n}[X]$ that satisfies the condition that for all $x, y \in \mathbb{F}_{q^n}^*$ such that $x/y \in \mathbb{F}_{q^t}$, if $f(x)/x = f(y)/y$, then $x/y \in \mathbb{F}_q$; f is called scattered if this implication holds for all $x, y \in \mathbb{F}_{q^n}^*$. Two polynomials in $\mathbb{F}_{q^n}[X]$ are said to be equivalent if their graphs are in the same orbit under the action of the group $\Gamma\mathrm{L}(2, q^n)$. For $n > 8$ only three families of scattered polynomials in $\mathbb{F}_{q^n}[X]$ are known: (i) monomials of pseudoregulus type, (ii) binomials of Lunardon-Polverino type, and (iii) a family of quadrinomials defined in [1,10] and extended in [8,13]. In this paper we prove that the polynomial $\varphi_{m,q^J} = X^{q^{J(t-1)}} + X^{q^{J(2t-1)}} + m(X^{q^J} - X^{q^{J(t+1)}}) \in \mathbb{F}_{q^{2t}}[X]$, q odd, $t \geq 3$ is R-q^t-partially scattered for every value of $m \in \mathbb{F}_{q^t}^*$ and J coprime with $2t$. Moreover, for every $t > 4$ and $q > 5$ there exist values of m for which $\varphi_{m,q}$ is scattered and new with respect to the polynomials mentioned in (i), (ii) and (iii) above. The related linear sets are of ΓL-class at least two.

© 2024 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

* Corresponding author.
E-mail addresses: valentino.smaldore@unipd.it (V. Smaldore), corrado.zanella@unipd.it (C. Zanella), ferdinando.zullo@unicampania.it (F. Zullo).

https://doi.org/10.1016/j.laa.2024.08.012
0024-3795/© 2024 The Author(s). Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

In this paper $q = p^\varepsilon$ denotes a power of a prime p. Let n be a positive integer. A *q-polynomial*, or *$\mathbb{F}_q$-linearized polynomial*, in $\mathbb{F}_{q^n}[X]$ is of type

$$f = \sum_{i=0}^{d} a_i X^{q^i}, \quad a_i \in \mathbb{F}_{q^n},\ i = 0, 1, \ldots, d. \tag{1}$$

If $a_d \neq 0$, then the q-polynomial f has *q-degree d*. The set of q-polynomials over $\mathbb{F}_{q^n}$ is denoted by $L_{n,q}$. Such a set, equipped with the operations of sum, multiplication by elements of $\mathbb{F}_q$, and the composition, results to be an $\mathbb{F}_q$-algebra. The quotient algebra $\mathcal{L}_{n,q} = L_{n,q}/(X^{q^n} - X)$ is isomorphic to the $\mathbb{F}_q$-algebra of the $\mathbb{F}_q$-linear endomorphisms of $\mathbb{F}_{q^n}$. Hence, for every $\mathbb{F}_q$-linear endomorphism Φ of $\mathbb{F}_{q^n}$ there exists a unique q-polynomial f of q-degree less than n such that $f(x) = \Phi(x)$ for any $x \in \mathbb{F}_{q^n}$. By abuse of notation, any $f \in L_{n,q}$ is identified with the class $f + (X^{q^n} - X) \in \mathcal{L}_{n,q}$.

q-polynomials have found many applications in various areas of combinatorics, coding theory and cryptography. Special attention has been paid to *scattered polynomials*, introduced by Sheekey in [16], in the context of optimal codes in the rank metric, as we will see later. A *scattered polynomial* is an $f \in \mathcal{L}_{n,q}$ such that for any $x, y \in \mathbb{F}_{q^n}^*$,

$$\frac{f(x)}{x} = \frac{f(y)}{y} \implies \frac{x}{y} \in \mathbb{F}_q. \tag{2}$$

A generalization of the notion of scattered polynomials was recently introduced in [9]. Let f be a q-polynomial in $\mathcal{L}_{n,q}$, and t a nontrivial divisor of n; so, $n = tt'$, and $1 < t, t' < n$. We say that f is L-*q^t-partially scattered* if for any $x, y \in \mathbb{F}_{q^n}^*$,

$$\frac{f(x)}{x} = \frac{f(y)}{y} \implies \frac{x}{y} \in \mathbb{F}_{q^t}, \tag{3}$$

and that f is R-*q^t-partially scattered* if for any $x, y \in \mathbb{F}_{q^n}^*$,

$$\frac{f(x)}{x} = \frac{f(y)}{y} \text{ and } \frac{x}{y} \in \mathbb{F}_{q^t} \implies \frac{x}{y} \in \mathbb{F}_q. \tag{4}$$

A q-polynomial is scattered if and only if it is both L-q^t- and R-q^t-partially scattered.

The *graph* of $f \in \mathbb{F}_{q^n}[X]$ is $U_f = \{(x, f(x)) \colon x \in \mathbb{F}_{q^n}\}$. If $f \in \mathcal{L}_{n,q}$, then U_f is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^2$. We say that two polynomials f and g in $\mathcal{L}_{n,q}$ are ΓL-*equivalent*, or simply *equivalent*, if their graphs are in the same orbit under the action of the group $\Gamma\mathrm{L}(2, q^n)$. Up to such a notion of equivalence, only three families of scattered polynomials in $\mathcal{L}_{n,q}$ are known for $n > 8$:

(*i*) X^{q^s}, with $\gcd(s, n) = 1$, known as *pseudoregulus type*;

(*ii*) $X^{q^{n-s}} + \delta X^{q^s}$, with $\gcd(s,n) = 1$ and $\mathrm{N}_{q^n/q}(\delta) = \delta^{\frac{q^n-1}{q-1}} \neq 0, 1$, known as *Lunardon-Polverino* type [12,16];

(*iii*) $\psi_{s,h} = X^{q^s} + X^{q^{s(t-1)}} + h^{1+q^s} X^{q^{s(t+1)}} + h^{1-q^{s(2t-1)}} X^{q^{s(2t-1)}} \in \mathcal{L}_{2t,q}$, where q is odd, $\gcd(s, 2t) = 1$, $h \in \mathbb{F}_{q^{2t}}$ and $h^{q^t+1} = -1$ [1,8,10,13].

It is convenient to split the family (*iii*) into two separate families (*iii-a*) of all polynomials $\psi_{s,h}$ such that $h \in \mathbb{F}_{q^t}$, and (*iii-b*), where $h \notin \mathbb{F}_{q^t}$.

One of the reasons that scattered polynomials and their generalizations have attracted so much attention is their connection to optimal codes in the theory of rank-metric codes. See [15,16] for a general overview of this topic. Rank-metric codes are sets of $n \times m$ matrices over a finite field $\mathbb{F}_q$, endowed with the rank metric. When $n = m$, the rank-metric codes can be represented in terms of q-polynomials, since the $\mathbb{F}_q$-algebra $\mathbb{F}_q^{n\times n}$ is isomorphic to $\mathcal{L}_{n,q}$. Of particular interest is the family of *maximum rank distance (MRD)* codes, which are of maximum size for given n and given minimum rank distance. The first construction of a family of MRD codes was due to Delsarte [3] and independently to Gabidulin [4]. The codes of this family are now known as the *Gabidulin codes*. Sheekey in [16] pointed out a way to construct special classes of MRD codes: if $f \in \mathcal{L}_{n,q}$ is a scattered polynomial then $\mathcal{C}_f = \langle X, f\rangle_{\mathbb{F}_{q^n}}$ is an MRD code of size q^{2n} and minimum distance $n-1$. In the same paper, he also proved that the equivalence of q-polynomials corresponds to the equivalence of rank-metric codes. Therefore, the scattered polynomials (*i*), (*ii*) and (*iii*) give rise to three disjoint families of MRD codes.

The *adjoint* of a q-polynomial $f = \sum_{i=0}^{n-1} a_i X^{\sigma^i}$ with respect to the trace form is the polynomial $f^\top$ which satisfies $\mathrm{Tr}_{q^n/q}(f(x)y) = \mathrm{Tr}_{q^n/q}(xf^\top(y))$ for every $x, y \in \mathbb{F}_{q^n}$ ([1]). It holds

$$f^\top = \sum_{i=0}^{n-1} a_i^{\sigma^{n-i}} X^{\sigma^{n-i}}.$$

Such $f^\top$ is scattered if and only if f is. Even, f and $f^\top$ determine the same linear set $L_f = L_{f^\top}$ [2]. However, the polynomials f and $f^\top$ need not to be equivalent. The classes (*i*), (*ii*), and (*iii-b*) described above contain their own adjoints up to equivalence. Furthermore, every polynomial in the collection (*iii-b*) is equivalent to its adjoint [8, Theorem 4.6], [13, Proposition 4.17].

The scattered polynomials can also be used to construct scattered linear sets. We refer the reader to [6,14,15] for generalities on this topic. Any linear set of rank n in the projective line $\mathrm{PG}(1, q^n)$ can be defined, up to the action of $\mathrm{GL}(2, q^n)$, by a q-polynomial f as follows

$$L_f = \{\langle (x, f(x))\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\},$$

[1] $\mathrm{Tr}_{q^n/q}(x) = x + x^q + \cdots + x^{q^{n-1}}$ for $x \in \mathbb{F}_{q^n}$.

and we say that it is *scattered* if $|L_f| = (q^n - 1)/(q - 1)$. It is a straightforward check that f is scattered if and only if L_f is scattered. Scattered linear sets on the projective line have been related to various objects in Galois geometries, such as linear minimal blocking sets of largest order, translation planes and many more; see for example [6,10,14].

In this paper, we study the q-polynomials

$$\varphi_{m,\sigma} = X^{\sigma^{t-1}} + X^{\sigma^{2t-1}} + m(X^{\sigma} - X^{\sigma^{t+1}}) \in \mathcal{L}_{2t,q},$$

where $t \geq 3$, $m \in \mathbb{F}_{q^t}^*$, $x \mapsto x^{\sigma}$ is a generator of $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $\sigma = q^J$, $J \in \{1, 2, \ldots, 2t-1\}$, $\gcd(J, 2t) = 1$, and q is odd. In Section 2, we will first prove that any such $\varphi_{m,\sigma}$ is R-q^t-partially scattered, and then we will show some conditions on m that ensure that $\varphi_{m,\sigma}$ is scattered. In Section 3, we find the stabilizer of the graph of $\varphi_{m,\sigma}$ under the action of the group $\mathrm{GL}(2, q^n)$, which turns out to be an invariant for equivalence. In the last section we consider the question of equivalence between $\varphi_{m,q}$ and the known families of scattered polynomials. The adjoint $\varphi_{m,q}^{\top}$ of a scattered polynomial $\varphi_{m,q}$ is not equivalent to $\varphi_{k,q}$ for any $k \in \mathbb{F}_{q^t}$; hence, $\varphi_{m,q}$ does not belong to the family (*iii*-*b*) (Proposition 4.4). The main result of this paper is Theorem 4.7. It states that for $t > 4$, if t is even and $q > 3$ or t is odd and $q > 5$, there exists at least one scattered polynomial of type $\varphi_{m,q}$ that is not equivalent to any known scattered polynomial.

In [2] the notion of ΓL-*class* of a linear set L has been introduced, which is the number of nonequivalent polynomials f such that $L_f = L$. As a consequence of Proposition 4.4, the ΓL-class of any scattered linear set of type $L_{\varphi_{m,q}}$ is at least two.

2. A family of R- q^t-partially scattered polynomials

From now on we will assume that q is an odd prime power, $t \geq 3$ is an integer, and $n = 2t$. We will show a family of R- q^t-partially scattered polynomials in $\mathcal{L}_{n,q}$.

For $m \in \mathbb{F}_{q^n}$ and $\sigma = q^J$, $J \in \{1, \ldots, n-1\}$, $\gcd(J, n) = 1$, consider the following q-polynomials in $\mathcal{L}_{n,q}$:

$$\alpha = \alpha_{\sigma} = X^{\sigma^{t-1}} + X^{\sigma^{2t-1}} \text{ and } \beta = \beta_{m,\sigma} = m(X^{\sigma} - X^{\sigma^{t+1}}).$$

Define

$$W = \{x \in \mathbb{F}_{q^n} : x^{q^t} + x = 0\},$$

which is a one-dimensional $\mathbb{F}_{q^t}$-subspace of $\mathbb{F}_{q^n}$. Note that $x^{-1}, x^q, x^{\sigma} \in W$ for any $x \in W$, $x \neq 0$. Some results in the sequel, such as the next ones, are based on the fact that the kernel of a non-trivial $\mathbb{F}_q$-linear map of type $\Phi(x) = \sum_{i=0}^{d} a_i x^{\sigma^i}$ has dimension at most d over $\mathbb{F}_q$ (see e.g. [5, Theorem 5]).

Lemma 2.1. *The following hold:*

1. *if* $A \in \mathbb{F}_{q^t}$ *and* $B \in W$ *then* $AB \in W$*;*
2. *if* $A, B \in W$ *then* $AB \in \mathbb{F}_{q^t}$*;*
3. $\mathbb{F}_{q^{2t}} = \mathbb{F}_{q^t} \oplus W$*;*
4. $\ker(\alpha) = W$*;*
5. $\mathrm{Im}(\alpha) = \mathbb{F}_{q^t}$*;*
6. $\ker(\beta) = \mathbb{F}_{q^t}$*;*
7. $\mathrm{Im}(\beta) = W$

Proof. We only prove 4. and 5. Raising to the σ one obtains

$$\ker(\alpha) = \{x^{\sigma^t} + x = 0\}.$$

Furthermore, if $x \in W$, then $x^{\sigma^t} = (((x^{q^t})^{q^t}) \cdots)^{q^t}$, an odd number of powers, hence $x^{\sigma^t} = -x$, that is $x \in \ker(\alpha)$. This implies $W \subseteq \ker(\alpha)$, and 4. follows from $\dim_{\mathbb{F}_q} \ker(\alpha) \leq t$.

Next, noting that $\mathbb{F}_{q^t} = \{y \in \mathbb{F}_{q^n} : y^{\sigma^t} - y = 0\}$; if $y = \alpha(x)$, then

$$y^{\sigma^t} - y = (x^{\sigma^{t-1}} + x^{\sigma^{2t-1}})^{\sigma^t} - (x^{\sigma^{t-1}} + x^{\sigma^{2t-1}}) = 0. \quad \square$$

Theorem 2.2. *Let* $t \geq 3$ *be an integer. Assume* $m \in \mathbb{F}_{q^t}^*$ *and* $\sigma = q^J$, $J \in \{1, \ldots, 2t-1\}$, $\gcd(J, 2t) = 1$*. Then the polynomial*

$$\varphi_{m,\sigma} = X^{\sigma^{t-1}} + X^{\sigma^{2t-1}} + m(X^{\sigma} - X^{\sigma^{t+1}}) \in \mathcal{L}_{2t,q} \tag{5}$$

is R- q^t*-partially scattered.*

Proof. The polynomial $\varphi_{m,\sigma} = \alpha + \beta$ is R- q^t-partially scattered if and only if $\varphi_{m,\sigma}$ satisfies the condition that for any $\rho \in \mathbb{F}_{q^t}$ and $x \in \mathbb{F}_{q^n}$ such that $x \neq 0$, if

$$\varphi_{m,\sigma}(\rho x) = \rho \varphi_{m,\sigma}(x), \tag{6}$$

then $\rho \in \mathbb{F}_q$. So, suppose that (6) holds and, because of 3. of Lemma 2.1, we can write $x = x_1 + x_2$, where $x_1 \in \mathbb{F}_{q^t}$ and $x_2 \in W$. Using 1., 2., 4. and 5. of Lemma 2.1 we obtain

$$\varphi_{m,\sigma}(\rho x) = \alpha(\rho x_1) + \beta(\rho x_2)$$

and

$$\rho \varphi_{m,\sigma}(x) = \rho \alpha(x_1) + \rho \beta(x_2).$$

Since $\mathbb{F}_{q^{2t}} = \mathbb{F}_{q^t} \oplus W$, by 5. and 7. of Lemma 2.1 we have

$$\begin{cases} \alpha(\rho x_1) = \rho \alpha(x_1), \\ \beta(\rho x_2) = \rho \beta(x_2), \end{cases} \tag{7}$$

which can be rewritten as

$$\begin{cases} (\rho^{\sigma^{t-1}}-\rho)x_1^{\sigma^{t-1}}=0, \\ m(\rho^{\sigma}-\rho)x_2^{\sigma}=0, \end{cases}$$

and since $m \neq 0$ and at least one among x_1 and x_2 is nonzero, then $\rho^{\sigma^{t-1}}-\rho=0$ or $\rho^{\sigma}-\rho=0$. In each case we get $\rho \in \mathbb{F}_q$. □

In the following we show that for certain values of m the polynomial $\varphi_{m,\sigma}$ is also L- q^t-partially scattered.

Theorem 2.3. *Let $t \geq 3$ be an integer, and $W=\{x\colon x \in \mathbb{F}_{q^{2t}},\, x^{q^t}+x=0\}$. Assume $\sigma=q^J$, $J \in \{1,\dots,2t-1\}$, $\gcd(J,2t)=1$. If $m \in \mathbb{F}_{q^t}$ is neither a $(q-1)$-th power nor a $(q+1)$-th power of any element of W then the polynomial $\varphi_{m,\sigma}=X^{\sigma^{t-1}}+X^{\sigma^{2t-1}}+m(X^{\sigma}-X^{\sigma^{t+1}}) \in \mathcal{L}_{2t,q}$ is scattered.*

Proof. By Theorem 2.2, it is enough to prove that $\varphi_{m,\sigma}$ is L- q^t-partially scattered; that is, it satisfies the condition that for any $\rho, x \in \mathbb{F}_{q^n}$ such that $x \neq 0$, if

$$\varphi_{m,\sigma}(\rho x)=\rho\varphi_{m,\sigma}(x), \tag{8}$$

then $\rho \in \mathbb{F}_{q^t}$. So, suppose that (8) holds. Because of 3. of Lemma 2.1, we can write

$$\rho=h+r \text{ and } x=x_1+x_2,$$

where $h, x_1 \in \mathbb{F}_{q^t}$ and $r, x_2 \in W$. Using 1., 2., 4. and 5. of Lemma 2.1 we obtain

$$\varphi_{m,\sigma}(\rho x)=\alpha(hx_1)+\alpha(rx_2)+\beta(hx_2)+\beta(rx_1)$$

and

$$\rho\varphi_{m,\sigma}(x)=h\alpha(x_1)+h\beta(x_2)+r\alpha(x_1)+r\beta(x_2).$$

Since $\mathbb{F}_{q^{2t}}=\mathbb{F}_{q^t}\oplus W$, by 5. and 7. of Lemma 2.1 we have

$$\begin{cases} \alpha(hx_1)+\alpha(rx_2)=h\alpha(x_1)+r\beta(x_2), \\ \beta(hx_2)+\beta(rx_1)=h\beta(x_2)+r\alpha(x_1), \end{cases} \tag{9}$$

which can be rewritten as

$$\begin{cases} mx_2^{\sigma}r-x_2^{\sigma^{t-1}}r^{\sigma^{t-1}}=(h^{\sigma^{t-1}}-h)x_1^{\sigma^{t-1}}, \\ x_1^{\sigma^{t-1}}r-mx_1^{\sigma}r^{\sigma}=-m(h-h^{\sigma})x_2^{\sigma}, \end{cases}$$

and raising the first equation to the σ we obtain

$$\begin{cases} -x_2 r + m^\sigma x_2^{\sigma^2} r^\sigma = (h - h^\sigma)x_1, \\ -x_1^{\sigma^{t-1}} r + m x_1^\sigma r^\sigma = m(h - h^\sigma)x_2^\sigma. \end{cases} \tag{10}$$

Suppose by contradiction that $r \neq 0$. We divide the proof in four cases. Since J is odd, every $(\sigma - 1)$-th power (resp. $(\sigma + 1)$-th power) of an element of W is also a $(q - 1)$-th power (resp. $(q + 1)$-th power) of an element of W.

Case 1: $x_1 = 0$.

In this case $x_2 \neq 0$, and from the first equation of (10) we obtain

$$m^\sigma = x_2^{1-\sigma^2} r^{1-\sigma} = \left(x_2^{-1-\sigma} r^{-1}\right)^{\sigma-1},$$

that is $m = \delta^{q-1}$ for some $\delta \in W$, a contradiction to our assumptions.

Case 2: $x_2 = 0$.

We have $x_1 \neq 0$. From the second equation of (10) we obtain

$$m = x_1^{\sigma^{t-1}-\sigma} r^{1-\sigma} = \left(x_1^{\sigma(1+\sigma+\cdots+\sigma^{t-3})}/r\right)^{\sigma-1},$$

again a contradiction.

Case 3: $h - h^\sigma = 0$.

Argue as in Case 1. or 2, depending on whether $x_2 \neq 0$ or $x_1 \neq 0$.

Case 4: $x_1 x_2 (h - h^\sigma) \neq 0$.

We start by proving that

$$D = \det \begin{pmatrix} -x_2 & m^\sigma x_2^{\sigma^2} \\ -x_1^{\sigma^{t-1}} & m x_1^\sigma \end{pmatrix}$$

is non zero. Indeed, if $D = 0$ then, since (10) admits solutions for r and r^σ, we have

$$\text{rk} \begin{pmatrix} -x_2 & m^\sigma x_2^{\sigma^2} & (h - h^\sigma)x_1 \\ -x_1^{\sigma^{t-1}} & m x_1^\sigma & m(h - h^\sigma)x_2^\sigma \end{pmatrix} = 1,$$

and in particular

$$\det \begin{pmatrix} m^\sigma x_2^{\sigma^2} & (h - h^\sigma)x_1 \\ m x_1^\sigma & m(h - h^\sigma)x_2^\sigma \end{pmatrix} = 0,$$

that is

$$m^\sigma x_2^{\sigma^2+\sigma} - x_1^{\sigma+1} = 0 \;\Rightarrow\; m = u^{\sigma+1},$$

where

$$u = \frac{x_1^{\sigma^{t-1}}}{x_2} \in W,$$

a contradiction. Therefore $D \neq 0$. From (10) we obtain

$$r = \frac{\det\begin{pmatrix} (h-h^\sigma)x_1 & m^\sigma x_2^{\sigma^2} \\ m(h-h^\sigma)x_2^\sigma & mx_1^\sigma \end{pmatrix}}{D} = \frac{mx_1^{\sigma+1} - m^{\sigma+1}x_2^{\sigma^2+\sigma}}{D}(h-h^\sigma)$$

and

$$r^\sigma = \frac{\det\begin{pmatrix} -x_2 & (h-h^\sigma)x_1 \\ -x_1^{\sigma^{t-1}} & m(h-h^\sigma)x_2^\sigma \end{pmatrix}}{D} = \frac{-mx_2^{\sigma+1} + x_1^{\sigma^{t-1}+1}}{D}(h-h^\sigma).$$

Therefore,

$$r^{\sigma-1} = \frac{-mx_2^{\sigma+1} + x_1^{\sigma^{t-1}+1}}{mx_1^{\sigma+1} - m^{\sigma+1}x_2^{\sigma^2+\sigma}} = \frac{1}{m}(-mx_2^{\sigma+1} + x_1^{\sigma^{t-1}+1})^{1-\sigma},$$

that is m is a $(\sigma-1)$-th power of an element in W, again a contradiction.

In each of the cases analyzed, the condition $r \neq 0$ leads to a contradiction. It follows that $\rho \in \mathbb{F}_{q^t}$. □

By the following result at least one of the assumptions above cannot be removed.

Proposition 2.4. *Let $t \geq 3$. If m is a $(\sigma+1)$-th power of an element of W, then $\varphi_{m,\sigma}$ is not scattered.*

Proof. By assumption $m = w^{\sigma+1}$ where $w \in W$. Define $x_1 = 1$, $x_2 = w^{-1}$. Under these assumptions the equations in (10) coincide up to a factor with

$$-r + w^{\sigma+1}r^\sigma = w(h-h^\sigma).$$

The images of the $\mathbb{F}_q$-linear maps $r \in W \mapsto -r + w^{\sigma+1}r^\sigma \in W$ and $h \in \mathbb{F}_{q^t} \mapsto w(h-h^\sigma) \in W$ both are of $\mathbb{F}_q$-dimension at least $t-1$; this implies that their intersection is not trivial, and $r \in W$, $h \in \mathbb{F}_{q^t}$ exist such that $r \neq 0$ and (10) is satisfied. □

Proposition 2.5.

(*i*) *For any $t \geq 3$ there are precisely $(q^t-1)/(q-1)$ elements of $\mathbb{F}_{q^t}^*$ which are $(q-1)$-th powers of elements in W; more precisely, they are the solutions of*

$$x^{\frac{q^t-1}{q-1}} = -1, \quad x \in \mathbb{F}_{q^n}.$$

(*ii*) *If t is even, then there are precisely $(q^t-1)/(q+1)$ elements of $\mathbb{F}_{q^t}^*$ which are $(q+1)$-th powers of elements in W; more precisely, they are the solutions of*

$$x^{\frac{q^t-1}{q+1}} = -1, \quad x \in \mathbb{F}_{q^n}.$$

(*iii*) *If t is odd, then there are precisely $(q^t - 1)/2$ elements of $\mathbb{F}_{q^t}^*$ which are $(q+1)$-th powers of elements in W; more precisely, they are the solutions of*

$$x^{\frac{q^t-1}{2}} = (-1)^{\frac{q+1}{2}}, \quad x \in \mathbb{F}_{q^n}.$$

Proof. Let $W^* = W \setminus \{0\}$. For any positive integer D define the set S_D of all D-powers of elements of W^*. Let $\delta = \gcd(D, q^t - 1)$. The D-powers of elements of $\mathbb{F}_{q^t}^*$ are precisely the solutions of the equation

$$x^{\frac{q^t-1}{\delta}} = 1, \quad x \in \mathbb{F}_{q^n}.$$

Let $w_0 \in W^*$. It holds $(w_0^D)^{\frac{q^t-1}{\delta}} = (w_0^{q^t-1})^{D/\delta} = (-1)^{D/\delta}$. We have

$$S_D = \{w_0^D y^D : y \in \mathbb{F}_{q^t}^*\} = \{w_0^D x : x^{\frac{q^t-1}{\delta}} = 1, \, x \in \mathbb{F}_{q^n}\}.$$

Therefore, S_D has equation

$$x^{\frac{q^t-1}{\delta}} = (-1)^{D/\delta}. \tag{11}$$

Taking into account that

$$\gcd(q+1, q^t - 1) = \begin{cases} q+1 & \text{for } t \text{ even}, \\ 2 & \text{for } t \text{ odd}, \end{cases}$$

the statements (*i*), (*ii*), and (*iii*) follow from (11). □

Corollary 2.6. *There is at least one scattered polynomial of type $\varphi_{m,\sigma}$ for any $t \geq 4$ even and $q \geq 3$, or $t \geq 3$ and $q > 3$.*

Proof. The sum of the sizes of S_{q-1} and S_{q+1} is less than $q^t - 1$, hence there exist in $\mathbb{F}_{q^t}^*$ elements which are neither $(q-1)$- nor $(q+1)$-powers of elements of W. Therefore, Theorem 2.3 can be applied for at least one value of m. □

Remark 2.7. By Theorem 2.3 and Proposition 2.5, if t is even, or t is odd and $q \equiv 1 \pmod 4$, then $\varphi_{1,q}$ is scattered. On the other hand, by Proposition 2.4, if t is odd and $q \equiv 3 \pmod 4$, then $\varphi_{1,q}$ is not scattered. This is consistent with [10, Theorem 2.4] for $k = 1$. It follows that the family we are studying contains examples of R-q^t-partially scattered polynomials that are not scattered.

3. Matrices stabilizing the graph of $\varphi_{m,\sigma}$

Here we investigate the matrices in $\mathbb{F}_{q^n}^{2\times 2}$ that stabilize the graph $U_{m,\sigma}$ of $\varphi_{m,\sigma}$. More precisely, we will compute the set $\mathbb{S}_{m,\sigma}$ of matrices A such that $AU_{m,\sigma} \subseteq U_{m,\sigma}$. Such $\mathbb{S}_{m,\sigma}$ has been studied in [17], where in particular it has been proved that it is isomorphic to the right idealizer of $\mathcal{C}_{\varphi_{m,\sigma}}$. As a consequence, $\mathbb{S}_{m,\sigma}$ is invariant up to equivalence of polynomials.

For use in the Theorem 3.2 we prove the following

Proposition 3.1. *Let t be even. The set S of all $x \in \mathbb{F}_{q^t}^*$ which are $(\sigma+1)$-powers of elements in W coincides with $\left\{x\colon x \in \mathbb{F}_{q^t},\, x^{\frac{\sigma^t-1}{\sigma+1}} = -1\right\}$.*

Proof. If $x_0 = \xi^{\sigma+1}$ and $y = \eta^{\sigma+1}$ for $\xi, \eta \in W \setminus \{0\}$, then $x_0 y^{-1} = (\xi\eta^{-1})^{\sigma+1}$ is a $(\sigma+1)$-power of an element of $\mathbb{F}_{q^t}^*$; that is, $y = \ell^{\sigma+1}x_0$ for some $\ell \in \mathbb{F}_{q^t}^*$. Conversely, $h^{\sigma+1}x_0 \in S$ for any $h \in \mathbb{F}_{q^t}^*$. So,

$$S = \{h^{\sigma+1}x_0 \colon h \in \mathbb{F}_{q^t}^*\}.$$

The assertion follows by combining (i) $x_0^{\frac{\sigma^t-1}{\sigma+1}} = \xi^{\sigma^t-1} = -1$, and (ii) since t is even and $\sigma+1$ divides σ^t-1, the set of all $(\sigma+1)$-powers of elements of $\mathbb{F}_{q^t}^*$ has equation $x^{\frac{\sigma^t-1}{\sigma+1}} = 1$. □

Theorem 3.2. *Suppose that $t > 4$. Then the set $\mathbb{S}_{m,\sigma}$ of matrices $A \in \mathbb{F}_{q^n}^{2\times 2}$ such that $AU_{m,\sigma} \subseteq U_{m,\sigma}$ is equal to*

$$\left\{\begin{pmatrix} a & b \\ 4mb^\sigma & a^\sigma \end{pmatrix} \;:\; a \in \mathbb{F}_{q^{\gcd(t,2)}},\; b \in \mathbb{F}_{q^n},\; b = -b^{\sigma^t} = m^{\sigma-1}b^{\sigma^2}\right\}. \tag{12}$$

For t even, $\mathbb{S}_{m,\sigma}$ contains non-diagonal matrices if and only if m is a $(\sigma+1)$-power of an element of W; in this case, b takes q^2 distinct values.

For t odd, b takes always q distinct values.

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{F}_{q^n}^{2\times 2}$, and

$$A\begin{pmatrix} x \\ \varphi_{m,\sigma}(x) \end{pmatrix} = \begin{pmatrix} y \\ \varphi_{m,\sigma}(y) \end{pmatrix};$$

that is, $cx + d\varphi_{m,\sigma}(x) = \varphi_{m,\sigma}(ax + b\varphi_{m,\sigma}(x))$ for all $x \in \mathbb{F}_{q^n}$. This leads, after reducing modulo $X^{\sigma^{2t}} - X$, to the following polynomial identity

$$cX + d(X^{\sigma^{t-1}} + X^{\sigma^{2t-1}} + m(X^\sigma - X^{\sigma^{t+1}})) =$$

$$
\begin{aligned}
& a^{\sigma^{t-1}} X^{\sigma^{t-1}} + b^{\sigma^{t-1}} (X^{\sigma^{2t-2}} + X^{\sigma^{t-2}} + m^{\sigma^{t-1}} (X^{\sigma^t} - X)) \\
& + a^{\sigma^{2t-1}} X^{\sigma^{2t-1}} + b^{\sigma^{2t-1}} (X^{\sigma^{t-2}} + X^{\sigma^{2t-2}} + m^{\sigma^{2t-1}} (X - X^{\sigma^t})) \\
& + m a^{\sigma} X^{\sigma} + m b^{\sigma} (X^{\sigma^t} + X + m^{\sigma} (X^{\sigma^2} - X^{\sigma^{t+2}})) \\
& - m a^{\sigma^{t+1}} X^{\sigma^{t+1}} - m b^{\sigma^{t+1}} (X + X^{\sigma^t} + m^{\sigma^{t+1}} (X^{\sigma^{t+2}} - X^{\sigma^2})). \qquad (13)
\end{aligned}
$$

Taking into account the coefficients of monomials of the same degree one obtains the ten equations

$$c = -m^{\sigma^{t-1}} b^{\sigma^{t-1}} + m^{\sigma^{2t-1}} b^{\sigma^{2t-1}} + m b^{\sigma} - m b^{\sigma^{t+1}} \qquad \text{(e:0)}$$

$$md = m a^{\sigma} \qquad \text{(e:1)}$$

$$0 = m^{\sigma+1} b^{\sigma} + m^{1+\sigma^{t+1}} b^{\sigma^{t+1}} \qquad \text{(e:2)}$$

$$0 = b^{\sigma^{t-1}} + b^{\sigma^{2t-1}} \qquad \text{(e:t-2)}$$

$$d = a^{\sigma^{t-1}} \qquad \text{(e:t-1)}$$

$$0 = m^{\sigma^{t-1}} b^{\sigma^{t-1}} - m^{\sigma^{2t-1}} b^{\sigma^{2t-1}} + m b^{\sigma} - m b^{\sigma^{t+1}} \qquad \text{(e:t)}$$

$$-md = -m a^{\sigma^{t+1}} \qquad \text{(e:t+1)}$$

$$0 = -m^{\sigma+1} b^{\sigma} - m^{1+\sigma^{t+1}} b^{\sigma^{t+1}} \qquad \text{(e:t+2)}$$

$$0 = b^{\sigma^{t-1}} + b^{\sigma^{2t-1}} \qquad \text{(e:2t-2)}$$

$$d = a^{\sigma^{2t-1}} \qquad \text{(e:2t-1)}$$

The equations (e:1), (e:t-1), (e:t+1), (e:2t-1) are equivalent to $a \in \mathbb{F}_{q^{\gcd(t,2)}}$, $d = a^q$. The equations (e:2), (e:t-2), (e:t+2), and (e:2t-2) are equivalent to $b \in W$. Then (e:t) is equivalent to $m^{\sigma^{t-1}} b^{\sigma^{t-1}} + m b^{\sigma} = 0$, or

$$b^{\sigma^2} = m^{1-\sigma} b. \qquad (14)$$

Equations (e:t) and (e:0) imply $c = 2(mb^{\sigma} - mb^{\sigma^{t+1}}) = 4mb^{\sigma}$, leading to (12).

The equation (14) in the unknown b determines the kernel of an $\mathbb{F}_{q^2}$-linear map, and has one or q^2 solutions. Since W is an $\mathbb{F}_{q^t}$-linear subspace, the number of allowable values b in (12) is either one or $q^{\gcd(t,2)}$.

Assume t **even**. It holds

$$-b = b^{\sigma^t} = m^{-\sigma^{t-1} + \sigma^{t-2} - \cdots - \sigma + 1} b.$$

Assume that (14) has at least one nonzero solution (and hence q^2 solutions). Then

$$m^{(\sigma-1)(1+\sigma^2+\cdots+\sigma^{t-2})} = -1,$$

equivalent to $m^{\frac{\sigma^t-1}{\sigma+1}}=-1$, that is, by Proposition 3.1, m is a $(\sigma+1)$-power of an element of W. Conversely if $m=\beta^{-(\sigma+1)}$ for $\beta\in W$, then (14) has the nonzero solution $b=\beta$, hence q^2 solutions in W.

Assume t **odd**. Define $R=-\frac{\sigma^{t+1}-1}{\sigma^2-1}$ which is an integer. Furthermore, a $z\in\mathbb{F}_{q^n}^*$ exists satisfying $z^\sigma+z=0$, and $z\in W$. Then by a direct check the solutions in W to (14) are $b=\lambda z m^R$ for $\lambda\in\mathbb{F}_q$. □

Remark 3.3. If t is even (including now the case $t=4$) and $\varphi_{m,\sigma}$ is scattered, then $\varphi_{m,\sigma}$ is in standard form with respect to the subfield $\mathbb{F}_{q^2}$; that is, $L=2$ is the greatest integer such that $\varphi_{m,\sigma}=F(X^{q^s})$ where F is a q^L-polynomial, and $\gcd(s,L)=1$. This implies that the set of matrices stabilizing $U_{m,\sigma}$ is isomorphic to $\mathbb{F}_{q^2}$ [11,17].

In particular: (i) if $m=1$ and t is even, the matrices are all diagonal; (ii) if $m=1$ and t is odd, then the conditions on b are equivalent to $b^q+b=0$.

Remark 3.4. For the case $t\geq 3$ is odd, $m=1$ and $q\equiv 3 \pmod 4$, it can be shown that in this case the kernel and the image of any matrix of rank one in $\mathbb{S}_{1,\sigma}$ are points of $\mathrm{PG}(1,q^n)$ of weight $n/2$, i.e., such that their intersection with the graph is an $\mathbb{F}_q$-subspace of dimension $n/2$. Polynomials of this type have been studied in [17].

4. Nonequivalence with previously known scattered polynomials

Our main goal is to show that there are new scattered polynomials in the family we introduce. For this purpose it will be sufficient to consider the case where $\sigma=q$, $n=2t$, $t\geq 3$. We compare our construction with the known examples of scattered polynomials.

The first nonequivalence is a simple consequence of the fact that the right idealizer of the MRD code associated with a polynomial of pseudoregulus type in $\mathcal{L}_{n,q}$ is isomorphic to $\mathbb{F}_{q^n}$, combined with Theorem 3.2. Analogously we proceed with the second nonequivalence if t is odd, since the right idealizer of the MRD code associated with a polynomial of Lunardon-Polverino type in $\mathcal{L}_{n,q}$ is isomorphic to $\mathbb{F}_{q^2}$.

Proposition 4.1. *Let $f=X^{q^s}\in\mathcal{L}_{n,q}$ be a scattered polynomial of pseudoregulus type. Then $\varphi_{m,q}$ and f are not equivalent.*

Proposition 4.2. *Let $g=X^{q^{2t-s}}+\delta X^{q^s}$ be a Lunardon-Polverino scattered polynomial, $t>4$. Then $\varphi_{m,q}$ and g are not equivalent.*

Proof. The subspaces $U_{\varphi_{m,q}}$ and U_g are in the same orbit under the action of $\Gamma\mathrm{L}(2,q^n)$ if and only if an integer k and a matrix

$$M=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in \mathrm{GL}(2,q^{2t})$$

exist such that for any $x\in\mathbb{F}_{q^{2t}}$ there is $y\in\mathbb{F}_{q^{2t}}$ satisfying

$$M\begin{pmatrix} x^{p^k} \\ \varphi_{m,q}(x)^{p^k} \end{pmatrix} = \begin{pmatrix} y \\ g(y) \end{pmatrix}.$$

Let $e = m^{p^k}$ and $z = x^{p^k}$. The condition above is equivalent to

$$\begin{aligned} az + b(z^{q^{t-1}} + z^{q^{2t-1}}) + be(z^q - z^{q^{t+1}}) &= y, \\ cz + d(z^{q^{t-1}} + z^{q^{2t-1}}) + de(z^q - z^{q^{t+1}}) &= y^{q^{2t-s}} + \delta y^{q^s}, \end{aligned}$$

from which after reducing modulo $Z^{\sigma^{2t}} - Z$ we derive the polynomial identity

$$\begin{aligned} &a^{q^{2t-s}} Z^{q^{2t-s}} + b^{q^{2t-s}}(Z^{q^{t-s-1}} + Z^{q^{2t-s-1}}) + b^{q^{2t-s}} e^{q^{2t-s}}(Z^{q^{2t-s+1}} - Z^{q^{t-s+1}}) + \\ &+\delta a^{q^s} Z^{q^s} + \delta b^{q^s}(Z^{q^{t+s-1}} + Z^{q^{s-1}}) + \delta b^{q^s} e^{q^s}(Z^{q^{s+1}} - Z^{q^{t+s+1}}) = \\ &= cZ + d(Z^{q^{t-1}} + Z^{q^{2t-1}}) + de(Z^q - Z^{q^{t+1}}). \end{aligned}$$

Let t be even. We consider the cases $s \in \{1, t-1, t+1, 2t-1\}$.

Let $s = 1$. When $t > 4$, we have the following system

$$\begin{cases} b^{q^{2t-1}} e^{q^{2t-1}} + \delta b^q = c \\ \delta a^q = de \\ \delta b^q e^q = 0 \\ b^{q^{2t-1}} = 0 \\ 0 = d \\ -b^{q^{2t-1}} e^{q^{2t-1}} + \delta b^q = 0 \\ 0 = -de \\ -\delta b^q e^q = 0 \\ b^{q^{2t-1}} = 0 \\ a^{q^{2t-1}} = d. \end{cases} \tag{15}$$

Which implies $a = b = c = d = 0$. For $s \in \{t-1, t+1, 2t-1\}$ we get analogous conditions that yield to $a = b = c = d = 0$.

Finally, for $s \notin \{1, t-1, t+1, 2t-1\}$ the analogous system as in (15) leads to the same conclusion. In fact, the exponents of the indeterminate Z depending on s equal some of the exponents of Z in the right side of the polynomial identity $(1, q, q^{t+1}, q^{t-1}, q^{2t-1})$ if and only if $s \in \{1, t+1, t-1, 2t-1, t+2, t-2\}$. Since t is even we exclude $t-2$ and $t+2$, and then, apart from the already considered cases, we get the condition $c = d = 0$. The case t odd arises from similar calculations while $s \in \{1, t-2, t+2\}$, while in this case we can exclude $t = \pm 1$ and $t = 2t - 1$. □

The fact that $\varphi_{1,\sigma}$ belongs to the family (*iii-a*) motivates our interest in the next result.

Proposition 4.3. *Let $t \in \mathbb{N}$, $t > 4$. Then $\varphi_{m,q}$ and $\varphi_{1,\sigma}$ are equivalent only if $\mathrm{N}_{q^t/q}(m) = 1$.*

Proof. Assume that $\varphi_{m,q}$ and $\varphi_{1,\sigma}$ are equivalent. Then there exist an integer k and a matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, q^n)$$

such that for any $x \in \mathbb{F}_{q^{2t}}$ there is $y \in \mathbb{F}_{q^{2t}}$ satisfying

$$M \begin{pmatrix} x^{p^k} \\ \varphi_{m,q}(x)^{p^k} \end{pmatrix} = \begin{pmatrix} y \\ \varphi_{1,\sigma}(y) \end{pmatrix}.$$

Let $e = m^{p^k}$ and $z = x^{p^k}$. The condition above is equivalent to

$$az + b(z^{q^{t-1}} + z^{q^{2t-1}}) + be(z^q - z^{q^{t+1}}) = y,$$
$$cz + d(z^{q^{t-1}} + z^{q^{2t-1}}) + de(z^q - z^{q^{t+1}}) = y^\sigma - y^{\sigma^{t+1}} + y^{\sigma^{t-1}} + y^{\sigma^{2t-1}},$$

and, taking into account $e^{\sigma^t} = e$ and that J is odd, we get the following identity in $\mathcal{L}_{n,q}$:

$$\begin{aligned} cZ + d(Z^{q^{t-1}} + Z^{q^{2t-1}}) + de(Z^q - Z^{q^{t+1}}) = \\ = a^\sigma Z^{q^J} + b^\sigma(Z^{q^{t+J-1}} + Z^{q^{J-1}}) + b^\sigma e^\sigma(Z^{q^{J+1}} - Z^{q^{t+J+1}}) \\ -a^{\sigma^{t+1}} Z^{q^{t+J}} - b^{\sigma^{t+1}}(Z^{q^{J-1}} + Z^{q^{t+J-1}}) - b^{\sigma^{t+1}} e^\sigma(Z^{q^{t+J+1}} - Z^{q^{J+1}}) \\ +a^{\sigma^{t-1}} Z^{q^{t-J}} + b^{\sigma^{t-1}}(Z^{q^{2t-J-1}} + Z^{q^{t-J-1}}) + b^{\sigma^{t-1}} e^{\sigma^{t-1}}(Z^{q^{t-J+1}} - Z^{q^{2t-J+1}}) \\ +a^{\sigma^{2t-1}} Z^{q^{2t-J}} + b^{\sigma^{2t-1}}(Z^{q^{t-J-1}} + Z^{q^{2t-J-1}}) + b^{\sigma^{2t-1}} e^{\sigma^{2t-1}}(Z^{q^{2t-J+1}} - Z^{q^{t-J+1}}). \end{aligned} \quad (16)$$

By comparing the monomials having the same degree, if $J \notin \{\pm 1, t \pm 1\}$, one obtains without any assumption on $\mathrm{N}_{q^t/q}(m)$ that M has a zero row.

If $J = 1$, by (16),

$$\begin{cases} c = b^q - b^{q^{t+1}} - b^{q^{t-1}} e^{q^{t-1}} + b^{q^{2t-1}} e^{q^{t-1}} \\ de = a^q \\ 0 = b^q + b^{q^{t+1}} \\ 0 = b^{q^{t-1}} + b^{q^{2t-1}} \\ d = a^{q^{t-1}} \\ 0 = b^q - b^{q^{t+1}} + b^{q^{t-1}} e^{q^{t-1}} - b^{q^{2t-1}} e^{q^{t-1}} \\ de = a^{q^{t+1}} \\ 0 = -b^q e^q - b^{q^{t+1}} e^q \\ 0 = b^{q^{t-1}} + b^{q^{2t-1}} \\ d = a^{q^{2t-1}}. \end{cases} \quad (17)$$

If $a \neq 0$, then $d \neq 0$. By comparing the seventh and the second equation, one obtains $a \in \mathbb{F}_{q^t}$. From the second and the fifth equation, $a^{q-q^{t-1}} = e$ that implies $\mathrm{N}_{q^t/q}(m) = 1$. If $a = 0$, then $cb \neq 0$, $b^{q^t} + b = 0$ by the third equation and $b^{q^2} = eb$ by the sixth. This implies $\mathrm{N}_{q^t/q}(m) = 1$.

The cases $J = 2t - 1$ or $J = t \pm 1$ for t even can be dealt with in a similar way leading in each case to $\mathrm{N}_{q^t/q}(m) = 1$. $\square$

We now investigate the equivalence between polynomials of type $\varphi_{m,q}$ and their adjoints. Define $\phi_\mu = X^q + X^{q^{t+1}} + \mu(X^{q^{2t-1}} - X^{q^{t-1}})$, $\mu \in \mathbb{F}_{q^t}$; it holds

$$\varphi_{m,q}^\top = \phi_{m^{q^{t-1}}} \tag{18}$$

for any $m \in \mathbb{F}_{q^t}$.

Proposition 4.4. *Let $t > 4$. For any $m, \mu \in \mathbb{F}_{q^t}$ such that $\varphi_{m,q}$ is scattered, $\varphi_{m,q}$ and ϕ_μ are nonequivalent.*

Proof. Starting from

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ x^{q^{t-1}} + x^{q^{2t-1}} + m(x^q - x^{q^{t+1}}) \end{pmatrix} = \begin{pmatrix} y \\ y^q + y^{q^{t+1}} + \mu(y^{q^{2t-1}} - y^{q^{t-1}}) \end{pmatrix}$$

one obtains the polynomial identity modulo $x^{\sigma^{2t}} - x$

$$\begin{aligned} cX + d[X^{q^{t-1}} + X^{q^{2t-1}} + m(X^q - X^{q^{t+1}})] &= a^q X^q + b^q[X^{q^t} + X + m^q(X^{q^2} - X^{q^{t+2}})] \\ &+ a^{q^{t+1}} X^{q^{t+1}} + b^{q^{t+1}}[X + X^{q^t} + m^{q^{t+1}}(X^{q^{t+2}} - X^{q^2})] \\ &+ \mu a^{q^{2t-1}} X^{q^{2t-1}} + \mu b^{q^{2t-1}}[X^{q^{t-2}} + X^{q^{2t-2}} + m^{2^{2t-1}}(X - X^{q^t})] \\ &- \mu a^{q^{t-1}} X^{q^{t-1}} - \mu b^{q^{t-1}}[X^{q^{2t-2}} + X^{q^{t-2}} + m^{q^{t-1}}(X^{q^t} - X)]. \end{aligned}$$

This gives ten equations, four equations equivalent to $b \in \mathbb{F}_{q^t}$ and four equations equivalent to $d = m^{-1}a^q = -\mu a^{q^{t-1}} = -m^{-1}a^{q^{t+1}}$, that is

$$a \in W, \ d = m^{-1}a^q, \ \mu = -m^{-1}a^{q-q^{t-1}}.$$

By comparing the coefficients of X^{q^t} one obtains $\mu = m^{-q^{t-1}} b^{q-q^{t-1}}$, and finally

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

As a consequence, $m^{(q^t-1)/(q+1)} = (a/b)^{q^t-1} = -1$ for t even end $m^{(q^t-1)/2} = (a/b)^{(q^t-1)(q+1)/2} = (-1)^{(q+1)/2}$ for t odd and this implies by Propositions 2.4 and 2.5 that $\varphi_{m,q}$ is not scattered. $\square$

In [2] the notion of a $\Gamma\mathrm{L}$-*class* of a linear set L has been introduced, which is the number of nonequivalent polynomials f such that $L_f = L$. As a corollary of Proposition 4.4 it results:

Theorem 4.5. *For $t > 4$ the $\Gamma\mathrm{L}$-class of any scattered linear set of type $L_{\varphi_{m,q}}$ is at least two.*

It is possible to prove the nonequivalence of the polynomials of type $\varphi_{m,q}$ with the polynomials in the class (*iii-b*) with a case-by-case analysis. However, the following result makes it possible to shorten the proof.

Proposition 4.6. *[7] Let $f, g \in \mathcal{L}_{n,q}$ be equivalent. Then $f^\top$ and $g^\top$ are equivalent.*

The main result of this paper is a summary of the propositions of this section.

Theorem 4.7. *Let q be odd and $t > 4$. If t is even and $q > 3$ or t is odd and $q > 5$, then there exists $m \in \mathbb{F}_{q^t}$ such that*

$$\varphi_{m,q} = X^{q^{t-1}} + X^{q^{2t-1}} + m(X^q - X^{q^{t+1}})$$

is a scattered q-polynomial that is not equivalent to any previously known scattered q-polynomial in $\mathbb{F}_{q^{2t}}[X]$.

Proof. Take into account a scattered $\varphi_{m,q}$. This $\varphi_{m,q}$ does not belong to the families (i) and (ii) by Propositions 4.1 and 4.2. Since any element of the family (*iii-b*) is equivalent to its adjoint, by Propositions 4.4 and 4.6 such family does not contain $\varphi_{m,q}$. The family (*iii-a*) contains elements of type $\varphi_{1,\sigma}$ and if $\mathrm{N}_{q^t/q^{\gcd(2,t)}}(m) \neq 1$, $\varphi_{m,q}$ is nonequivalent to these by Proposition 4.3. So it remains to prove that at least one scattered $\varphi_{m,q}$ exists satisfying that condition. Taking into account Theorem 2.3, it is enough to show that the sum of the cardinalities of the following three sets is less than $q^t - 1$.

1. S_{q-1}, that is, the set of elements in $\mathbb{F}_{q^t}^*$ which are $(q-1)$-powers of elements of W;
2. S_{q+1}, that is, the set of elements in $\mathbb{F}_{q^t}^*$ which are $(q+1)$-powers of elements of W;
3. T, the set of elements $m \in \mathbb{F}_{q^t}$ such that $\mathrm{N}_{q^t/q}(m) = 1$.

The equation $\mathrm{N}_{q^t/q}(x) = 1$ has $(q^t - 1)/(q - 1)$ solutions.

Assume that t is even. Combining with Proposition 2.5,

$$|S_{q-1} \cup S_{q+1} \cup T| \leq \frac{q^t - 1}{q - 1} + \frac{q^t - 1}{q + 1} + \frac{q^t - 1}{q - 1} = \frac{(q^t - 1)(3q + 1)}{q^2 - 1}, \tag{19}$$

that for $q > 3$ is less than $q^t - 1$.

In the case that t is odd one obtains similarly

$$|S_{q-1} \cup S_{q+1} \cup T| \leq \frac{q^t-1}{q-1} + \frac{q^t-1}{2} + \frac{q^t-1}{q-1} = \frac{q^t-1}{2(q-1)}(q+3).$$

For $q > 5$ this is less than $q^t - 1$. $\square$

Declaration of competing interest

None declared.

Data availability

No data was used for the research described in the article.

Acknowledgements

The authors are very thankful to Giovanni Longobardi for pointing out Proposition 4.6 and to the anonymous referees for their comments. The authors were partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The research of the third author was partially supported by the project COMBINE of the University of Campania Luigi Vanvitelli.

The research of the first and the third author was partially supported by the INdAM - GNSAGA Project *Tensors over finite fields and their applications*, number E53C23001670001.

References

[1] D. Bartoli, C. Zanella, F. Zullo, A new family of maximum scattered linear sets in $\mathrm{PG}(1, q^6)$, Ars Math. Contemp. 19 (1) (2020) 125–145.
[2] B. Csajbók, G. Marino, O. Polverino, Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$, J. Comb. Theory, Ser. A 157 (2018) 402–426.
[3] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, J. Comb. Theory, Ser. A 25 (1978) 226–241.
[4] E. Gabidulin, Theory of codes with maximum rank distance, Probl. Inf. Transm. 21 (3) (1985) 3–16.
[5] R. Gow, R. Quinlan, Galois extensions and subspaces of alterning bilinear forms with special rank properties, Linear Algebra Appl. 430 (2009) 2212–2224.
[6] M. Lavrauw, Scattered spaces in Galois geometry, in: Contemporary Developments in Finite Fields and Applications, 2016, pp. 195–216.
[7] G. Longobardi, Private communication, 2024.
[8] G. Longobardi, G. Marino, R. Trombetti, Y. Zhou, A large family of maximum scattered linear sets of $\mathrm{PG}(1, q^n)$ and their associated MRD codes, Combinatorica 43 (2023) 681–716.
[9] G. Longobardi, C. Zanella, Partially scattered linearized polynomials and rank metric codes, Finite Fields Appl. 76 (2021) 101914.
[10] G. Longobardi, C. Zanella, Linear sets and MRD-codes arising from a class of scattered linearized polynomials, J. Algebraic Comb. 53 (2021) 639–661.
[11] G. Longobardi, C. Zanella, A standard form for scattered linearized polynomials and properties of the related translation planes, J. Algebraic Comb. 59 (2024) 917–937.

[12] G. Lunardon, O. Polverino, Blocking sets and derivable partial spreads, J. Algebraic Comb. 14 (2001) 44–56.
[13] A. Neri, P. Santonastaso, F. Zullo, Extending two families of maximum rank distance codes, Finite Fields Appl. 81 (2022) 102045.
[14] O. Polverino, Linear sets in finite projective spaces, Discrete Math. 310 (22) (2010) 3096–3107.
[15] O. Polverino, F. Zullo, Connections between scattered linear sets and MRD-codes, Bull. Inst. Comb. Appl. 89 (2020) 46–74.
[16] J. Sheekey, A new family of linear maximum rank distance codes, Adv. Math. Commun. 10 (3) (2016) 475–488.
[17] V. Smaldore, C. Zanella, F. Zullo, On the stabilizer of the graph of linear functions over finite fields, https://arxiv.org/abs/2401.06085v1.