J. Geom. (2019) 110:50

0047-2468/19/030001-9
*published online* September 23, 2019
https://doi.org/10.1007/s00022-019-0505-z

**Journal of Geometry**

# A condition for scattered linearized polynomials involving Dickson matrices

Corrado Zanella

**Abstract.** A linearized polynomial over $\mathbb{F}_{q^n}$ is called scattered when for any $t, x \in \mathbb{F}_{q^n}$, the condition $xf(t) - tf(x) = 0$ holds if and only if $x$ and $t$ are $\mathbb{F}_q$-linearly dependent. General conditions for linearized polynomials over $\mathbb{F}_{q^n}$ to be scattered can be deduced from the recent results in Csajbók (Scalar $q$-subresultants and Dickson matrices, 2018), Csajbók et al. (Finite Fields Appl 56:109–130, 2019), McGuire and Sheekey (Finite Fields Appl 57:68–91, 2019), Polverino and Zullo (On the number of roots of some linearized polynomials, 2019). Some of them are based on the Dickson matrix associated with a linearized polynomial. Here a new condition involving Dickson matrices is stated. This condition is then applied to the Lunardon–Polverino binomial $x^{q^s} + \delta x^{q^{n-s}}$, allowing to prove that for any $n$ and $s$, if $\mathrm{N}_{q^n/q}(\delta) = 1$, then the binomial is not scattered. Also, a necessary and sufficient condition for $x^{q^s} + bx^{q^{2s}}$ to be scattered is shown which is stated in terms of a special plane algebraic curve.

**Mathematics Subject Classification.** 51E20, 05B25, 51E22.

**Keywords.** Linear set, Linearized polynomial, $q$-Polynomial, Finite projective line, Scattered linear set, Dickson matrix.

## 1. Introduction

A point $P$ of the projective space $\mathrm{PG}(d-1, q^n)$ is a one-dimensional subspace of the vector space $\mathbb{F}_{q^n}^d$; that is, $P = \langle v \rangle_{\mathbb{F}_{q^n}} = \{cv \colon c \in \mathbb{F}_{q^n}\}$ for some nonzero $v \in \mathbb{F}_{q^n}^d$.

Let $U$ be an $r$-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^d$. Then

$$L_U := \{\langle v \rangle_{\mathbb{F}_{q^n}} : v \in U, v \neq 0\}$$

is an $\mathbb{F}_q$-*linear set* (or just *linear set*) of *rank* $r$ in $\mathrm{PG}(d-1, q^n)$. Let $u, v \in U$. If $u = cv$, $c \in \mathbb{F}_q$, then clearly $\langle u \rangle_{\mathbb{F}_{q^n}} = \langle v \rangle_{\mathbb{F}_{q^n}}$. If this is the only case in which two vectors of $U$ determine the same point of $\mathrm{PG}(d-1,q)$, that is, $\langle v\rangle_{\mathbb{F}_{q^n}} = \langle u\rangle_{\mathbb{F}_{q^n}}$ if and only if $\langle v\rangle_{\mathbb{F}_q} = \langle u\rangle_{\mathbb{F}_q}$, then $L_U$ is called a *scattered* linear set. Equivalently, $L_U$ is scattered if and only if it has maximum size $(q^r-1)/(q-1)$ with respect to $r$. The linear sets are related to combinatorial objects, such as blocking sets, two-intersection sets, finite semifields, rank-distance codes, and many others. The interested reader is referred to the survey by Polverino [18] and to [20], where J. Sheekey builds a bridge with the rank-distance codes.

Assume that in particular $U$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^2$, $\dim_{\mathbb{F}_q} U = n$. In this case $L_U := \{\langle v\rangle_{\mathbb{F}_{q^n}} : v \in U, v \neq 0\} \subseteq \mathrm{PG}(1,q^n)$, is called a *maximum* linear set of $\mathrm{PG}(1,q^n)$, since by the dimension formula any linear set of rank greater than $n$ equals $\mathrm{PG}(1,q^n)$. Up to projectivities of $\mathrm{PG}(1,q^n)$ it may be assumed that $\langle(0,1)\rangle_{\mathbb{F}_{q^n}} \notin L_U$. Hence

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

where $f(x)$ is a suitable $\mathbb{F}_q$-linear map, that is a linearized polynomial:

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}, \quad a_i \in \mathbb{F}_{q^n}, \quad i = 0,1,\ldots,n-1. \tag{1}$$

If $L_f$ is scattered, then $f(x)$ is called a *scattered* linearized polynomial, or *scattered $q$-polynomial* with respect to $n$. A property characterizing the scattered $q$-polynomials is that for any $x,y \in \mathbb{F}_{q^n}^*$, $f(x)/x = f(y)/y$ if and only if $\langle x\rangle_{\mathbb{F}_q} = \langle y\rangle_{\mathbb{F}_q}$.

A first example of scattered $q$-polynomial is $f(x) = x^q$ [3], with respect to any $n$. Indeed, for any $x,y \in \mathbb{F}_{q^n}^*$, $f(x)/x = f(y)/y$, is equivalent to $x^{q-1} = y^{q-1}$, hence to $x/y \in \mathbb{F}_q^*$. A derived example is $f(x) = x^{q^s}$, $\gcd(n,s) = 1$. Indeed $(x/y)^{q^s-1} = 1$ implies $x/y \in \mathbb{F}_{q^s} \cap \mathbb{F}_{q^n}^* = \mathbb{F}_q^*$. In both cases above, $L_f = \{\langle(x,f(x))\rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\} = \{\langle(1,z)\rangle_{\mathbb{F}_{q^n}} : z \in \mathbb{F}_{q^n}, \mathrm{N}_{q^n/q}(z) = 1\}$, where $\mathrm{N}_{q^n/q}(z) = z^{(q^n-1)/(q-1)}$ denotes the norm over $\mathbb{F}_q$ of $z \in \mathbb{F}_{q^n}$. The related linear set is called a *linear set of pseudoregulus type*.

The next example has been given by Lunardon and Polverino [12] and generalized in [11,20]:

$$f(x) = x^{q^s} + \delta x^{q^{n-s}}, \quad n \geq 4, \quad \gcd(n,s) = 1, \quad \mathrm{N}_{q^n/q}(\delta) \neq 1.$$

In particular cases, the condition $\mathrm{N}_{q^n/q}(\delta) \neq 1$ has been proved to be necessary for $f(x)$ to be scattered [2,10,11,22]. In Sect. 3 it will proved that actually it is necessary for any $n$ and $s$. Further examples of scattered $q$-polynomials are given in [5,6,14,22]. All of them are with respect to $n = 6$ or $n = 8$. Bartoli et al. [1] proved that if $\hat{f}(x)$ is the adjoint of $f(x)$ with respect to the bilinear form $\langle x,y\rangle = \mathrm{Tr}_{q^n/q}(xy)$ in $\mathbb{F}_{q^n}^2$, where $\mathrm{Tr}_{q^n/q}(z) = \sum_{i=0}^{n-1} z^{q^i}$ denotes the trace over $\mathbb{F}_q$ of $z \in \mathbb{F}_{q^n}$, then $L_f = L_{\hat{f}}$. This implies that if the polynomial $f(x)$ in (1) is scattered, then also $\hat{f}(x) = \sum_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}$ is. Up to the knowledge of the author of this paper, no more examples of scattered $q$-polynomials are known. So, it would seem that scattered $q$-polynomials are rare. Bartoli and Zhou [2] formalized such an idea of scarcity by proving that the pseudoregulus and Lunardon–Polverino polynomials are, roughly speaking, the only $q$-polynomials of a certain type which are scattered for infinitely many $n$.

Recently, a great deal of effort has been put in finding conditions for $q$-polynomials to be scattered [4,7,15,19]. Some of them are based on the *Dickson matrix* associated with the $q$-polynomial in (1), that is, the $n \times n$ matrix

$$M_{q,f} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & a_1^q & \cdots & a_{n-2}^q \\ a_{n-2}^{q^2} & a_{n-1}^{q^2} & a_0^{q^2} & \cdots & a_{n-3}^{q^2} \\ \vdots & & & & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & a_3^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}.$$

It is well-known that the rank of $M_{q,f}$ equals the rank of $f(x)$, see for example [21, Proposition 4.4]. This rank can be computed by applying the following result by B. Csajbók:

**Theorem 1.1.** ([4, Theorem 3.4]) *Let $M_{q,f}$ be the Dickson matrix associated with the q-polynomial in (1). Denote by $M_{q,f}^{(r)}$ the $r \times r$ submatrix of $M_{q,f}$ obtained by considering the last $r$ columns and the first $r$ rows of $M_{q,f}$. Then the rank of $f(x)$ is $t$ if and only if* $\det(M_{q,f}^{(n)}) = \det(M_{q,f}^{(n-1)}) = \cdots = \det(M_{q,f}^{(t+1)}) = 0$, *and* $\det(M_{q,f}^{(t)}) \neq 0$.

A $q$-polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ is scattered if and only if for any $m \in \mathbb{F}_{q^n}$ the dimension of the kernel of $f_m(x) = mx + f(x)$ is at most one. So, by Theorem 1.1 a necessary and sufficient condition for $f(x)$ to be scattered is that the system of two equations

$$\det(M_{q,f_m}^{(n)}) = \det(M_{q,f_m}^{(n-1)}) = 0$$

has no solution in the variable $m \in \mathbb{F}_{q^n}$.

In this paper a condition consisting of one equation (Proposition 2.2) is proved, and applied to two binomials. It would seem that one equation is better than two in order to prove that a given $q$-polynomial $f(x)$ is not scattered, while two equations will usually be more helpful in the proof that $f(x)$ is. As a matter of fact, here the condition $\mathrm{N}_{q^n/q}(\delta) \neq 1$ is proved to be necessary for the Lunardon–Polverino binomial to be scattered (cf. Theorem 3.4). Furthermore, two necessary and sufficient conditions for $x^{q^s} + bx^{q^{2s}}$ (where $\gcd(s, n) = 1$) to be scattered are stated in Propositions 3.5 and 3.10 . This leads to the fact that the polynomial $x^q + bx^{q^2}$, $b \neq 0$, is never scattered if $n \geq 5$ (cf. Proposition 3.8 and Remark 3.11).

## 2. A condition for scattered linearized polynomials

In this paper $s$, $n$, $q$ and $\sigma$ will always denote natural numbers such that $n \geq 3$, $\gcd(s,n) = 1$, $q$ is the power of a prime and $\sigma = q^s$. Any $\mathbb{F}_q$-linear endomorphism of $\mathbb{F}_{q^n}$ can be represented in the form

$$f(x) = a_0 x + a_1 x^{\sigma} + a_2 x^{\sigma^2} + \cdots + a_{n-1} x^{\sigma^{n-1}} \in \mathbb{F}_{q^n}[x]. \tag{2}$$

As a matter of fact, if $\tau$ is the permutation $i \mapsto is$ of $\mathbb{Z}/(n)$, then $f(x)$ is the same function of $\tilde{f}(x) = \sum_{i=0}^{n-1} a_{\tau^{-1}(i)} x^{q^i}$. Generalizing the notion of Dickson matrix given in the previous section, the *$\sigma$-matrix of Dickson* associated with the linearized polynomial $g(t) = \sum_{i=0}^{n-1} a_i t^{\sigma^i}$ is

$$M_{\sigma,g} = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1}^{\sigma} & a_0^{\sigma} & a_1^{\sigma} & \cdots & a_{n-2}^{\sigma} \\ a_{n-2}^{\sigma^2} & a_{n-1}^{\sigma^2} & a_0^{\sigma^2} & \cdots & a_{n-3}^{\sigma^2} \\ \vdots & & & & \vdots \\ a_1^{\sigma^{n-1}} & a_2^{\sigma^{n-1}} & a_3^{\sigma^{n-1}} & \cdots & a_0^{\sigma^{n-1}} \end{pmatrix}.$$

This is just the Dickson matrix $M_{q,\tilde{g}}$ associated with $\tilde{g}(t)$ after a permutation of the row and columns. Indeed, the element in row $r$ and column $c$ of $M_{q,\tilde{g}}$, $r, c \in \{0, 1, \ldots, n-1\}$, is $m_{rc} = a_{\tau^{-1}(c-r)}^{q^r} = a_{\tau^{-1}(c)-\tau^{-1}(r)}^{q^r}$. By applying $\tau$ to both the row and column index, $m_{\tau(r)\tau(c)} = a_{c-r}^{\sigma^r}$ follows. Therefore, the rank of $M_{\sigma,g}$ equals the rank of $g(t)$.

*Remark 2.1.* Each row of an $n$-order $\sigma$-matrix of Dickson is obtained from the previous one (cyclically) by the map

$$\phi : (X_0, X_1, \ldots, X_{n-1}) \mapsto (X_{n-1}, X_0, \ldots, X_{n-2})^{\sigma}$$

which is an invertible semilinear map of $\mathbb{F}_{q^n}^n$ into itself.

The polynomial (2) is scattered if and only if $f_1(x) = \sum_{i=1}^{n-1} a_i x^{\sigma^i}$ is. Hence in the following $a_0$ will always be zero.

**Proposition 2.2.** *Let $f(x) = \sum_{i=1}^{n-1} a_i x^{\sigma^i}$ be a linearized polynomial over $\mathbb{F}_{q^n}$, and*

$$g(t) = g_x(t) = -f(x)t + \sum_{i=1}^{n-1} a_i x^{\sigma^i} t^{\sigma^i} = -f(x)t + f(xt).$$

*Then the following conditions are equivalent:*

(i) *the polynomial $f(x)$ is scattered;*
(ii) *for any $x \in \mathbb{F}_{q^n}^*$, a nonsingular $(n-1)$-order minor of $M_{\sigma,g}$ exists;*
(iii) *for any $x \in \mathbb{F}_{q^n}^*$, all $(n-1)$-order minors of $M_{\sigma,g}$ are nonsingular.*

*Proof.* The polynomial $f(x)$ is scattered if and only if for any $x \in \mathbb{F}_{q^n}^*$ the rank of $h(t) = xf(t) - tf(x)$ is $n-1$, that is, the rank of

$$M_{\sigma,h} = \begin{pmatrix} -f(x) & a_1x & a_2x & \dots & a_{n-1}x \\ a_{n-1}^{\sigma}x^{\sigma} & -f(x)^{\sigma} & a_1^{\sigma}x^{\sigma} & \dots & a_{n-2}^{\sigma}x^{\sigma} \\ a_{n-2}^{\sigma^2}x^{\sigma^2} & a_{n-1}^{\sigma^2}x^{\sigma^2} & -f(x)^{\sigma^2} & \dots & a_{n-3}^{\sigma^2}x^{\sigma^2} \\ \vdots & & & & \vdots \\ a_1^{\sigma^{n-1}}x^{\sigma^{n-1}} & a_2^{\sigma^{n-1}}x^{\sigma^{n-1}} & a_3^{\sigma^{n-1}}x^{\sigma^{n-1}} & \dots & -f(x)^{\sigma^{n-1}} \end{pmatrix}$$

is always $n-1$. By dividing the rows of $M_{\sigma,h}$ by $x$'s, $x^{\sigma}$, $x^{\sigma^2}$, ..., $x^{\sigma^{n-1}}$, respectively, and then multiplying the columns for that same elements, one obtains

$$\begin{pmatrix} -f(x) & a_1x^{\sigma} & a_2x^{\sigma^2} & \dots & a_{n-1}x^{\sigma^{n-1}} \\ a_{n-1}^{\sigma}x & -f(x)^{\sigma} & a_1^{\sigma}x^{\sigma^2} & \dots & a_{n-2}^{\sigma}x^{\sigma^{n-1}} \\ a_{n-2}^{\sigma^2}x & a_{n-1}^{\sigma^2}x^{\sigma} & -f(x)^{\sigma^2} & \dots & a_{n-3}^{\sigma^2}x^{\sigma^{n-1}} \\ \vdots & & & & \vdots \\ a_1^{\sigma^{n-1}}x & a_2^{\sigma^{n-1}}x^{\sigma} & a_3^{\sigma^{n-1}}x^{\sigma^2} & \dots & -f(x)^{\sigma^{n-1}} \end{pmatrix},$$

that is, the matrix $M_{\sigma,g}$. By Remark 2.1, if a $\sigma$-matrix of Dickson is singular, then any row is a linear combination of the remaining ones. Hence the rank of $M_{\sigma,g}$ equals the rank of any $(n-1)\times n$ matrix obtained from it by deleting a row. Furthermore, since the sum of the columns of $M_{\sigma,g}$ is zero, all $(n-1)$-order minors have the same rank of $M_{\sigma,g}$. □

## 3. Two linearized binomials

**Definition 3.1.** For any $\delta \in \mathbb{F}_{q^n}$,

$$f_{\sigma,\delta}(x) = x^{\sigma} + \delta x^{\sigma^{n-1}}$$

is the *Lunardon–Polverino binomial.*

If $\mathrm{N}_{q^n/q}(\delta) \neq 1$, then $f_{\sigma,\delta}$ is scattered [11–13,20].

**Proposition 3.2.** *The polynomial $f_{\sigma,\delta}(x)$ is scattered if only if there is no $x \in \mathbb{F}_{q^n}^*$ such that*

$$\sum_{i=0}^{n-1} z^{(\sigma^i-1)/(\sigma-1)} = 0, \tag{3}$$

*where $z = \delta x^{\sigma^{n-1}-\sigma}$.*

*Proof.* The $(n-1)$-th order North-West principal minor of the $\sigma$-matrix of Dickson associated with the polynomial

$$g(t) = -f_{\sigma,\delta}(x)t + \sum_{i=1}^{n-1} a_i x^{\sigma^i} t^{\sigma^i} = -f_{\sigma,\delta}(x)t + x^{\sigma}t^{\sigma} + \delta x^{\sigma^{n-1}} t^{\sigma^{n-1}},$$

further normalized row by row, is

$$B(z)=\begin{pmatrix} -(1+z) & 1 & 0 & 0 & \cdots & 0 & 0 \\ z^{\sigma} & -(1+z)^{\sigma} & 1 & 0 & \cdots & 0 & 0 \\ 0 & z^{\sigma^2} & -(1+z)^{\sigma^2} & 1 & \cdots & 0 & 0 \\ \vdots & & & & & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & -(1+z)^{\sigma^{n-3}} & 1 \\ 0 & 0 & 0 & 0 & \cdots & z^{\sigma^{n-2}} & -(1+z)^{\sigma^{n-2}} \end{pmatrix}. \tag{4}$$

By Laplace expansion along the last column and induction on $n$, the determinant of $B(z)$ can be computed as $(-1)^{n+1}\sum_{i=0}^{n-1} z^{(\sigma^i-1)/(\sigma-1)}$. □

The following can be useful in understanding the role of $\delta$:

**Proposition 3.3.** *Let $z\in\mathbb{F}_{q^n}$. Then (3) holds if and only if there exists a $y\in\mathbb{F}_{q^n}^*$ such that $z=y^{\sigma-1}$ and $Tr_{q^n/q}(y)=0$.*

*Proof.* Any solution of (3) is nonzero. Raising $\sum_{i=0}^{n-1} z^{(\sigma^i-1)/(\sigma-1)}$ to the $\sigma$, multiplying by $z$ and then subtracting to the original equation yields $1-\mathrm{N}_{q^n/q}(z)=0$. So, $z$ is a solution of (3) if and only if $z=y^{\sigma-1}$ for some $y\in\mathbb{F}_{q^n}^*$, and $\sum_{i=0}^{n-1} y^{\sigma^i-1}=0$. The latter equation is equivalent to $\mathrm{Tr}_{q^n/q}(y)=0$. □

Propositions 3.2 and 3.3 together show that, if $f_{\sigma,\delta}$ is not scattered, then there is an $x\in\mathbb{F}_{q^n}$ such that $\mathrm{N}_{q^n/q}(\delta x^{\sigma^{n-1}-\sigma})=\mathrm{N}_{q^n/q}(\delta)\,\mathrm{N}_{q^n/q}(x^{\sigma^{n-1}-\sigma})=1$. On the other hand, $q-1$ divides $\sigma^{n-1}-\sigma$, hence $\mathrm{N}_{q^n/q}(x^{\sigma^{n-1}-\sigma})=1$. Summarizing, if $\mathrm{N}_{q^n/q}(\delta)\neq 1$, then the Lunardon–Polverino binomial is scattered, as is known.

**Theorem 3.4.** *If $\mathrm{N}_{q^n/q}(\delta)=1$, then the Lunardon–Polverino binomial $f_{\sigma,\delta}(x)$ is not scattered.*

*Proof.* <u>Case odd $n$.</u> Since

$$x^{\sigma^{n-1}-\sigma}=(x^{\sigma})^{\sigma^{n-2}-1}$$

and $\gcd(s(n-2),n)=1$, the expression $x^{\sigma^{n-1}-\sigma}$ takes all values in $\mathbb{F}_{q^n}$ whose norm over $\mathbb{F}_q$ is equal to one. This allows the substitution $\delta x^{\sigma^{n-1}-\sigma}=w^{\sigma-1}$ into (3). So, $f_{\sigma,\delta}(x)$ is not scattered if and only if $\mathrm{Tr}_{q^n/q}(w)=0$ for some nonzero $w$ and this is trivial.

<u>Case even $n$.</u> Since $\gcd(\sigma^{n-2}-1,\sigma^n-1)=\sigma^2-1$, the set of all powers of elements in $\mathbb{F}_{q^n}$ with exponent $\sigma^{n-2}-1$ coincides with the set of all powers with exponent $\sigma^2-1$. Hence for any $x\in\mathbb{F}_{q^n}$ there exists $u\in\mathbb{F}_{q^n}$ such that $x^{\sigma^{n-1}-\sigma}=u^{\sigma^2-1}$, and conversely. This allows the substitution $z=\delta u^{\sigma^2-1}$ in (3), meaning that if there is $u$ such that

$$\sum_{i=0}^{n-1}\left(\delta u^{\sigma^2-1}\right)^{(\sigma^i-1)/(\sigma-1)}=0, \tag{5}$$

then $f_{\sigma,\delta}(x)$ is not scattered. So, taking $\delta = d^{\sigma-1}$, (5) is equivalent to $\mathrm{Tr}_{q^n/q}(du^{\sigma+1}) = 0$, $u \neq 0$. This is a quadratic form in $u$ in a vector space over $\mathbb{F}_q$ of dimension greater than two which has at least one nontrivial zero. □

The theorem above has been proved in the particular cases $n = 4$ in [10], $s = 1$ in [2], both $n$ and $q$ odd in [11], and odd $n$ in [22].

**Proposition 3.5.** *The polynomial $f(x) = x^\sigma + bx^{\sigma^2}$ is scattered if only if there is no $x \in \mathbb{F}_{q^n}^*$ such that*

$$\sum_{i=0}^{n-1} w^{(\sigma^i-1)/(\sigma-1)} = 0, \quad \textit{where } w = -(1 + b^{-1}x^{\sigma-\sigma^2}). \tag{6}$$

*Proof.* The $\sigma$-matrix of Dickson associated with the polynomial

$$g(t) = -f(x)t + x^\sigma t^\sigma + bx^{\sigma^2} t^{\sigma^2},$$

further normalized by dividing the rows by $bx^{\sigma^2}$, $b^\sigma x^{\sigma^3}$, ... is

$$A = \begin{pmatrix} w & -(1+w) & 1 & \cdots & 0 & 0 \\ 0 & w^\sigma & -(1+w)^\sigma & \cdots & 0 & 0 \\ 0 & 0 & w^{\sigma^2} & \cdots & 0 & 0 \\ \vdots & & & & & \vdots \\ 1 & 0 & 0 & \cdots & w^{\sigma^{n-2}} & -(1+w)^{\sigma^{n-2}} \\ -(1+w)^{\sigma^{n-1}} & 1 & 0 & \cdots & 0 & w^{\sigma^{n-1}} \end{pmatrix}.$$

The matrix obtained by deleting the last row and first column is $B(w)$ (cf. (4)). □

**Corollary 3.6.** *Assume $b_1, b_2 \in \mathbb{F}_{q^n}$ and $\mathrm{N}_{q^n/q}(b_1) = \mathrm{N}_{q^n/q}(b_2)$. Then the polynomials $f_i(x) = x^\sigma + b_i x^{\sigma^2}$, $i = 1, 2$, are either both scattered, or both non-scattered.*

*Proof.* If the norm of $b_1$ is zero then the statement is trivial, so assume that it is not. Define $w_i(x) = -(1+b_i^{-1}x^{\sigma-\sigma^2})$ for $i = 1, 2$, and note that $w_1(x) = w_2(y)$ is equivalent to $b_1/b_2 = ((x/y)^\sigma)^{\sigma-1}$, that is, $((x/y)^\sigma)^{\sigma-1} = c^{\sigma-1}$ for some $c \in \mathbb{F}_{q^n}^*$. This equation can be always solved in both $x$ and $y$, whence $w_1(x)$ and $w_2(y)$ take the same set of values. □

*Remark 3.7.* Corollary 3.6 allows to look at only $q-1$ linearized polynomials, given $s$, $n$, and $q$. This makes a computer search easier. Computations with GAP[1] show that there are no scattered linearized polynomials of the form $l_b(x) = x^q + bx^{q^2}$, $b \neq 0$, for any $q < 223$ if $n = 5$. In [17] it is proved that for $n = 5$ and $q \geq 223$ the linearized polynomial $l_b(x)$ is not scattered for any $b \neq 0$. The next proposition summarizes this.

[1]Code: https://pastebin.com/pgTXX76C.

**Proposition 3.8.** *If $n = 5$ and $b \in \mathbb{F}^*_{q^5}$, then the $q$-polynomial $l_b(x) = x^q + bx^{q^2} \in \mathbb{F}_{q^5}[x]$ is non-scattered.*

*Remark 3.9.* For $n = 4$ there are scattered polynomials of type $l_b(x)$, $b \neq 0$. By the results in [9,10], all the related linear sets are of Lunardon–Polverino type, up to collineations.

**Proposition 3.10.** *Let $b \in \mathbb{F}^*_{q^n}$. The polynomial $x^\sigma + bx^{\sigma^2} \in \mathbb{F}_{q^n}[x]$ is not scattered if and only if the algebraic curve $b^{-1}X^{q-1}+Y^{\sigma-1}+1 = 0$ in $\mathrm{AG}(2, q^n)$ has a point $(x_0, y_0)$ with coordinates in $\mathbb{F}^*_{q^n}$, such that $Tr_{q^n/q}(y_0) = 0$.*

*Proof.* By Proposition 3.3, the first equation in (6) is equivalent to the existence of $y \in \mathbb{F}^*_{q^n}$ such that $w = y^{\sigma-1}$, $\mathrm{Tr}_{q^n/q}(y) = 0$. The second equation $y^{\sigma-1} + 1 + b^{-1}x^{q-q^2} = 0$ has solutions with $x \neq 0$ if and only if $b^{-1}x^{q-1} + y^{\sigma-1} + 1 = 0$ does. □

*Remark 3.11.* Very recently, Montanucci [16] proved that if $n > 5$, then for any $q$ the algebraic curve $b^{-1}X^{q-1} + Y^{q-1} + 1 = 0$ has a point with the properties above. Together with Propositions 3.8 and 3.10 this implies that for $n \geq 5$ no $q$-polynomial of type $l_b(x) = x^q + bx^{q^2}$, $b \neq 0$, is scattered.

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

## References

[1] Bartoli, D., Giulietti, M., Marino, G., Polverino, O.: *Maximum scattered linear sets and complete caps in Galois spaces*. Combinatorica **38**, 255–278 (2018)

[2] Bartoli, D., Zhou, Y.: *Exceptional scattered polynomials*. J. Algebra **509**, 507–534 (2018)

[3] Blokhuis, A., Lavrauw, M.: *Scattered spaces with respect to a spread in* $\mathrm{PG}(n, q)$. Geom. Dedicata **81**, 231–243 (2000)

[4] Csajbók: Scalar $q$-subresultants and Dickson matrices (2019). arXiv:1909.06409

[5] Csajbók, B., Marino, G., Polverino, O., Zanella, C.: *A new family of MRD-codes*. Linear Algebra Appl. **548**, 203–220 (2018)

[6] Csajbók, B., Marino, G., Zullo, F.: *New maximum scattered linear sets of the projective line*. Finite Fields Appl. **54**, 133–150 (2018)

[7] Csajbók, B., Marino, G., Polverino, O., Zullo, F.: *A characterization of linearized polynomials with maximum kernel*. Finite Fields Appl. **56**, 109–130 (2019)

[8] Csajbók, B., Zanella, C.: *On the equivalence of linear sets*. Des. Codes Cryptogr. **81**, 269–281 (2016)

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

[10] Csajbók, B., Zanella, C.: *Maximum scattered* $\mathbb{F}_q$-linear sets of $\mathrm{PG}(1, q^4)$. Discrete Math. **341**, 74–80 (2018)

[11] Lavrauw, M., Marino, G., Polverino, O., Trombetti, R.: *Solution to an isotopism question concerning rank 2 semifields*. J. Combin. Des. **23**, 60–77 (2015)

[12] Lunardon, G., Polverino, O.: *Blocking sets and derivable partial spreads*. J. Algebr. Combin. **14**, 49–56 (2001)

[13] Lunardon, G., Trombetti, R., Zhou, Y.: *Generalized twisted Gabidulin codes*. J. Combin. Theory Ser. A **159**, 79–106 (2018)

[14] Marino, G., Montanucci, M., Zullo, F.: MRD-codes arising from the trinomial $x^q + x^{q^3} + cx^{q^5} \in \mathbb{F}_{q^6}[x]$ (2019). arXiv:1907.08122

[15] McGuire, G., Sheekey, J.: *A characterization of the number of roots of linearized and projective polynomials in the field of coefficients*. Finite Fields Appl. **57**, 68–91 (2019)

[16] Montanucci, M.: Private communication (2019) (**in progress**)

[17] Montanucci, M., Zanella, C.: A class of linear sets in $\mathrm{PG}(1, q^5)$ (2019). arXiv:1905.10772

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

[19] Polverino, O., Zullo, F.: On the number of roots of some linearized polynomials (2019). arXiv:1909.00802

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

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

[22] Zanella, C., Zullo, F.: Vertex properties of maximum scattered linear sets of $\mathrm{PG}(1, q^n)$ (2019). arXiv:1906.05611

Corrado Zanella
Dipartimento di Tecnica e Gestione dei Sistemi Industriali
Università degli Studi di Padova
Stradella S. Nicola, 3
36100 Vicenza VI
Italy
e-mail: corrado.zanella@unipd.it

Received: August 4, 2019.
Revised: September 10, 2019.