A characterization of linearized polynomials with maximum kernel

Bence Csajbók, Giuseppe Marino, Olga Polverino, Ferdinando Zullo*

Abstract

We provide sufficient and necessary conditions for the coefficients of a q-polynomial f over $\mathbb{F}_{q^n}$ which ensure that the number of distinct roots of f in $\mathbb{F}_{q^n}$ equals the degree of f. We say that these polynomials have maximum kernel. As an application we study in detail q-polynomials of degree q^{n-2} over $\mathbb{F}_{q^n}$ which have maximum kernel and for $n \leq 6$ we list all q-polynomials with maximum kernel. We also obtain information on the splitting field of an arbitrary q-polynomial. Analogous results are proved for q^s-polynomials as well, where $\gcd(s, n) = 1$.

AMS subject classification: 11T06, 15A04

Keywords: Linearized polynomials, linear transformations, semilinear transformations

1 Introduction

A q-polynomial over $\mathbb{F}_{q^n}$ is a polynomial of the form $f(x) = \sum_i a_i x^{q^i}$, where $a_i \in \mathbb{F}_{q^n}$. We will denote the set of these polynomials by $\mathcal{L}_{n,q}$. Let $\mathbb{K}$ denote

*The research was supported by Ministry for Education, University and Research of Italy MIUR (Project PRIN 2012 "Geometrie di Galois e strutture di incidenza") and by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The first author was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and by OTKA Grant No. K 124950.

the algebraic closure of $\mathbb{F}_{q^n}$. Then for every $\mathbb{F}_{q^n} \leq \mathbb{L} \leq \mathbb{K}$, f defines an $\mathbb{F}_q$-linear transformation of $\mathbb{L}$, when $\mathbb{L}$ is viewed as an $\mathbb{F}_q$-vector space. If $\mathbb{L}$ is a finite field of size q^m then the polynomials of $\mathcal{L}_{n,q}$ considered modulo $(x^{q^m}-x)$ form an $\mathbb{F}_q$-subalgebra of the $\mathbb{F}_q$-linear transformations of $\mathbb{L}$. Once this field $\mathbb{L}$ is fixed, we can define the *kernel* of f as the kernel of the corresponding $\mathbb{F}_q$-linear transformation of $\mathbb{L}$, which is the same as the set of roots of f in $\mathbb{L}$; and the *rank* of f as the rank of the corresponding $\mathbb{F}_q$-linear transformation of $\mathbb{L}$. Note that the kernel and the rank of f depend on this field $\mathbb{L}$ and from now on we will consider the case $\mathbb{L} = \mathbb{F}_{q^n}$. In this case $\mathcal{L}_{n,q}$ considered modulo $(x^{q^n}-x)$ is isomorphic to the $\mathbb{F}_q$-algebra of $\mathbb{F}_q$-linear transformations of the n-dimensional $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$. The elements of this factor algebra are represented by $\tilde{\mathcal{L}}_{n,q} := \{\sum_{i=0}^{n-1} a_i x^{q^i} : a_i \in \mathbb{F}_{q^n}\}$. For $f \in \tilde{\mathcal{L}}_{n,q}$ if $\deg f = q^k$ then we call k the *q-degree* of f. It is clear that in this case the kernel of f has dimension at most k and the rank of f is at least $n-k$.

Let $U = \langle u_1, u_2, \ldots, u_k \rangle_{\mathbb{F}_q}$ be a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$. It is well known that, up to a scalar factor, there is a unique q-polynomial of q-degree k, which has kernel U. We can get such a polynomial as the determinant of the matrix

$$\begin{pmatrix} x & x^q & \cdots & x^{q^k} \\ u_1 & u_1^q & \cdots & u_1^{q^k} \\ \vdots & & & \\ u_k & u_k^q & \cdots & u_k^{q^k} \end{pmatrix}.$$

The aim of this paper is to study the other direction, i.e. when a given $f \in \tilde{\mathcal{L}}_{n,q}$ with q-degree k has kernel of dimension k. If this happens then we say that f is a q-polynomial with *maximum kernel*.

If $f(x) \equiv a_0 x + a_1 x^{\sigma} + \cdots + a_k x^{\sigma^k} \pmod{x^{q^n} - x}$, with $\sigma = q^s$ for some s with $\gcd(s,n) = 1$, then we say that $f(x)$ is a σ-polynomial (or q^s-polynomial) with σ-degree (or q^s-degree) k. Regarding σ-polynomials the following is known.

Result 1.1. *[7, Theorem 5] Let $\mathbb{L}$ be a cyclic extension of a field $\mathbb{F}$ of degree n, and suppose that σ generates the Galois group of $\mathbb{L}$ over $\mathbb{F}$. Let k be an integer satisfying $1 \leq k \leq n$, and let $a_0, a_1, \ldots, a_k$ be elements of $\mathbb{L}$, not all them are zero. Then the $\mathbb{F}$-linear transformation defined as*

$$f(x) = a_0 x + a_1 x^{\sigma} + \cdots + a_k x^{\sigma^k}$$

has kernel with dimension at most k in $\mathbb{L}$.

Similarly to the $s = 1$ case we will say that a σ-polynomial is of *maximum kernel* if the dimension of its kernel equals its σ-degree.

Linearized polynomials have been used to describe families of $\mathbb{F}_q$-linear *maximum rank distance codes* (*MRD-codes*), i.e. $\mathbb{F}_q$-subspaces of $\tilde{\mathcal{L}}_{n,q}$ of order q^{nk} in which each element has kernel of dimension at most k. The first examples of MRD-codes found were the *generalized Gabidulin codes* [3, 5], that is $\mathcal{G}_{k,s} = \langle x, x^{q^s}, \ldots, x^{q^{s(k-1)}} \rangle_{\mathbb{F}_{q^n}}$ with $\gcd(s,n) = 1$; the fact that $\mathcal{G}_{k,s}$ is an MRD-code can be shown simply by using Result 1.1. It is important to have explicit conditions on the coefficients of a linearized polynomial characterizing the number of its roots. Further connections with projective polynomials can be found in [8].

Our main result provides sufficient and necessary conditions on the coefficients of a σ-polynomial with maximum kernel.

Theorem 1.2. *Consider*

$$f(x) = a_0 x + a_1 x^{\sigma} + \cdots + a_{k-1} x^{\sigma^{k-1}} - x^{\sigma^k},$$

with $\sigma = q^s$, $\gcd(s,n) = 1$ *and* $a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}$. *Then* $f(x)$ *is of maximum kernel if and only if the matrix*

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix} \tag{1}$$

satisfies

$$AA^{\sigma} \cdots A^{\sigma^{n-1}} = I_k,$$

where A^{σ^i} *is the matrix obtained from* A *by applying to each of its entries the automorphism* $x \mapsto x^{\sigma^i}$ *and* I_k *is the identity matrix of order* k.

An immediate consequence of this result gives information on the splitting field of an arbitrary σ-polynomial, cf. Theorem 4.1.

In Section 3.1 we study in details the σ-polynomials of σ-degree $n-2$ for each n. For $n \leq 6$ we also provide a list of all σ-polynomials with maximum kernel cf. Sections 3.2, 3.3 and 3.4. These results might yield further classification results and examples of $\mathbb{F}_q$-linear MRD-codes.

2 Preliminary Results

In this section we recall some results of Dempwolff, Fisher and Herman from [4], adapting them to our needs in order to make this paper self-contained.

Let V be a k-dimensional vector space over the field $\mathbb{F}$ and let T be a semilinear transformation of V. A T-cyclic subspace of V is an $\mathbb{F}$-subspace of V spanned by $\{\mathbf{v}, T(\mathbf{v}), \ldots\}$ over $\mathbb{F}$ for some $\mathbf{v} \in V$, which will be denoted by $[\mathbf{v}]$. We first recall the following lemma.

Lemma 2.1. *[4, Theorem 1] Let V be an n-dimensional vector space over the field $\mathbb{F}$, σ an automorphism of $\mathbb{F}$ and T an invertible σ-semilinear transformation on V. Then*

$$V = [\mathbf{u}_1] \oplus \ldots \oplus [\mathbf{u}_r]$$

for T-cyclic subspaces satisfying $\dim[\mathbf{u}_1] \geq \dim[\mathbf{u}_2] \geq \ldots \geq \dim[\mathbf{u}_r] \geq 1$.

Theorem 2.2. *Let T be an invertible semilinear transformation of $V = V(k, q^n)$ of order n, with companion automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that $\mathrm{Fix}(\sigma) = \mathbb{F}_q$. Then $\mathrm{Fix}(T)$ is a k-dimensional $\mathbb{F}_q$-subspace of V and $\langle \mathrm{Fix}(T) \rangle_{\mathbb{F}_{q^n}} = V$.*

Proof. First assume that the companion automorphism of T is $x \mapsto x^q$ and that there exists $\mathbf{v} \in V$ such that

$$V = \langle \mathbf{v}, T(\mathbf{v}), \ldots, T^{k-1}(\mathbf{v}) \rangle_{\mathbb{F}_{q^n}}.$$

Following the proof of [4, Main Theorem], consider the ordered basis $\mathcal{B}_T = (\mathbf{v}, T(\mathbf{v}), \ldots, T^{k-1}(\mathbf{v}))$ and let A be the matrix associated with T with respect to the basis $\mathcal{B}_T$, i.e.

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & \alpha_0 \\ 1 & 0 & \cdots & 0 & \alpha_1 \\ 0 & 1 & \cdots & 0 & \alpha_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & \alpha_{k-1} \end{pmatrix} \in \mathbb{F}_{q^n}^{k \times k}, \tag{2}$$

where $T^k(\mathbf{v}) = \sum_{i=1}^{k} \alpha_{i-1} T^i(\mathbf{v})$ with $\alpha_0, \ldots, \alpha_{k-1} \in \mathbb{F}_{q^n}$ and, since T is invertible, we have $\alpha_0 \neq 0$. Denote by $\overline{T}$ the semilinear transformation of $\mathbb{F}_{q^n}^k$ having A as the associated matrix with respect to the canonical ordered basis $\mathcal{B}_C = (\mathbf{e}_1, \ldots, \mathbf{e}_k)$ of $\mathbb{F}_{q^n}^k$ and companion automorphism $x \mapsto x^q$. Note that $c_{\mathcal{B}_T}(\mathrm{Fix}(T)) = \mathrm{Fix}(\overline{T})$, where $c_{\mathcal{B}_T}$ is the coordinatization with respect to the basis $\mathcal{B}_T$. Also, since T has order n, we have

$$AA^q \cdots A^{q^{n-1}} = I_k, \tag{3}$$

where A^{q^i}, for $i \in \{1, \ldots, n-1\}$, is the matrix obtained from A by applying to each of its entries the automorphism $x \mapsto x^{q^i}$. A vector $\mathbf{z} = (z_0, \ldots, z_{k-1}) \in \mathbb{F}_{q^n}^k$ is fixed by $\overline{T}$ if and only if

$$\begin{cases} \alpha_0 z_{k-1}^q = z_0 \\ z_0^q + \alpha_1 z_{k-1}^q = z_1 \\ \vdots \\ z_{k-2}^q + \alpha_{k-1} z_{k-1}^q = z_{k-1} \end{cases}$$

Eliminating $z_0, \ldots, z_{k-2}$, we obatin the equation

$$\alpha_0^{q^{k-1}} z_{k-1}^{q^k} + \alpha_1^{q^{k-2}} z_{k-1}^{q^{k-1}} + \ldots + \alpha_{k-1} z_{k-1}^q - z_{k-1} = 0,$$

which has q^k distinct solutions in the algebraic closure $\mathbb{K}$ of $\mathbb{F}_{q^n}$ by the derivative test. Each solution determines a unique vector of $\mathrm{Fix}(\overline{T})$ in $\mathbb{K}^k$. Also, the set $\mathrm{Fix}(\overline{T})$ is an $\mathbb{F}_q$-subspace of $\mathbb{K}^k$ and hence $\dim_{\mathbb{F}_q} \mathrm{Fix}(\overline{T}) = k$. Let $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ be an $\mathbb{F}_q$-basis of $\mathrm{Fix}(\overline{T})$ and note that since $|\mathrm{Fix}(\overline{T})| = q^k$, a vector $\sum_{i=1}^{k} a_i \mathbf{w}_i$ is fixed by $\overline{T}$ if and only if $a_i \in \mathbb{F}_q$. This implies that $\mathbf{w}_1, \ldots, \mathbf{w}_k$ are also $\mathbb{K}$-independent. Thus $\langle \mathrm{Fix}(\overline{T}) \rangle_{\mathbb{K}} = \mathbb{K}^k$ and $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ is also a $\mathbb{K}$-basis of $\mathbb{K}^k$. Denote by ϕ the $\mathbb{K}$-linear transformation such that $\phi(\mathbf{w}_i) = \mathbf{e}_i$ and by P the associated matrix with respect to the canonical basis $\mathcal{B}_C$, so $P \in \mathrm{GL}(k, \mathbb{K})$. The semilinear transformation $\phi \circ \overline{T} \circ \phi^{-1}$ has companion automorphism $x \mapsto x^q$, order n and associated matrix with respect to the canonical basis $P \cdot A \cdot P^{-q}$, where P^{-q} is the inverse of P in which the automorphism $x \mapsto x^q$ is applied entrywise. Note that $\phi \circ \overline{T} \circ \phi^{-1}(\mathbf{e}_i) = \phi(\overline{T}(\mathbf{w}_i)) = \phi(\mathbf{w}_i) = \mathbf{e}_i$, hence

$$P \cdot A \cdot P^{-q} = I_k, \tag{4}$$

i.e.

$$P^q = P \cdot A. \tag{5}$$

By Equations (3) and (5) and using induction we get

$$P^{q^n} = P \cdot A \cdot A^q \cdot \ldots \cdot A^{q^{n-1}} = P,$$

i.e. $P \in \mathbb{F}_{q^n}^{k\times k}$. This implies that $\mathrm{Fix}(\overline{T})$ is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}^k$ of dimension k and hence $\mathrm{Fix}(T) = c_{\mathcal{B}_T}^{-1}(\mathrm{Fix}(\overline{T}))$ is a k-dimensional subspace of $V(k, q^n)$ with the property that $\langle \mathrm{Fix}(T)\rangle_{\mathbb{F}_{q^n}} = V$.

Consider now the general case, i.e. suppose T as in the statement, that is T is an invertible semilinear map of order n with companion automorphism $x \mapsto x^{q^s}$ and $\gcd(s, n) = 1$. Since $\gcd(s, n) = 1$ there exist $l, m \in \mathbb{N}$ such that $1 = sl + mn$, and hence $\gcd(l, n) = 1$. Then the semilinear transformation T^l has order n, companion automorphism $x \mapsto x^q$ and $\mathrm{Fix}(T) = \mathrm{Fix}(T^l)$. By Lemma 2.1, we may write

$$V = [\mathbf{u}_1] \oplus \ldots \oplus [\mathbf{u}_r],$$

where $[\mathbf{u}_i]$ is a T^l-cyclic subspace of V of dimension $m_i \geq 1$, for each $i \in \{1, \ldots, r\}$, and $\sum_{i=1}^r m_i = k$. Then we can restrict T^l to each subspace $[\mathbf{u}_i]$ and by applying the previous arguments we get that $U_i = \mathrm{Fix}(T^l|_{[\mathbf{u}_i]})$ is an $\mathbb{F}_q$-subspace of $[\mathbf{u}_i]$ of dimension m_i with the property that $\langle U_i\rangle_{\mathbb{F}_{q^n}} = [\mathbf{u}_i]$. Thus

$$\mathrm{Fix}(T) = \mathrm{Fix}(T^l) = U_1 \oplus \ldots \oplus U_r$$

is an $\mathbb{F}_q$-subspace of dimension k of V with the property that $\langle \mathrm{Fix}(T)\rangle_{\mathbb{F}_{q^n}} = V$. $\square$

The existence of a matrix $P \in \mathrm{GL}(k, \mathbb{K})$, with $\mathbb{K}$ the algebraic closure of a finite field of order q, satisfying (4) is also a consequence of the celebrated Lang's Theorem [9] on connected linear algebraic groups. More precisely, by Lang's Theorem, since $\mathrm{GL}(k, \mathbb{K})$ is a connected linear algebraic group, the map $M \in \mathrm{GL}(k, \mathbb{K}) \mapsto M^{-1} \cdot M^q \in \mathrm{GL}(k, \mathbb{K})$ is onto. In Theorem 2.2 it is proved that, if the semilinear transformation of $V(k, q^n)$ having A as associated matrix has order n, then $P \in \mathrm{GL}(k, \mathbb{F}_{q^n})$.

Remark 2.3. *Let T be an invertible semilinear transformation of $V = V(k, q^n)$ with companion automorphism $x \mapsto x^q$ and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_{q^n}$. Denote by $\overline{T}$ the semilinear transformation of $\mathbb{K}^k$ associated with T as in the proof of Theorem 2.2. If $\lambda \in \mathbb{K}$, then the set $E(\lambda) := \{\mathbf{v} \in \mathbb{K}^k : \overline{T}(\mathbf{v}) = \lambda\mathbf{v}\}$ is an $\mathbb{F}_q$-subspace of $\mathbb{K}^k$. By [4, page 293], it follows that $E(\lambda) = \lambda^{\frac{1}{q-1}}\mathrm{Fix}(\overline{T})$ and by [4, Main Theorem] $E(\lambda)$ is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{K}^k$. Also, when T has order n and $\lambda^{\frac{1}{q-1}} \in \mathbb{F}_{q^n}$, by Theorem 2.2, $E(\lambda)$ is a k-dimensional $\mathbb{F}_q$-subspace contained in $\mathbb{F}_{q^n}^k$ such that $\langle E(\lambda)\rangle_{\mathbb{F}_{q^n}} = \mathbb{F}_{q^n}^k$.*

3 Main Results

Now we are able to prove our main result:

Proof of Theorem 1.2. First suppose $\dim_{\mathbb{F}_q} \ker f = k$. Then there exist $u_0, u_1, \ldots, u_{k-1} \in \mathbb{F}_{q^n}$ which form an $\mathbb{F}_q$-basis of $\ker f$.
Put $\mathbf{u} := (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_{q^n}^k$. Since $u_0, u_1, \ldots, u_{k-1}$ are $\mathbb{F}_q$-linearly independent, by [10, Lemma 3.51], we get that $\mathcal{B} := (\mathbf{u}, \mathbf{u}^{q^s}, \ldots, \mathbf{u}^{q^{s(k-1)}})$ is an ordered $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^n}^k$. Also, $\mathbf{u}^{q^{sk}} = a_0\mathbf{u} + a_1\mathbf{u}^{q^s} + \cdots + a_{k-1}\mathbf{u}^{q^{s(k-1)}}$. It can be seen that the matrix (1) represents the $\mathbb{F}_{q^n}$-linear part of the $\mathbb{F}_{q^n}$-semilinear map $\overline{\sigma}\colon \mathbf{v} \in \mathbb{F}_{q^n}^k \mapsto \mathbf{v}^{q^s} \in \mathbb{F}_{q^n}^k$ w.r.t. the basis $\mathcal{B}$. Since $\gcd(s,n) = 1$, $\overline{\sigma}$ has order n and hence the assertion follows.

Viceversa, let τ be defined as follows

$$\tau\colon \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{pmatrix} \in \mathbb{F}_{q^n}^k \mapsto A \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{pmatrix}^{q^s} \in \mathbb{F}_{q^n}^k, \tag{6}$$

where A is as in (1) with the property $AA^{q^s} \cdots A^{q^{s(n-1)}} = I_k$. Then τ has order n and, by Theorem 2.2, it fixes a k-dimensional $\mathbb{F}_q$-subspace $\mathcal{S}$ of $\mathbb{F}_{q^n}^k$ with the property that $\langle \mathcal{S} \rangle_{\mathbb{F}_{q^n}} = \mathbb{F}_{q^n}^k$.

Let $\mathcal{B}_{\mathcal{S}} = (\mathbf{s}_0, \ldots, \mathbf{s}_{k-1})$ be an $\mathbb{F}_q$-basis of $\mathcal{S}$ and note that, since $\langle \mathcal{S} \rangle_{\mathbb{F}_{q^n}} = \mathbb{F}_{q^n}^k$, $\mathcal{B}_{\mathcal{S}}$ is also an $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^n}^k$, then denoting by $\mathcal{B}_C$ the canonical ordered basis of $\mathbb{F}_{q^n}^k$, there exists a unique isomorphism ϕ of $\mathbb{F}_{q^n}^k$ such that $\phi(\mathbf{s}_i) = \mathbf{e}_i$ for each $i \in \{1, \ldots, k\}$. Then $\overline{\sigma} = \phi \circ \tau \circ \phi^{-1}$, where $\overline{\sigma}\colon \mathbf{v} \in \mathbb{F}_{q^n}^k \mapsto \mathbf{v}^{q^s} \in \mathbb{F}_{q^n}^k$. Also,

$$\overline{\sigma}^i = \phi \circ \tau^i \circ \phi^{-1}, \tag{7}$$

for each $i \in \{1, \ldots, n-1\}$. Also, by (6)

$$\begin{aligned}
&\tau(\mathbf{e}_0) = \mathbf{e}_1, \\
&\tau(\mathbf{e}_1) = \tau^2(\mathbf{e}_0) = \mathbf{e}_2, \\
&\vdots \\
&\tau(\mathbf{e}_{k-1}) = \tau^k(\mathbf{e}_0) = (a_0, \ldots, a_{k-1}) = a_0\mathbf{e}_0 + \cdots + a_{k-1}\mathbf{e}_{k-1}.
\end{aligned}$$

So, we get that

$$\tau^k(\mathbf{e}_0) = a_0\mathbf{e}_0 + a_1\tau(\mathbf{e}_0) + \cdots + a_{k-1}\tau^{k-1}(\mathbf{e}_0),$$

and applying ϕ it follows that

$$\phi(\tau^k(\mathbf{e}_0)) = a_0\phi(\mathbf{e}_0) + a_1\phi(\tau(\mathbf{e}_0)) + \cdots + a_{k-1}\phi(\tau^{k-1}(\mathbf{e}_0)).$$

By (7) the previous equation becomes

$$\overline{\sigma}^k(\phi(\mathbf{e}_0)) = a_0\phi(\mathbf{e}_0) + a_1\overline{\sigma}(\phi(\mathbf{e}_0)) + \cdots + a_{k-1}\overline{\sigma}^{k-1}(\phi(\mathbf{e}_0)).$$

Put $\mathbf{u} = \phi(\mathbf{e}_0)$, then

$$\mathbf{u}^{q^{sk}} = a_0\mathbf{u} + a_1\mathbf{u}^{q^s} + \cdots + a_{k-1}\mathbf{u}^{q^{s(k-1)}}.$$

This implies that $u_0, u_1, \ldots, u_{k-1}$ are elements of $\ker f$, where $\mathbf{u} = (u_0, \ldots, u_{k-1})$. Also, they are $\mathbb{F}_q$-independent since $\mathcal{B} = (\mathbf{u}, \ldots, \mathbf{u}^{q^{s(k-1)}}) = (\phi(\mathbf{e}_0), \ldots, \phi(\mathbf{e}_{k-1}))$ is an ordered $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^n}^k$. This completes the proof. □

As a corollary we get the second part of [6, Theorem 10], see also [12, Lemma 3] for the case $s = 1$ and [11] for the case when q is a prime. Indeed, by evaluating the determinants in $AA^{q^s} \cdots A^{q^{s(n-1)}} = I_k$ we obtain the following corollary.[1]

Corollary 3.1. *If the kernel of a q^s-polynomial $f(x) = a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} - x^{q^{sk}}$ has dimension k, then $\mathrm{N}(a_0) = (-1)^{n(k+1)}$.*

Corollary 3.2. *Let A be a matrix as in Theorem 1.2. The condition*

$$AA^{q^s} \cdots A^{q^{s(n-1)}} = I_k$$

is satisfied if and only if $AA^{q^s} \cdots A^{q^{s(n-1)}}$ fixes $\mathbf{e}_0 = (1, 0, \ldots, 0)$.

Proof. The only if part is trivial, we prove the if part by induction on $0 \le i \le k-1$. Suppose $AA^{q^s} \cdots A^{q^{s(n-1)}}\mathbf{e}_i^T = \mathbf{e}_i^T$ for some $0 \le i \le k-1$. Then by taking q^s-th powers of each entry we get $A^{q^s}A^{q^{2s}} \cdots A\mathbf{e}_i^T = \mathbf{e}_i^T$. Since $A\mathbf{e}_i^T = \mathbf{e}_{i+1}^T$ this yields $A^{q^s}A^{q^{2s}} \cdots A^{q^{s(n-1)}}\mathbf{e}_{i+1}^T = \mathbf{e}_i^T$. Then multiplying both sides by A yields $AA^{q^s}A^{q^{2s}} \cdots A^{q^{s(n-1)}}\mathbf{e}_{i+1}^T = \mathbf{e}_{i+1}^T$. □

[1] For $x \in \mathbb{F}_{q^n}$ and for a subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$ we will denote by $\mathrm{N}_{q^n/q^m}(x)$ the norm of x over $\mathbb{F}_{q^m}$ and by $\mathrm{Tr}_{q^n/q^m}(x)$ we will denote the trace of x over $\mathbb{F}_{q^m}$. If n is clear from the context and $m = 1$ then we will simply write $\mathrm{N}(x)$ and $\mathrm{Tr}(x)$.

Consider a q^s-polynomial $f(x) = a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} - x^{q^{sk}}$, the matrix $A \in \mathbb{F}_{q^n}^{k\times k}$ as in Theorem 1.2 and the semilinear map τ defined in (6).

Note that

$$\begin{aligned}
\mathbf{e}_0^{\tau} &= (0,1,0,\ldots,0) = \mathbf{e}_1 \\
\mathbf{e}_0^{\tau^2} &= (0,0,1,\ldots,0) = \mathbf{e}_2 \\
&\vdots \\
\mathbf{e}_0^{\tau^{k-1}} &= (0,0,0,\ldots,1) = \mathbf{e}_{k-1} \\
\mathbf{e}_0^{\tau^k} &= (a_0,a_1,a_2,\ldots,a_{k-1}) \\
\mathbf{e}_0^{\tau^{k+1}} &= (a_0a_{k-1}^{q^s}, a_0^{q^s} + a_1a_{k-1}^{q^s}, a_1^{q^s} + a_2a_{k-1}^{q^s}, \ldots, a_{k-2}^{q^s} + a_{k-1}^{q^s+1}).
\end{aligned} \tag{8}$$

Hence, if

$$\mathbf{e}_0^{\tau^i} = (Q_{0,i}, Q_{1,i}, \ldots, Q_{k-1,i})$$

where $Q_{j,i}$ can be seen as polynomials in $a_0, a_1, \ldots, a_{k-1}$, for $i \geq 0$, then

$$\mathbf{e}_0^{\tau^{i+1}} = (a_0Q_{k-1,i}^{q^s}, Q_{0,i}^{q^s} + a_1Q_{k-1,i}^{q^s}, \ldots, Q_{k-2,i}^{q^s} + a_{k-1}Q_{k-1,i}^{q^s}),$$

i.e. the polynomials $Q_{j,i}$ for $0 \leq j \leq k-1$ can be defined by the following recursive relations for $0 \leq i \leq k-1$:

$$Q_{j,i} = \begin{cases} 1 & \text{if } j = i, \\ 0 & \text{otherwise,} \end{cases}$$

and by the following relations for $i \geq k$:

$$\begin{aligned}
Q_{0,i+1} &= a_0Q_{k-1,i}^{q^s} \\
Q_{j,i+1} &= Q_{j-1,i}^{q^s} + a_jQ_{k-1,i}^{q^s}.
\end{aligned} \tag{9}$$

Now, we are able to prove the following.

Theorem 3.3. *The kernel of a q^s-polynomial $f(x) = a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} - x^{q^{sk}} \in \mathbb{F}_{q^n}[x]$, where $\gcd(s,n) = 1$, has dimension k if and only if*

$$Q_{j,n}(a_0, a_1, \ldots, a_{k-1}) = \begin{cases} 1 & \text{if } j = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

Proof. Relations (9) can be written as follows

$$\begin{pmatrix} Q_{0,i+1} \\ Q_{1,i+1} \\ \vdots \\ Q_{k-1,i+1} \end{pmatrix} = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{k-1} \end{pmatrix} \begin{pmatrix} Q_{0,i}^{q^s} \\ Q_{1,i}^{q^s} \\ \vdots \\ Q_{k-1,i}^{q^s} \end{pmatrix},$$

with $i \in \{0, \ldots, n-1\}$. Also, $(Q_{0,0}, Q_{1,0}, \ldots, Q_{k-1,0}) = (1, 0, \ldots, 0)$ and $\mathbf{e}_0^{\tau^t} = (Q_{0,t}, \ldots, Q_{k-1,t})$ for $t \in \{0, \ldots, n\}$. By Theorem 1.2 and by Corollary 3.2, the kernel of $f(x)$ has dimension k if and only if $\mathbf{e}_0 = (Q_{0,0}, Q_{1,0}, \ldots, Q_{k-1,0})$ is fixed by $AA^{q^s} \cdots A^{q^{s(n-1)}}$, so this happens if and only if

$$\mathbf{e}_0^{\tau^n} = (Q_{0,n}, Q_{1,n}, \ldots, Q_{k-1,n}) = (1, 0, \ldots, 0).$$

□

Theorem 3.3 with $k = n-1$ and $s = 1$ gives the following well-known result as a corollary.

Corollary 3.4. *[10, Theorem 2.24] The dimension of the kernel of a q-polynomial $f(x) \in \mathbb{F}_{q^n}[x]$ is $n-1$ if and only if there exist $\alpha, \beta \in \mathbb{F}_{q^n}^*$ such that*

$$f(x) = \alpha \operatorname{Tr}(\beta x).$$

Again from Theorem 3.3 we can deduce the following.

Corollary 3.5. *[10, Ex. 2.14] The q^s-polynomial $a_0x - x^{q^{sk}} \in \mathbb{F}_{q^n}[x]$, with* $\gcd(s, n) = 1$ *and $1 \le k \le n-1$, admits q^k roots if and only if $k \mid n$ and* $\mathrm{N}_{q^n/q^k}(a_0) = 1$.

3.1 When the q^s-degree equals $n-2$

In this section we investigate q^s-polynomials

$$f(x) = a_0x + a_1x^{q^s} + \cdots + a_{n-3}x^{q^{s(n-3)}} - x^{q^{s(n-2)}}$$

with $\gcd(s, n) = 1$. By Theorem 3.3, $\dim\ker f(x) = n-2$ if and only if $a_0, a_1, \ldots, a_{n-3}$ satisfy the following system of equations

$$\begin{cases} Q_{0,n} = a_0(a_{n-4}^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 1, \\ Q_{1,n} = a_0^{q^s} a_{n-3}^{q^{2s}} + a_1(a_{n-4}^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 0, \\ Q_{2,n} = a_0^{q^{2s}} + a_{n-3}^{q^{2s}} a_1^{q^s} + a_2(a_{n-4}^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 0, \\ Q_{3,n} = a_1^{q^{2s}} + a_{n-3}^{q^{2s}} a_2^{q^s} + a_3(a_{n-4}^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 0, \\ \vdots \\ Q_{n-3,n} = a_{n-5}^{q^{2s}} + a_{n-3}^{q^{2s}} a_{n-4}^{q^s} + a_{n-3}(a_{n-4}^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 0, \end{cases} \tag{11}$$

which is equivalent to

$$\begin{cases} a_0(a_{n-4}^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 1, \\ a_1 = -a_0^{q^s+1} a_{n-3}^{q^{2s}} =: g_1(a_0, a_{n-3}), \\ a_j = -a_{j-2}^{q^{2s}} a_0 - a_{n-3}^{q^{2s}} a_{j-1}^{q^s} a_0 =: g_j(a_0, a_{n-3}), \text{ for } 2 \leq j \leq n-3. \end{cases} \tag{12}$$

So, $\dim_{\mathbb{F}_q} \ker f(x) = n-2$ if and only if a_0 and a_{n-3} satisfy the equations

$$\begin{cases} a_0(g_{n-4}(a_0, a_{n-3})^{q^{2s}} + a_{n-3}^{q^{2s}+q^s}) = 1, \\ a_{n-3} = g_{n-3}(a_0, a_{n-3}), \end{cases}$$

and $a_j = g_j(a_0, a_{n-3})$ for $j \in \{1, \ldots, n-4\}$.

Theorem 3.6. *Suppose that $f(x) = a_0x + a_1x^q + \cdots + a_{n-3}x^{q^{n-3}} - x^{q^{n-2}}$ has maximum kernel. Then for $t \geq 2$ with $\gcd(t-1, n) = 1$ the coefficients a_{t-2} and a_{n-t} are non-zero and, with $s = n - t + 1$,*

$$a_{n-2t+1} a_{t-2}^{q^{2s}+q^s} = -a_{n-t}^{q^s+1} a_{2t-3}^{q^{2s}}. \tag{13}$$

Also, it holds that

$$-a_{n-t}(-a_{t-2}^{q^s} a_{3t-4}^{q^{2s}} + a_{2t-3}^{q^{2s}+q^s}) = a_{t-2}^{q^{2s}+q^s+1}. \tag{14}$$

In particular, for $t \geq 2$ with $\gcd(t-1, n) = 1$ we get

$$\mathrm{N}(a_{n-t}) = (-1)^n \, \mathrm{N}(a_{t-2}) \tag{15}$$

and

$$\mathrm{N}(a_{n-2t+1}) = (-1)^n \, \mathrm{N}(a_{2t-3}), \tag{16}$$

where $n - 2t + 1$ and $2t - 3$ are considered modulo n.

Proof. Let $t \geq 2$ with $\gcd(t-1,n)=1$ and consider the polynomial $F(x) = f(x^{q^t})$, that is,

$$F(x) = a_0 x^{q^t} + a_1 x^{q^{t+1}} + \cdots + a_{n-3} x^{q^{n+t-3}} - x^{q^{n+t-2}}.$$

Clearly $\dim_{\mathbb{F}_q} \ker F = \dim_{\mathbb{F}_q} \ker f = n-2$. By renaming the coefficients, $F(x)$ can be written as

$$\begin{aligned} F(x) &= \alpha_0 x + \alpha_1 x^{q^{n-t+1}} + \alpha_2 x^{q^{2(n-t+1)}} + \cdots + \alpha_{n-3} x^{q^{(n-t+1)(n-3)}} + \alpha_{n-2} x^{q^{(n-t+1)(n-2)}} \\ &= \alpha_0 x + \alpha_1 x^{q^{n-t+1}} + \cdots + \alpha_{n-3} x^{q^{3t-3}} + \alpha_{n-2} x^{q^{2t-2}}. \end{aligned}$$

Since $F(x)$ has maximum kernel, by the second equation of (12) we get $\alpha_0 \neq 0$, $\alpha_{n-2} \neq 0$ and the following relation

$$-\frac{\alpha_1}{\alpha_{n-2}} = -\left(-\frac{\alpha_0}{\alpha_{n-2}}\right)^{q^s+1} \left(-\frac{\alpha_{n-3}}{\alpha_{n-2}}\right)^{q^{2s}}. \tag{17}$$

The coefficient α_j of $F(x)$ equals the coefficient a_i of $f(x)$ with $i \equiv n-t+j(1-t) \pmod{n}$, in particular

$$\begin{cases} \alpha_0 = a_{n-t}, \\ \alpha_1 = a_{n-2t+1}, \\ \alpha_{n-3} = a_{2t-3}, \\ \alpha_{n-2} = a_{t-2}, \\ \alpha_{n-4} = a_{3t-4}, \end{cases} \tag{18}$$

and by (17), we get that a_{t-2} and a_{n-t} are nonzero, and

$$a_{n-2t+1} a_{t-2}^{q^{2s}+q^s} = -a_{n-t}^{q^s+1} a_{2t-3}^{q^{2s}},$$

which gives (13). The first equation of (12) gives

$$-\frac{\alpha_0}{\alpha_{n-2}} \left(\left(-\frac{\alpha_{n-4}}{\alpha_{n-2}}\right)^{q^{2s}} + \left(-\frac{\alpha_{n-3}}{\alpha_{n-2}}\right)^{q^{2s}+q^s} \right) = 1,$$

that is,

$$-\alpha_0(-\alpha_{n-2}^{q^s} \alpha_{n-4}^{q^{2s}} + \alpha_{n-3}^{q^{2s}+q^s}) = \alpha_{n-2}^{q^{2s}+q^s+1}.$$

Then (18) and $\alpha_{n-4} = a_{3t-4}$ imply

$$-a_{n-t}(-a_{t-2}^{q^s} a_{3t-4}^{q^{2s}} + a_{2t-3}^{q^{2s}+q^s}) = a_{t-2}^{q^{2s}+q^s+1},$$

which gives (14). By Corollary 3.1 with $s = n - t + 1$ we obtain

$$\mathrm{N}\left(-\frac{\alpha_0}{\alpha_{n-2}}\right) = 1,$$

and taking (18) into account we get

$$\mathrm{N}(a_{n-t}) = (-1)^n\,\mathrm{N}(a_{t-2}).$$

Then (13) and the previous relation yield

$$\mathrm{N}(a_{n-2t+1}) = (-1)^n\,\mathrm{N}(a_{2t-3}).$$

□

Proposition 3.7. *Let $f(x)$ be a q^s-polynomial with q^s-degree $n-2$ and with maximum kernel. If the coefficient of x^{q^s} is zero, then n is even and $f(x) = \alpha\,\mathrm{Tr}_{q^n/q^2}(\beta x)$ for some $\alpha, \beta \in \mathbb{F}^*_{q^n}$.*

Proof. We may assume $f(x) = a_0x + a_1x^{q^s} + \cdots + a_{n-3}x^{q^{s(n-3)}} - x^{q^{s(n-2)}}$ with $a_1 = 0$. By the second equation of (12), it follows that $a_{n-3} = 0$. By the third equation of (12), we get that $a_j = 0$ for every odd integer $j \in \{3, \ldots, n-3\}$. If j is even then we have

$$a_j = (-1)^{\frac{j}{2}} a_0^{q^{sj}+q^{s(j-2)}+\cdots+q^{2s}+1}. \tag{19}$$

If $n-3$ is even, then this gives us a contradiction with $j = n-3$. It follows that $n-3$ is odd and hence n is even. By $\mathrm{N}(a_0) = (-1)^n$, there exists $\lambda \in \mathbb{F}^*_{q^n}$ such that $a_0 = -\lambda^{1-q^{s(n-2)}}$. So, by (19) we get $a_j = \lambda^{q^{js}-q^{s(n-2)}}$, and hence

$$f(x) = \frac{\mathrm{Tr}_{q^n/q^2}(\lambda x)}{\lambda^{q^{s(n-2)}}}.$$

□

In the next sections we list all the q^s-polynomials of $\mathbb{F}_{q^n}$ with maximum kernel for $n \le 6$. By Corollaries 3.4 and 3.5 the $n \le 3$ case can be easily described hence we will consider only the $n \in \{4, 5, 6\}$ cases.

For $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \tilde{\mathcal{L}}_{n,q}$ we denote by $\hat{f}(x) := \sum_{i=0}^{n-1} a_i^{q^{n-i}} x^{q^{n-i}}$ the adjoint (w.r.t. the symmetric non-degenerate bilinear form defined by $\langle x, y\rangle = \mathrm{Tr}(xy)$) of f.

By [1, Lemma 2.6], see also [2, pages 407–408], the kernel of f and $\hat{f}$ has the same dimension and hence the following result holds.

Proposition 3.8. *If $f(x) \in \tilde{\mathcal{L}}_{n,q}$ is a q^s-polynomial with maximum kernel, then $\hat{f}(x)$ is a q^{n-s}-polynomial with maximum kernel.*

This will allow us to consider only the $s \leq n/2$ case.

3.2 The $n = 4$ case

In this section we determine the linearized polynomials over $\mathbb{F}_{q^4}$ with maximum kernel. Without loss of generality, we can suppose that the leading coefficient of the polynomial is -1.

Because of Proposition 3.8, we can assume $s = 1$. Corollaries 3.4 and 3.5 cover the cases when the q-degree of f is 1 or 3 so from now on we suppose $f(x) = a_0x + a_1x^q - x^{q^2}$. If $a_1 = 0$ then we can use again Corollary 3.5 and we get $a_0x - x^{q^2}$, with $\mathrm{N}_{q^4/q^2}(a_0) = 1$. Suppose $a_1 \neq 0$. By Equation (12), we get the conditions

$$\begin{cases} a_0(a_0^{q^2} + a_1^{q^2+q}) = 1, \\ a_1 = -a_0^{q+1}a_1^{q^2}, \end{cases}$$

which is equivalent to

$$\begin{cases} \mathrm{N}_{q^4/q}(a_0) = 1, \\ a_1^{q+1} = a_0^{q^2+q+1} - a_0^q, \end{cases}$$

see (A1) of Section 5.

Here we list the q-polynomials of $\mathcal{L}_{4,q}$ with maximum kernel, up to a non-zero scalar in $\mathbb{F}_{q^4}^*$. Applying the adjoint operation we can obtain the list of q^3-polynomials over $\mathbb{F}_{q^4}$ with maximum kernel. In the following table the q-degree will be denoted by k.

k	polynomial form	conditions
3	$\mathrm{Tr}(\lambda x)$	$\lambda \in \mathbb{F}_{q^4}^*$
2	$a_0x - x^{q^2}$	$\mathrm{N}_{q^4/q^2}(a_0) = 1$
2	$a_0x + a_1x^q - x^{q^2}$	$\begin{cases} \mathrm{N}_{q^4/q}(a_0) = 1 \\ a_1^{q+1} = a_0^{q^2+q+1} - a_0^q \end{cases}$
1	$a_0x - x^q$	$\mathrm{N}_{q^4/q}(a_0) = 1$

Table 1: Linearized polynomials of $\mathbb{F}_{q^4}$ with maximum kernel with $s = 1$

3.3 The $n = 5$ case

In this section we determine the linearized polynomials over $\mathbb{F}_{q^5}$ with maximum kernel. Without loss of generality, we can suppose that the leading coefficient of the polynomial is -1. Because of Proposition 3.8, we can assume $s \in \{1, 2\}$. Corollaries 3.4 and 3.5 cover the cases when the q^s-degree of f is 1 or 4. First we suppose that f has q^s-degree 3, i.e.

$$f(x) = a_0 x + a_1 x^{q^s} + a_2 x^{q^{2s}} - x^{q^{3s}}.$$

From (12), $f(x)$ has maximum kernel if and only if a_0, a_1 and a_2 satisfy the following system:

$$\begin{cases} a_1 = -a_0^{q^s+1} a_2^{q^{2s}}, \\ -a_0^{q^{3s}+q^{2s}+1} a_2^{q^{4s}} + a_2^{q^{2s}+q^s} a_0 = 1, \\ a_2 = -a_0^{q^{2s}+1} + a_2^{q^{3s}+q^{2s}} a_0^{q^{2s}+q^s+1}, \end{cases}$$

which is equivalent to

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_1 = -a_0^{q^s+1} a_2^{q^{2s}}, \\ -a_0^{q^{3s}+q^{2s}+1} a_2^{q^{4s}} + a_0 a_2^{q^{2s}+q^s} = 1, \end{cases}$$

see (A2) of Section 5.

Suppose now that the q^s-degree is 2, i.e.

$$f(x) = a_0 x + a_1 x^{q^s} - x^{q^{2s}}.$$

By Theorem 3.3 the polynomial $f(x)$ has maximum kernel if and only if its coefficients satisfy

$$\begin{cases} a_0 (a_0^{q^{2s}} a_1^{q^{3s}} + a_1^{q^s} (a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}})) = 1, \\ a_0^{q^s+1} (a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}}) + a_1 = 0, \end{cases}$$

which is equivalent to

$$\begin{cases} \mathrm{N}(a_0) = -1, \\ a_0^{q^s} + a_1^{q^s+1} = a_0^{q^{2s}+q^s+1} a_1^{q^{3s}}, \end{cases}$$

see (A3) of Section 5.

Here we list the q^s-polynomials, $s \in \{1, 2\}$ of $\mathcal{L}_{5,q}$ with maximum kernel, up to a non-zero scalar in $\mathbb{F}_{q^5}^*$. Applying the adjoint operation we can obtain the list of q^t-polynomials, $t \in \{3, 4\}$, over $\mathbb{F}_{q^5}$ with maximum kernel. As before, the q^s-degree is denoted by k.

k	polynomial form	conditions
4	$\mathrm{Tr}(\lambda x)$	$\lambda \in \mathbb{F}_{q^5}^*$
3	$a_0x + a_1x^{q^s} + a_2x^{q^{2s}} - x^{q^{3s}}$	$\begin{cases} \mathrm{N}(a_0) = 1 \\ a_1 = -a_0^{q^s+1}a_2^{q^{2s}} \\ -a_0^{q^{3s}+q^{2s}+1}a_2^{q^{4s}} + a_0a_2^{q^{2s}+q^s} = 1 \end{cases}$
2	$a_0x + a_1x^{q^s} - x^{q^{2s}}$	$\begin{cases} \mathrm{N}(a_0) = -1 \\ a_1^{q^s+1} + a_0^{q^s} = a_1^{q^{3s}}a_0^{q^{2s}+q^s+1} \end{cases}$
1	$a_0x - x^{q^s}$	$\mathrm{N}(a_0) = 1$

Table 2: Linearized polynomials of $\mathbb{F}_{q^5}$ with maximum kernel with $s \in \{1, 2\}$

3.4 The $n = 6$ case

In this section we determine the linearized polynomials over $\mathbb{F}_{q^6}$ with maximum kernel. Without loss of generality, we can suppose that the leading coefficient of the polynomial is -1. Because of Proposition 3.8, we can assume $s = 1$. Corollaries 3.4 and 3.5 cover the cases when the q-degree of f is 1 or 5. As before, denote by k the q^s-degree of f.

We first consider the case $k = 2$, i.e. $f(x) = a_0x + a_1x^{q^s} - x^{q^{2s}}$. By Theorem 3.3, $f(x)$ has maximum kernel if and only if the coefficients satisfy

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ (a_0^q + a_1^{q+1})^{q^3} = a_0^{q^5+q^4+q^3}(a_0^q + a_1^{q+1}), \\ a_1^{q^4}a_0^{q^3} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) = -\frac{a_1}{a_0^{q+1}}, \end{cases}$$

see (A4) of Section 5.

If $k = 3$, then $f(x) = a_0x + a_1x^{q^s} + a_2x^{q^{2s}} - x^{q^{3s}}$, and by Theorem 3.3 it has maximum kernel if and only the coefficients fulfill

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0^{q^3+q+1} + a_2^{q^3}a_1^{q^2}a_0^{q+1} - a_2^q a_1 = a_0^q, \\ a_2^{q+1} = -a_0^{q^3+q^2+q+1}a_1^{q^4} - a_1^q, \\ a_1^{q+1} = a_2a_0^q + a_0^{q^2+q+1}a_2^{q^3}, \end{cases}$$

see (A5) of Section 5. Note that $a_1 = 0$ if and only if $a_2 = 0$ and in this case we get the trace over $\mathbb{F}_{q^3}$.

Finally, let $k = 4$. Then the polynomial $f(x) = a_0x + a_1x^{q^s} + a_2x^{q^{2s}} + a_3x^{q^{3s}} - x^{q^{4s}}$ has maximum kernel if and only if the coefficients satisfy

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0(-a_0^{q^4+q^2} + a_3^{q^5+q^4}a_0^{q^4+q^3+q^2} + a_3^{q^2+q}) = 1, \\ a_1 = -a_0^{q+1}a_3^{q^2}, \\ a_2 = -a_0^{q^2+1} + a_3^{q^3+q^2}a_0^{q^2+q+1}, \\ a_3 = a_3^{q^4}a_0^{q^3+q^2+1} + a_3^{q^2}a_0^{q^3+q+1} - a_0^{q^3+q^2+q+1}a_3^{q^4+q^3+q^2}, \end{cases}$$

see (A6) of Section 5.

Here we list the q-polynomials of $\mathcal{L}_{6,q}$ with maximum kernel, up to a non-zero scalar in $\mathbb{F}_{q^6}^*$. Applying the adjoint operation we can obtain the list of q^5-polynomials over $\mathbb{F}_{q^6}$ with maximum kernel.

Table 3: Linearized polynomials of $\mathbb{F}_{q^6}$ with maximum kernel with $s = 1$

k	polynomial form	conditions
5	$\mathrm{Tr}_{q^6/q}(\lambda x)$	$\lambda \in \mathbb{F}_{q^6}^*$
4	$a_0x + a_1x^q + a_2x^{q^2} + a_3x^{q^3} - x^{q^4}$	$\begin{cases} a_1 \neq 0 \\ \mathrm{N}(a_0) = 1 \\ a_0(-a_0^{q^4+q^2} + a_3^{q^5+q^4} a_0^{q^4+q^3+q^2} + a_3^{q^2+q}) = 1 \\ a_1 = -a_0^{q+1} a_3^{q^2} \\ a_2 = -a_0^{q^2+1} + a_3^{q^3+q^2} a_0^{q^2+q+1} \\ a_3 = a_3^{q^4} a_0^{q^3+q^2+1} + a_3^{q^2} a_0^{q^3+q+1} - a_0^{q^3+q^2+q+1} a_3^{q^4+q^3+q^2} \end{cases}$
4	$\mathrm{Tr}_{q^6/q^2}(\lambda x)$	$\lambda \in \mathbb{F}_{q^6}^*$
3	$a_0x + a_1x^q + a_2x^{q^2} - x^{q^3}$	$\begin{cases} \mathrm{N}(a_0) = 1 \\ a_0^{q^3+q+1} + a_2^{q^3} a_1^{q^2} a_0^{q+1} - a_2^q a_1 = a_0^q \\ a_2^{q+1} = -a_0^{q^3+q^2+q+1} a_1^{q^4} - a_1^q \\ a_1^{q+1} = a_2 a_0^q + a_0^{q^2+q+1} a_2^{q^3} \end{cases}$
3	$\mathrm{Tr}_{q^6/q^3}(\lambda x)$	$\lambda \in \mathbb{F}_{q^6}^*$
2	$a_0x + a_1x^q - x^{q^2}$	$\begin{cases} a_1 \neq 0 \\ \mathrm{N}(a_0) = 1 \\ (a_0^q + a_1^{q+1})^{q^3} = a_0^{q^5+q^4+q^3}(a_0^q + a_1^{q+1}) \\ a_1^{q^4} a_0^{q^3} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) = -\frac{a_1}{a_0^{q+1}} \end{cases}$
2	$a_0x - x^{q^2}$	$\mathrm{N}_{q^6/q^2}(a_0) = 1$
1	$a_0x - x^q$	$\mathrm{N}_{q^6/q}(a_0) = 1$

4 Application

As an application of Theorem 1.2 we are able to prove the following result on the splitting field of q-polynomials.

Theorem 4.1. *Let $f(x) = a_0 x + a_1 x^q + \cdots + a_{k-1} x^{q^{k-1}} - x^{q^k} \in \mathbb{F}_{q^n}[x]$ with $a_0 \neq 0$ and let A be defined as in (1). Then the splitting field of $f(x)$ is $\mathbb{F}_{q^{nm}}$ where m is the (multiplicative) order of the matrix $B := AA^q \cdots A^{q^{n-1}}$.*

Proof. The derivative of $f(x)$ is non-zero and hence $f(x)$ has q^k distinct roots in some algebraic extension of $\mathbb{F}_{q^n}$. Suppose that $\mathbb{F}_{q^{nm}}$ is the splitting field of $f(x)$ and let t denote the order of B. Then the kernel of the $\mathbb{F}_q$-linear $\mathbb{F}_{q^{nm}} \to \mathbb{F}_{q^{nm}}$ map defined as $x \mapsto f(x)$ has dimension k over $\mathbb{F}_q$ and hence by Theorem 1.2 we have

$$AA^q \cdots A^{q^{nm-1}} = I_k.$$

Since the coefficients of A are in $\mathbb{F}_{q^n}$, this is equivalent to $B^m = I_k$ and hence $t \mid m$. On the other hand

$$B^t = AA^q \cdots A^{q^{nt-1}} = I_k$$

and hence again by Theorem 1.2 the kernel of the $\mathbb{F}_q$-linear $\mathbb{F}_{q^{nt}} \to \mathbb{F}_{q^{nt}}$ map defined as $x \mapsto f(x)$ has dimension k over $\mathbb{F}_q$. It follows that $\mathbb{F}_{q^{nm}}$ is a subfield of $\mathbb{F}_{q^{nt}}$ from which $m \mid t$. □

A further application of Theorem 1.2 is the following.

Theorem 4.2. *Let n, m, s and t be positive integers such that $\gcd(s, nm) = \gcd(t, nm) = 1$ and $s \equiv t \pmod{m}$. Let $f(x) = a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{s(k-1)}} - x^{q^{sk}}$ and $g(x) = a_0 x + a_1 x^{q^t} + \cdots + a_{k-1} x^{q^{t(k-1)}} - x^{q^{tk}}$, where $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^m}$. The kernel of $f(x)$ considered as a linear transformation of $\mathbb{F}_{q^{nm}}$ has dimension k if and only if the kernel of $g(x)$ considered as a linear transformation of $\mathbb{F}_{q^{nm}}$ has dimension k.*

Proof. Denote by A the matrix associated with $f(x)$ as in (1). By hypothesis, $A \in \mathbb{F}_{q^m}^{k \times k}$ and it is the same as the matrix associated with $g(x)$. By Theorem 1.2 the kernel of $f(x)$, considered as a linear transformation of $\mathbb{F}_{q^{nm}}$, has dimension k if and only if

$$AA^{q^s} \cdots A^{q^{s(nm-1)}} = I_k.$$

Since $s \equiv t \pmod{m}$, we have

$$AA^{q^s} \cdots A^{q^{s(nm-1)}} = AA^{q^t} \cdots A^{q^{t(nm-1)}} = I_k,$$

and, again by Theorem 1.2, this holds if and only if the kernel of $g(x)$, considered as a linear transformation of $\mathbb{F}_{q^{nm}}$, has dimension k. $\square$

Addendum

During the "Combinatorics 2018" conference, the fourth author presented the results of this paper in the talk entitled "On q-polynomials with maximum kernel". In the same conference John Sheekey presented a joint work with Gary McGuire [8] in his talk entitled "Ranks of Linearized Polynomials and Roots of Projective Polynomials". It turned out that, independently from the authors of the present paper, they also obtained similar results.

5 Appendix

In this section we develop some calculations regarding the relations on the coefficients of a linearized polynomials with maximum kernel presented in Sections 3.2, 3.3 and 3.4, see also [13].

(A1) By Equation (11) with $n = 4$, $s = 1$ and $k = 2$, we get the conditions

$$\Sigma\colon \begin{cases} a_0(a_0^{q^2} + a_1^{q^2+q}) = 1, \\ a_1 = -a_0^{q+1}a_1^{q^2}. \end{cases}$$

By Corollary 3.1, the system Σ is equivalent to the following system

$$\Sigma'\colon \begin{cases} \mathrm{N}_{q^4/q}(a_0) = 1, \\ a_0(a_0^{q^2} + a_1^{q^2+q}) = 1, \\ a_1 = -a_0^{q+1}a_1^{q^2}, \end{cases}$$

which can be rewritten as follows

$$\Sigma'\colon \begin{cases} \mathrm{N}_{q^4/q}(a_0) = 1, \\ a_1^{q^2-1} = -\frac{1}{a_0^{q+1}}, \\ a_1^{q+1} = a_0^{q^2+q+1} - a_0^q. \end{cases}$$

Now consider the system

$$\Sigma^*\colon \begin{cases} \mathrm{N}_{q^4/q}(a_0) = 1, \\ a_1^{q+1} = a_0^{q^2+q+1} - a_0^q. \end{cases}$$

Clearly, $S(\Sigma') \subseteq S(\Sigma^*)$, where $S(\Sigma')$ and $S(\Sigma^*)$ denote the set of solutions of Σ' and Σ^*, respectively. Let $(a_0, a_1) \in S(\Sigma^*)$, then by using the norm condition on a_0

$$a_1^{q^2-1} = \left(\frac{1}{a_0^{q^3}} - a_0^q\right)^{q-1} = \left(\frac{1 - a_0^{q+q^3}}{a_0^{q^3}}\right)^{q-1} =$$

$$= \frac{1 - a_0^{1+q^2}}{1 - a_0^{q+q^3}}a_0^{q^3-1} = \frac{1 - \frac{1}{a_0^{q+q^3}}}{1 - a_0^{q+q^3}}a_0^{q^3-1} = -\frac{1}{a_0^{q+1}},$$

i.e. $(a_0, a_1) \in S(\Sigma')$ and hence $S(\Sigma^*) = S(\Sigma') = S(\Sigma)$.

(A2) From (11) with $n = 5$, $\gcd(s, 5) = 1$ and $k = 3$, we get the following conditions:

$$\Sigma\colon \begin{cases} a_0(a_1^{q^{2s}} + a_2^{q^{2s}+q^s}) = 1, \\ a_1 = -a_0^{q^s+1} a_2^{q^{2s}}, \\ a_2 = -a_0^{q^{2s}+1} - a_2^{q^{2s}} a_1^{q^s} a_0. \end{cases}$$

By Corollary 3.1, Σ is equivalent to

$$\Sigma'\colon \begin{cases} \mathrm{N}_{q^5/q}(a_0) = 1, \\ a_0(a_1^{q^{2s}} + a_2^{q^{2s}+q^s}) = 1, \\ a_1 = -a_0^{q^s+1} a_2^{q^{2s}}, \\ a_2 = -a_0^{q^{2s}+1} - a_2^{q^{2s}} a_1^{q^s} a_0. \end{cases}$$

which can be rewritten as follows

$$\Sigma'\colon \begin{cases} \mathrm{N}_{q^5/q}(a_0) = 1, \\ a_1 = -a_0^{q^s+1} a_2^{q^{2s}}, \\ -a_0^{q^{3s}+q^{2s}+1} a_2^{q^{4s}} + a_2^{q^{2s}+q^s} a_0 = 1, \\ a_2 = -a_0^{q^{2s}+1} + a_2^{q^{3s}+q^{2s}} a_0^{q^{2s}+q^s+1}. \end{cases}$$

By raising the third equation to q^s and multiplying by $a_0^{q^{2s}+1}$, since $\mathrm{N}(a_0) = 1$, we get the fourth equation. Therefore Σ', and hence Σ, is equivalent to

$$\begin{cases} \mathrm{N}_{q^5/q}(a_0) = 1, \\ a_1 = -a_0^{q^s+1} a_2^{q^{2s}}, \\ -a_0^{q^{3s}+q^{2s}+1} a_2^{q^{4s}} + a_0 a_2^{q^{2s}+q^s} = 1. \end{cases}$$

(A3) Applying Theorem 3.3 with $n = 5$ and $k = 2$, we get that the polynomial $f(x)$ has maximum kernel if and only if its coefficients satisfy

$$\Sigma\colon \begin{cases} Q_{0,5} = a_0(a_0^{q^{2s}} a_1^{q^{3s}} + a_1^{q^s}(a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}})) = 1, \\ Q_{1,5} = a_0^{q^s}(a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}}) + a_1(a_0^{q^{2s}} a_1^{q^{3s}} + a_1^{q^s}(a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}})) = 0, \end{cases}$$

which is equivalent to

$$\begin{cases} \mathrm{N}_{q^5/q}(a_0) = -1, \\ a_0(a_0^{q^{2s}} a_1^{q^{3s}} + a_1^{q^s}(a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}})) = 1, \\ a_0^{q^s+1}(a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}}) + a_1 = 0, \end{cases}$$

because of Corollary 3.1 and since $a_0^{q^{2s}} a_1^{q^{3s}} + a_1^{q^s}(a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}}) = \dfrac{1}{a_0}$. The above system can be rewritten as follows

$$\begin{cases} \mathrm{N}_{q^5/q}(a_0) = -1, \\ a_0^{q^{3s}} + a_1^{q^{3s}+q^{2s}} = -\frac{a_1}{a_0^{q^s+1}}, \\ a_1^{q^{3s}} a_0^{q^{2s}+q^s+1} - a_1^{q^s+1} = a_0^{q^s}, \end{cases}$$

which is equivalent to

$$\begin{cases} \mathrm{N}_{q^5/q}(a_0) = -1, \\ a_1^{q^s+1} + a_0^{q^s} = a_1^{q^{3s}} a_0^{q^{2s}+q^s+1}, \\ a_1 a_0^{q^{4s}+q^{3s}+q^{2s}} = -\frac{a_1}{a_0^{q^s+1}}. \end{cases}$$

If the first and the second equations are satisfied, clearly also the last one is fulfilled, hence Σ is equivalent to the following system

$$\begin{cases} \mathrm{N}_{q^5/q}(a_0) = -1, \\ a_1^{q^s+1} + a_0^{q^s} = a_1^{q^{3s}} a_0^{q^{2s}+q^s+1}. \end{cases}$$

(A4) By Theorem 3.3, with $n = 6$, $s = 1$ and $k = 2$, we get

$$\begin{cases} Q_{0,6} = a_0(a_0^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) + a_1^q(a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}))) = 1, \\ Q_{1,6} = a_0^{q^2} a_1(a_0^{q^4} + a_1^{q^4+q^3}) + (a_1^{q+1} + a_0^q)(a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3})) = 0, \end{cases}$$

which is equivalent to

$$\begin{cases} a_0^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) + a_1^q(a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3})) = \frac{1}{a_0}, \\ \frac{a_1}{a_0} + a_0^q(a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3})) = 0, \end{cases}$$

i.e.

$$\begin{cases} a_0^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) + a_1^q(a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3})) = \frac{1}{a_0}, \\ a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) = -\frac{a_1}{a_0^{q+1}}. \end{cases}$$

By Corollary 3.1, the previous system is equivalent to

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) + a_1^q(a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3})) = \frac{1}{a_0}, \\ a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) = -\frac{a_1}{a_0^{q+1}}, \end{cases}$$

which is equivalent to

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0^{q^2}(a_0^q + a_1^{q+1})^{q^3} - \frac{a_1^{q+1}}{a_0^{q+1}} = \frac{1}{a_0}, \\ a_0^{q^3} a_1^{q^4} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) = -\frac{a_1}{a_0^{q+1}}, \end{cases}$$

hence it is equivalent to

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ (a_0^q + a_1^{q+1})^{q^3} = a_0^{q^5+q^4+q^3}(a_0^q + a_1^{q+1}), \\ a_1^{q^4} a_0^{q^3} + a_1^{q^2}(a_0^{q^4} + a_1^{q^4+q^3}) = -\frac{a_1}{a_0^{q+1}}. \end{cases}$$

(A5) By Theorem 3.3 with $n = 6$, $s = 1$ and $k = 3$, we get

$$\begin{cases} a_0 Q_{2,5}^q = 1, \\ Q_{0,5}^q + a_1 Q_{2,5}^q = 0, \\ Q_{1,5}^q + a_2 Q_{2,5}^q = 0, \end{cases}$$

where

$$\begin{aligned} Q_{0,5} &= a_0(a_1^{q^2} + a_2^{q^2+q}), \\ Q_{1,5} &= a_0^q a_2^{q^2} + a_1(a_1^{q^2} + a_2^{q^2+q}), \\ Q_{2,5} &= a_0^{q^2} + a_2^{q^2} a_1^q + a_2(a_1^{q^2} + a_2^{q^2+q}), \end{aligned}$$

hence we obtain the following system

$$\begin{cases} a_0(a_0^{q^3} + a_2^{q^3} a_1^{q^2} + a_2^q(a_1^{q^3} + a_2^{q^3+q^2})) = 1, \\ \frac{a_1}{a_0} + a_0^q(a_1^{q^3} + a_2^{q^3+q^2}) = 0, \\ \frac{a_2}{a_0} + a_2^{q^3} a_0^{q^2} + a_1^q(a_1^{q^3} + a_2^{q^3+q^2}) = 0. \end{cases}$$

By Corollary 3.1 it is equivalent to

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0(a_0^{q^3} + a_2^{q^3} a_1^{q^2} + a_2^q(a_1^{q^3} + a_2^{q^3+q^2})) = 1, \\ a_1^{q^3} + a_2^{q^3+q^2} = -\frac{a_1}{a_0^{1+q}}, \\ \frac{a_2}{a_0} + a_2^{q^3} a_0^{q^2} + a_1^q(a_1^{q^3} + a_2^{q^3+q^2}) = 0, \end{cases}$$

by substituting the third equation into the others we get

$$\begin{cases} \mathrm{N}(a_0)=1,\\ a_0(a_0^{q^3}+a_2^{q^3}a_1^{q^2}-\frac{a_2^q a_1}{a_0^{1+q}})=1,\\ a_1^{q^3}+a_2^{q^3+q^2}=-\frac{a_1}{a_0^{1+q}},\\ \frac{a_2}{a_0}+a_2^{q^3}a_0^{q^2}-\frac{a_1^{q+1}}{a_0^{1+q}}=0, \end{cases}$$

i.e.

$$\begin{cases} \mathrm{N}(a_0)=1,\\ a_0^{q^3+q+1}+a_2^{q^3}a_1^{q^2}a_0^{q+1}-a_2^q a_1=a_0^q,\\ a_2^{q+1}=-a_0^{q^3+q^2+q+1}a_1^{q^4}-a_1^q,\\ a_1^{q+1}=a_2a_0^q+a_0^{q^2+q+1}a_2^{q^3}. \end{cases}$$

(A6) Equations (11) with $n=6$, $s=1$ and $k=4$ are

$$\begin{cases} a_0(a_2^{q^2}+a_3^{q^2+q})=1,\\ a_0^q a_3^{q^2}+a_1(a_2^{q^2}+a_3^{q^2+q})=0,\\ a_0^{q^2}+a_3^{q^2}a_1^q+a_2(a_2^{q^2}+a_3^{q^2+q})=0,\\ a_1^{q^2}+a_3^{q^2}a_2^q+a_3(a_2^{q^2}+a_3^{q^2+q})=0, \end{cases}$$

which, by Corollary 3.1, is equivalent to

$$\begin{cases} \mathrm{N}(a_0)=1,\\ a_0(a_2^{q^2}+a_3^{q^2+q})=1,\\ a_0^q a_3^{q^2}+a_1(a_2^{q^2}+a_3^{q^2+q})=0,\\ a_0^{q^2}+a_3^{q^2}a_1^q+a_2(a_2^{q^2}+a_3^{q^2+q})=0,\\ a_1^{q^2}+a_3^{q^2}a_2^q+a_3(a_2^{q^2}+a_3^{q^2+q})=0, \end{cases}$$

thus it can be rewritten as follows

$$\begin{cases} \mathrm{N}(a_0)=1,\\ a_2^{q^2}+a_3^{q^2+q}=\frac{1}{a_0},\\ a_0^q a_3^{q^2}+\frac{a_1}{a_0}=0,\\ a_0^{q^2}+a_3^{q^2}a_1^q+\frac{a_2}{a_0}=0,\\ a_1^{q^2}+a_3^{q^2}a_2^q+\frac{a_3}{a_0}=0, \end{cases}$$

and hence

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0(a_2^{q^2} + a_3^{q^2+q}) = 1, \\ a_1 = -a_0^{q+1} a_3^{q^2}, \\ a_2 = -a_0^{q^2+1} - a_3^{q^2} a_1^q a_0, \\ a_3 = -a_1^{q^2} a_0 - a_3^{q^2} a_2^q a_0, \end{cases}$$

i.e.

$$\begin{cases} \mathrm{N}(a_0) = 1, \\ a_0(-a_0^{q^4+q^2} + a_3^{q^5+q^4} a_0^{q^4+q^3+q^2} + a_3^{q^2+q}) = 1, \\ a_1 = -a_0^{q+1} a_3^{q^2}, \\ a_2 = -a_0^{q^2+1} + a_3^{q^3+q^2} a_0^{q^2+q+1}, \\ a_3 = a_3^{q^4} a_0^{q^3+q^2+1} + a_3^{q^2} a_0^{q^3+q+1} - a_0^{q^3+q^2+q+1} a_3^{q^4+q^3+q^2}. \end{cases}$$

References

[1] D. Bartoli, M. Giulietti, G. Marino and O. Polverino: Maximum scattered linear sets and complete caps in Galois spaces, Combinatorica **38**(2) (2018), 255—278.

[2] B. Csajbók, G. Marino and O. Polverino: Classes and equivalence of linear sets in $\mathrm{PG}(1, q^n)$, J. Combin. Theory Ser. A **157** (2018), 402–426.

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

[4] U. Dempwolff, J. C. Fisher and A. Herman: Semilinear transformations over finite fields are Frobenius maps, *Glasg. Math. J.* **42.2** (2000): 289–295.

[5] E. Gabidulin: Theory of codes with maximum rank distance, *Problems of information transmission*, **21(3)** (1985), 3–16.

[6] R. Gow and R. Quinlan: Galois theory and linear algebra, *Linear Algebra Appl.* **430** (2009), 1778–1789.

[7] R. Gow and R. Quinlan: Galois extensions and subspaces of alterning bilinear forms with special rank properties, *Linear Algebra Appl.* **430** (2009), 2212–2224.

[8] G. McGuire and J. Sheekey: A Characterization of the Number of Roots of Linearized and Projective Polynomials in the Field of Coefficients, https://arxiv.org/abs/1806.05853.

[9] S. Lang: Algebraic groups over finite fields, *Amer. J. Math.* **78** (1956), 555–563.

[10] R. Lidl and H. Niederreiter: Finite fields, *Cambridge university press,* Vol. **20**, 1997.

[11] O. Ore: On a special class of polynomials, *Trans. Amer. Math. Soc.* **35** (1933), 559–584.

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

[13] F. Zullo: Linear codes and Galois geometries: between two worlds, *PhD thesis*, Università degli Studi della Campania "Luigi Vanvitelli" (2018).

Bence Csajbók
MTA–ELTE Geometric and Algebraic Combinatorics Research Group
ELTE Eötvös Loránd University, Budapest, Hungary
Department of Geometry
1117 Budapest, Pázmány P. stny. 1/C, Hungary
csajbokb@cs.elte.hu

Giuseppe Marino
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli",
Viale Lincoln 5, I- 81100 Caserta, Italy

Dipartimento di Matematica e Applicazioni "Renato Caccioppoli"
Università degli Studi di Napoli "Federico II",
Via Cintia, Monte S.Angelo I-80126 Napoli, Italy
giuseppe.marino@unicampania.it, *giuseppe.marino@unina.it*

Olga Polverino and Ferdinando Zullo
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania "Luigi Vanvitelli",
I– 81100 Caserta, Italy
olga.polverino@unicampania.it,
ferdinando.zullo@unicampania.it