A Collection of
MTA–ELTE GAC manuscripts

Bence Csajbók, Giuseppe Marino, Olga Polverino,
Ferdinando Zullo

A CHARACTERIZATION OF LINEARIZED POLYNOMIALS WITH MAXIMUM KERNEL

2018

MTA–ELTE Geometric and Algebraic
Combinatorics Research Group

Hungarian Academy of Sciences
Eötvös University, Budapest

MANUSCRIPTS
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 \( K \) denote

\footnote{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 $(x^q^m - x)$ 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 $\tilde{\mathcal{L}}_{n,q} := \{ \sum_{i=0}^{n-1} a_i x^i : a_i \in \mathbb{F}_{q^n} \}$. 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

$$
\begin{pmatrix}
    x & x^q & \cdots & x^{q^{k-1}} \\
    u_1 & u_1^q & \cdots & u_1^{q^{k-1}} \\
    \vdots & \vdots & & \vdots \\
    u_k & u_k^q & \cdots & u_k^{q^{k-1}}
\end{pmatrix}.
$$

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

**Result 1.1.** [5, Theorem 5] Let $\mathbb{L}$ be a cyclic extension of a field $\mathbb{F}$ of degree $n$, and suppose that $\sigma$ generates the Galois group of $\mathbb{L}$ over $\mathbb{F}$. Let $k$ be an integer satisfying $1 \leq k < n$, and let $a_0, a_1, \ldots, a_k$ be elements of $\mathbb{L}$, not all 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 $\mathbb{L}$. 

2
Similarly to the $s = 1$ case we will say that a $\sigma$-polynomial is of maximum kernel if the dimension of its kernel equals its $\sigma$-degree.

Our main result provides sufficient and necessary conditions on the coefficients of a $\sigma$-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 $a_0, \ldots, a_k \in \mathbb{F}_{q^n}$. Then $f(x)$ is of maximum kernel if and only if the matrix
\[
A = \begin{pmatrix}
0 & 0 & \cdots & 0 & a_0 \\
1 & 0 & \cdots & 0 & a_1 \\
0 & 1 & \cdots & 0 & a_2 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 1 & a_{k-1}
\end{pmatrix}
\]
(1)
satisfies
\[ AA^\sigma \cdots A^{\sigma^{n-1}} = I_k, \]
where $A^\varphi$ is the matrix obtained from $A$ by applying to each of its entries the automorphism $x \mapsto x^\varphi$ 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 $\sigma$-polynomial, cf. Theorem 3.1.

In Section 2.1 we study in details the $\sigma$-polynomials of $\sigma$-degree $n - 2$ for each $n$. For $n \leq 6$ we also provide a list of all $\sigma$-polynomials with maximum kernel cf. Sections 2.2, 2.3 and 2.4.

## 2 Main Result

We will need the following lemma about the fixed points of a semilinear map. It is probably a well-known result, but we couldn’t find a reference for the $k \neq n$ case and hence we present here a proof.

**Lemma 2.1.** If $\tau$ is an $\mathbb{F}_{q^n}$-semilinear map of $V = \mathbb{F}_{q^n}^k$, $1 \leq k \leq n$, of order $n$, with companion automorphism $\sigma \in \text{Aut} (\mathbb{F}_{q^n})$ such that $\text{Fix}(\sigma) = \mathbb{F}_q$, then $\text{Fix}(\tau)$ is a $k$-dimensional $\mathbb{F}_q$-subspace of $V$ and $\langle \text{Fix}(\tau) \rangle_{\mathbb{F}_q^n} = V$. 


Proof. If $k = n$ then it is [3, Main Theorem]. Suppose $k < n$ and let $A$ denote the $k \times k$ matrix with entries in $\mathbb{F}_{q^n}$ representing the linear part of $\tau$, and let $\sigma$ denote the Frobenius automorphism $x \mapsto x^{q^n} \in \mathbb{F}_{q^n}$, with $\gcd(s, n) = 1$. Then $\tau$ is defined by the following rule

$$
\tau: \begin{pmatrix} x_0 \\ \vdots \\ x_{k-1} \end{pmatrix} \in \mathbb{F}_{q^n}^k \mapsto A \begin{pmatrix} x_0 \\ \vdots \\ x_{k-1} \end{pmatrix}^{q^n} \in \mathbb{F}_{q^n}^k.
$$

Embed $V$ in $W = \mathbb{F}_{q^n}^n$ in a way that $V$ has equations $x_k = x_{k+1} = \ldots = x_{n-1} = 0$, and let $\tilde{\tau}$ be the $\mathbb{F}_{q^n}$-semilinear map of $W$ defined as

$$
\tilde{\tau}: \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \in \mathbb{F}_{q^n}^n \mapsto \begin{pmatrix} A & O_{k,n-k} \\ O_{n-k,k} & I_{n-k} \end{pmatrix} \begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix}^{q^n} \in \mathbb{F}_{q^n}^n,
$$

where $O_{i,j}$ is the $i \times j$ zero matrix and $I_i$ is the identity matrix of order $i$. Then $\tilde{\tau}$ has order $n$, $\tilde{\tau}|_V = \tau$ and, by [3, Main Theorem], $\text{Fix}(\tilde{\tau}) \simeq \mathbb{F}_q^n$ and $(\text{Fix}(\tilde{\tau}))/_{\mathbb{F}_{q^n}} = W$.

The lattice of $\mathbb{F}_q$-subspaces defined by the non-zero vectors of $\text{Fix}(\tilde{\tau})$ form a canonical subgeometry isomorphic to $\text{PG}(n-1, q)$ in $\text{PG}(W, \mathbb{F}_{q^n}) = \text{PG}(n-1, \mathbb{F}_{q^n})$. It is well-known that a $d$-dimensional $\mathbb{F}_{q^n}$-space $U$ of $W$ meets $\text{Fix}(\tilde{\tau})$ in a $d$-dimension $\mathbb{F}_q$-space if and only if $\tilde{\tau}$ fixes $U$.

Since $\tilde{\tau}(V) = V$, we get $k = \dim_{\mathbb{F}_q}(V \cap \text{Fix}(\tilde{\tau})) = \dim_{\mathbb{F}_q}(\text{Fix}(\tau))$ and $V = \langle V \cap \text{Fix}(\tilde{\tau}) \rangle_{\mathbb{F}_{q^n}} = \langle \text{Fix}(\tau) \rangle_{\mathbb{F}_{q^n}}$. \qed

Now we are able to prove our main result:

Proof of Theorem 1.2. First suppose $\dim \ker f = k$. 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 $u := (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_{q^n}^k$. Since $u_0, u_1, \ldots, u_{k-1}$ are $\mathbb{F}_q$-linearly independent, by [7, Lemma 3.51], we get that $\mathcal{B} := (u, u^{q^s}, \ldots, u^{q^{s(k-1)}})$ is an ordered $\mathbb{F}_{q^n}$-basis of $\mathbb{F}_{q^n}^k$. Also, $u^{q^k} = a_0 u + a_1 u^{q^s} + \cdots + a_{k-1} u^{q^{s(k-1)}}$. It can be seen that the matrix (1) represents the $\mathbb{F}_{q^n}$-linear part of the $\mathbb{F}_{q^n}$-semilinear map $\sigma: v \in \mathbb{F}_{q^n}^k \mapsto v^{q^s} \in \mathbb{F}_{q^n}^k$ w.r.t. the basis $\mathcal{B}$. Since $\gcd(s, n) = 1$, $\sigma$ has order $n$ and hence the assertion follows.

Vice versa, let $\tau$ be defined as follows
\[
\tau : \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{pmatrix} \in \mathbb{F}_{q^n}^k \mapsto A \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{k-1} \end{pmatrix}^{q^i} \in \mathbb{F}_{q^n}^k, \quad (2)
\]

where \( A \) is as in (1) with the property \( A \mathbb{F}_{q^n} \cdots \mathbb{F}_{q^{i(n-1)}} = I_k \). Then \( \tau \) has order \( n \) and, by Lemma 2.1, it fixes a \( k \)-dimensional \( \mathbb{F}_q \)-subspace \( S \) of \( \mathbb{F}_{q^n}^k \).

Let now \( \beta \) be the \( \mathbb{F}_{q^n} \)-semilinear map

\[
\beta : (x_0, \ldots, x_{k-1}) \in \mathbb{F}_{q^n}^k \mapsto \left(x_0^{q^i}, x_1^{q^i}, \ldots, x_{k-1}^{q^i}\right) \in \mathbb{F}_{q^n}^k.
\]

Then \( \beta \) has order \( n \) and \( \text{Fix} \beta = \mathbb{F}_q^k \) since \( \text{gcd}(s, n) = 1 \).

Let \( s_0, \ldots, s_{k-1} \) be an \( \mathbb{F}_q \)-basis of \( S \) and let \( e_0 = (1, 0, \ldots, 0), \ldots, e_{k-1} = (0, \ldots, 0, 1) \) be an \( \mathbb{F}_q \)-basis of \( \mathbb{F}_q^k \). They also form an \( \mathbb{F}_q \)-basis of \( \mathbb{F}_{q^n}^k \). Let \( \phi \) be the unique isomorphism of \( \mathbb{F}_{q^n}^k \) such that \( \phi(s_i) = e_i \) for each \( i \in \{0, \ldots, k-1\} \). Then \( \beta = \phi \circ \tau \circ \phi^{-1} \) and also

\[
\beta^i = \phi \circ \tau^i \circ \phi^{-1}, \quad (3)
\]

for each \( i \in \{1, \ldots, n-1\} \). Also, by (2)

\[
\tau(e_0) = e_1,
\tau(e_1) = \tau^2(e_0) = e_2,
\vdots
\tau(e_{k-1}) = \tau^k(e_0) = (a_0, \ldots, a_{k-1}) = a_0 e_0 + \cdots + a_{k-1} e_{k-1}.
\]

So, we get that

\[
\tau^k(e_0) = a_0 e_0 + a_1 \tau(e_0) + \cdots + a_{k-1} \tau^{k-1}(e_0),
\]

and applying \( \phi \) it follows that

\[
\phi(\tau^k(e_0)) = a_0 \phi(e_0) + a_1 \phi(\tau(e_0)) + \cdots + a_{k-1} \phi(\tau^{k-1}(e_0)).
\]

By (3) the previous equation becomes

\[
\beta^k(\phi(e_0)) = a_0 \phi(e_0) + a_1 \beta(\phi(e_0)) + \cdots + a_{k-1} \beta^{k-1}(\phi(e_0)).
\]
Put \( u = \phi(e_0) \), then
\[
  u^{\tau^k} = a_0 u + a_1 u^{\tau^s} + \cdots + a_{k-1} u^{\tau^{(k-1)}}.
\]
This implies that \( u_0, u_1, \ldots, u_{k-1} \) are elements of \( \ker f \), where \( u = (u_0, \ldots, u_{k-1}) \), and they are \( \mathbb{F}_q \)-independent since \( B = (u, \ldots, u^{\tau^{(k-1)}}) = (\phi(e_0), \ldots, \phi(e_{k-1})) \) is an ordered \( \mathbb{F}_q \)-basis of \( \mathbb{F}_q^k \). This completes the proof. \( \square \)

As a corollary we get the second part of [4, Theorem 10], see also [9, Lemma 3] for the case \( s = 1 \) and [8] for the case when \( q \) is a prime. Indeed, by evaluating the determinants in \( AA^\tau \cdots A^{\tau^{(n-1)}} = I_k \) we obtain the following corollary. Here and later in the paper for \( x \in \mathbb{F}_q^s \) and for a subfield \( \mathbb{F}_q^m \) of \( \mathbb{F}_q^s \) we will denote by \( \mathcal{N}_{\mathbb{F}_q^m}(x) \) the norm of \( x \) over \( \mathbb{F}_q^m \), that is, \( x^{1+q^m+\cdots+q^{n-m}} \), and by \( \text{Tr}_{\mathbb{F}_q^m}(x) \) we will denote the trace of \( x \) over \( \mathbb{F}_q^m \), that is, \( x + x^{q^m} + \cdots + x^{q^{n-m}} \). If \( n \) is clear from the context and \( m = 1 \) then we will simply write \( \mathcal{N}(x) \) and \( \text{Tr}(x) \).

**Corollary 2.2.** If the kernel of a \( q^s \)-polynomial \( f(x) = a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{(k-1)}} - x^{q^k} \) has dimension \( k \), then \( \mathcal{N}(e_0) = (-1)^{n(k+1)} \).

**Corollary 2.3.** Let \( A \) be a matrix as in Theorem 1.2. The condition
\[
  AA^\tau \cdots A^{\tau^{(n-1)}} = I_k
\]
is satisfied if and only if \( AA^\tau \cdots A^{\tau^{(n-1)}} \) fixes \( e_0 = (1, 0, \ldots, 0) \).

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

Consider a \( q^s \)-polynomial \( f(x) = a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{(k-1)}} - x^{q^k} \), the matrix \( A \in \mathbb{F}_q^{k \times k} \) as in Theorem 1.2 and the semilinear map \( \tau \) defined in (2).

Note that
\[
  e_0^\tau = (0, 1, 0, \ldots, 0) = e_1
\]
\[
  e_0^{	au^2} = (0, 0, 1, \ldots, 0) = e_2
\]
\begin{equation}
\begin{aligned}
e_0^{r_{k-1}} &= (0, 0, 0, \ldots, 1) = e_{k-1} \\
e_0^r &= (a_0, a_1, a_2, \ldots, a_{k-1}) \\
e_0^{r_{k+1}} &= (a_0 a_{k-1}^q, a_0^q + a_1 a_{k-1}^{q^2}, a_1^q + a_2 a_{k-1}^{q^3}, \ldots, a_{k-2}^q + a_{k-1}^{q^{r_{k-1}}}).
\end{aligned}
\end{equation}

Hence, if

\[ e_0^{r_i} = (Q_0,i(a_0, a_1, \ldots, a_{k-1}), Q_1,i(a_0, a_1, \ldots, a_{k-1}), \ldots, Q_{k-1,i}(a_0, a_1, \ldots, a_{k-1})) \]

for \( i \geq 0 \), then

\[ e_0^{r_{i+1}} = (a_0 Q_{k-1,i}(a_0, a_1, \ldots, a_{k-1})^q, Q_0,i(a_0, a_1, \ldots, a_{k-1})^{q^2} + a_1 Q_{k-1,i}(a_0, a_1, \ldots, a_{k-1})^{q^2}, \ldots, Q_{k-2,i}(a_0, a_1, \ldots, a_{k-1})^{q^2} + a_{k-1} Q_{k-1,i}(a_0, a_1, \ldots, a_{k-1})^{q^2}) \]

i.e. the polynomials \( Q_{j,i}(a_0, a_1, \ldots, a_{k-1}) \) for \( 0 \leq j \leq k-1 \) can be defined by the following recursive relations for \( 0 \leq i \leq k-1 \):

\[ Q_{j,i}(a_0, a_1, \ldots, a_{k-1}) = \begin{cases} 
1 & \text{if } j = i, \\
0 & \text{otherwise},
\end{cases} \]

and by the following relations for \( i \geq k \):

\[ Q_{0,i+1}(a_0, a_1, \ldots, a_{k-1}) = a_0 Q_{k-1,i}(a_0, a_1, \ldots, a_{k-1})^{q^2} \]

\[ Q_{j,i+1}(a_0, a_1, \ldots, a_{k-1}) = Q_{j-1,i}(a_0, a_1, \ldots, a_{k-1})^{q^2} + a_j Q_{k-1,i}(a_0, a_1, \ldots, a_{k-1})^{q^2}. \]

When \( a_0, a_1, \ldots, a_{k-1} \) are clear from the context, we will denote \( Q_{j,i}(a_0, a_1, \ldots, a_{k-1}) \) by \( Q_{j,i} \). Now, we are able to prove the following.

**Theorem 2.4.** The kernel of a \( q^r \)-polynomial \( f(x) = a_0 x + a_1 x^{q^r} + \cdots + a_{k-1} x^{q^r(k-1)} - x^{q^r k} \in \mathbb{F}_{q^n}[x] \), where \( \gcd(s, n) = 1 \), has dimension \( k \) if and only if

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

**Proof.** Relations (5) can be written as follows

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

7
with \( i \in \{0, \ldots, n-1\} \). Also, \((Q_{0,0}, Q_{1,0}, \ldots, Q_{k-1,0}) = (1, 0, \ldots, 0)\) and \(e_0 = (Q_{0,t}, \ldots, Q_{k-1,t})\) for \( t \in \{0, \ldots, n\} \). By Theorem 1.2 and by Corollary 2.3, the kernel of \( f(x) \) has dimension \( k \) if and only if \( e_0 = (Q_{0,0}, Q_{1,0}, \ldots, Q_{k-1,0})\) is fixed by \( AA^T \cdots A^{(n-1)} \), so this happens if and only if

\[
e_0^{Tn} = (Q_{0,n}, Q_{1,n}, \ldots, Q_{k-1,n}) = (1, 0, \ldots, 0).
\]

\[\square\]

Theorem 2.4 with \( k = n - 1 \) and \( s = 1 \) gives the following well-known result as a corollary.

**Corollary 2.5.** [7, 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

\[
f(x) = \alpha \text{Tr}(\beta x).
\]

Again from Theorem 2.4 we can deduce the following.

**Corollary 2.6.** [7, Ex. 2.14] The \( q^s \)-polynomial \( a_0 x - x^{q^k} \in \mathbb{F}_{q^n}[x] \), with \( \gcd(s, n) = 1 \) and \( 1 \leq k \leq n - 1 \), admits \( q^k \) roots if and only if \( k \mid n \) and \( N_{q^s/q^n}(a_0) = 1 \).

### 2.1 When the \( q^s \)-degree equals \( n - 2 \)

In this section we investigate \( q^s \)-polynomials

\[
f(x) = a_0 x + a_1 x^{q^s} + \cdots + a_{n-3} x^{q^{s(n-3)}} - x^{q^{s(n-2)}}
\]

with \( \gcd(s, n) = 1 \). By Theorem 2.4, \( \dim \ker f(x) = n - 2 \) if and only if \( a_0, a_1, \ldots, a_{n-3} \) satisfy the following system of equations

\[
\begin{align*}
a_0(a_{n-4}^{2s} + a_{n-3}^{2s+q^s}) &= 1, \\
a_0^q a_{n-3} a_{n-4}^{2s} + a_1(a_{n-4}^{2s} + a_{n-3}^{2s+q^s}) &= 0, \\
a_0^{q^2} + a_{n-3} a_1^{q^2} + a_2(a_{n-4}^{2s} + a_{n-3}^{2s+q^s}) &= 0, \\
a_1^{q^2} + a_{n-3} a_2^{q^2} + a_3(a_{n-4}^{2s} + a_{n-3}^{2s+q^s}) &= 0, \\
& \vdots \\
a_{n-5}^{q^2} + a_{n-3} a_{n-4}^{q^2} + a_{n-3}(a_{n-4}^{2s} + a_{n-3}^{2s+q^s}) &= 0,
\end{align*}
\]
which is equivalent to

$$\begin{cases} a_0(a_{n-4}^{q^2} + a_{n-3}^{q^2 + q^s}) = 1, \\ a_1 = -a_0^{q+1} a_{n-3}^{q^2} =: g_1(a_0, a_{n-3}), \\ a_j = -a_{j-2}^{q^2} a_0 - a_{n-3}^{q^2} a_{j-1}^{q^s} a_0 =: g_j(a_0, a_{n-3}), \text{ for } 2 \leq j \leq n - 3. \end{cases}$$ (7)

So, dim ker $f(x) = n - 2$ if and only if $a_0$ and $a_{n-3}$ satisfy the equations

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

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

**Theorem 2.7.** Suppose that $f(x) = a_0 x + a_1 x^q + \cdots + a_{n-3} x^{q^{n-3}} - x^{q^{n-2}}$ 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

$$a_{n-2t+1} a_{t-2}^{q^2 + q^s} = -a_{n-t}^{q+1} a_{2t-3}^{q^2}.$$ (8)

Also, with $s = n - t + 1$ it holds that

$$-a_{n-t}(-a_{t-2}^{q^2} a_{3t-4}^{q^2} + a_{2t-3}^{q^2 + q^s}) = a_{t-2}^{q^2 + q^s + 1}.$$ (9)

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

$$N(a_{n-t}) = (-1)^n N(a_{t-2})$$ (10)

and

$$N(a_{n-2t+1}) = (-1)^n N(a_{2t-3}),$$ (11)

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

**Proof.** Let $t \geq 2$ with $(t - 1, n) = 1$ 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 ker $F = \dim \ker f = n - 2$. By renaming the coefficients $F(x)$ can be written as

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

9
\[ \alpha_0 x + \alpha_1 x^{q^{n-t}+1} + \cdots + \alpha_{n-3} x^{q^{n-3}} + \alpha_{n-2} x^{q^{2t}}. \]

Since \( F(x) \) has maximum kernel, by the second equation of (7) we get \( \alpha_0 \neq 0, \alpha_{n-2} \neq 0 \) and the following relation

\[ -\frac{\alpha_1}{\alpha_{n-2}} = -\left( -\frac{\alpha_0}{\alpha_{n-2}} \right)^{q^{n-t}+1} \left( -\frac{\alpha_{n-3}}{\alpha_{n-2}} \right)^{q^{2s}}. \]  \( \text{(12)} \)

The coefficient \( \alpha_j \) of \( F(x) \) equals the coefficient \( a_i \) of \( f(x) \) with \( i \equiv n-t+j(1-t) \) (mod \( n \)), in particular

\[ \begin{align*}
\alpha_0 &= a_{n-t}, \\
\alpha_1 &= a_{n-2t+1}, \\
\alpha_{n-3} &= a_{2t-3}, \\
\alpha_{n-2} &= a_{t-2}, \\
\alpha_{n-4} &= a_{3t-4},
\end{align*} \]  \( \text{(13)} \)

and by (12), we get that \( a_{t-2} \) and \( a_{n-t} \) are nonzero, and

\[ a_{n-2t+1} a_{t-2}^{q^{2s}+q^s} = -a_{n-t}^{q^{n-t}} a_{2t-3}^{q^{2s}}. \]

which gives (8). The first equation of (7) gives

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

that is,

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

Then (13) and \( \alpha_{n-4} = a_{3t-4} \) imply

\[ -a_{n-t}(-\alpha_{t-2}^{q^s} a_{3t-4}^{q^{2s}}+\alpha_{2t-3}^{q^{2s}})=a_{t-2}^{q^{2s}+q^s+1}, \]

which gives (9). By Corollary 2.2 with \( s = n-t+1 \) we obtain

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

and taking (13) into account we get

\[ N(a_{n-t}) = (-1)^n N(a_{t-2}). \]

Then (8) and the previous relation yield

\[ N(a_{n-2t+1}) = (-1)^n N(a_{2t-3}). \]

\( \Box \)
Proposition 2.8. Let \( f(x) \) be a \( q^s \)-polynomial with \( q^s \)-degree \( n - 2 \) and with maximum kernel. If the coefficient of \( x^{n-2} \) is zero, then \( n \) is even and \( f(x) = \alpha \text{Tr}_{q^n/q^2}(\beta x) \) for some \( \alpha, \beta \in \mathbb{F}_{q^n}^* \).

Proof. We may assume \( f(x) = a_0 x + a_1 x^{q^s} + \cdots + a_{n-3} x^{q^{s(n-3)}} - x^{q^{s(n-2)}} \) with \( a_1 = 0 \). By the second equation of (7), it follows that \( a_{n-3} = 0 \). By the third equation of (7), we get that \( a_j = 0 \) for every odd integer \( j \in \{3, \ldots, n-3\} \). If \( j \) is even then we have

\[
a_j = (-1)^{\frac{j}{2}} a_0^{q^{s(j-2)}+q^{s(j-4)}+\cdots+q^{s2}+1}.
\]

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 \( N(a_0) = (-1)^n \), there exists \( \lambda \in \mathbb{F}_{q^n}^* \) such that \( a_0 = -\lambda^{q^{s(n-2)}} \). So, by (14) we get \( a_j = \lambda^{q^{s(j-2)}} \), and hence

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

\[\square\]

In the next sections we list all the \( q^s \)-polynomials of \( \mathbb{F}_{q^n} \) with maximum kernel for \( n \leq 6 \). By Corollaries 2.5 and 2.6 the \( n \leq 3 \) case can be easily described hence we will consider only the \( n \in \{4, 5, 6\} \) cases.

For \( f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathcal{L}_{n,q} \) we denote by \( \hat{f}(x) := \sum_{i=0}^{n-1} a_i^{q^i} x^{q^{n-i}} \) the adjoint (w.r.t. the symmetric non-degenerate bilinear form defined by \( \langle x, y \rangle = \text{Tr}(xy) \)) 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 2.9. If \( f(x) \in \mathcal{L}_{n,q} \) 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.

2.2 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 2.9, we can assume $s = 1$. Corollaries 2.5 and 2.6 cover the cases when the $q$-degree of $f$ is 1 or 3 so from now on we suppose $f(x) = a_0 x + a_1 x^q - x^{q^2}$. If $a_1 = 0$ then we can use again Corollary 2.6 and we get $a_0 x - x^{q^2}$, with $N_{q^4/q^2}(a_0) = 1$. Suppose $a_1 \neq 0$. By Equation (7), we get the conditions
\[
\begin{align*}
\left\{ a_0 (a_0^q + a_1^{q^2 + q}) = 1,
\right.
\left\{ a_1 = -a_0^{q+1}a_1^{q^2}.
\right.
\end{align*}
\]
This system can be rewritten as
\[
\Sigma: \begin{cases}
  a_1^{q^2 - 1} = -\frac{1}{a_0^{q+1}}, \\
  a_1^{q+1} = a_0^{q^2 + q^2} - a_0^q,
\end{cases}
\]
which is equivalent to
\[
\Sigma': \begin{cases}
  N_{q^4/q^2}(a_0) = 1, \\
  a_1^{q+1} = a_0^{q^2 + q^2} - a_0^q.
\end{cases}
\]
Indeed, consider the system
\[
\Sigma^*:\begin{cases}
  N_{q^4/q^2}(a_0) = 1, \\
  a_1^{q^2 - 1} = -\frac{1}{a_0^{q+1}}, \\
  a_1^{q+1} = a_0^{q^2 + q^2} - a_0^q.
\end{cases}
\]
Denote by $S(\Sigma)$, $S(\Sigma')$ and $S(\Sigma^*)$ the set of solutions of $\Sigma$, $\Sigma'$ and $\Sigma^*$, respectively. Clearly, $S(\Sigma^*) \subseteq S(\Sigma') \cap S(\Sigma)$. By Corollary 2.2, if $(a_0, a_1) \in S(\Sigma)$, then $N_{q^4/q^2}(a_0) = 1$ and so $S(\Sigma^*) = S(\Sigma)$. Furthermore, if $(a_0, a_1) \in S(\Sigma')$, then
\[
a_1^{q^2 - 1} = \left(\frac{1}{a_0^q} - a_0^{q^2} \right)^{q-1} = -\frac{1}{a_0^{q+1}},
\]
i.e. $(a_0, a_1) \in S(\Sigma^*)$ and hence $S(\Sigma) = S(\Sigma')$.

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 $q^2$-polynomials over $\mathbb{F}_{q^4}$ with maximum kernel. In the following table the $q$-degree will be denoted by $k$. 

12
2.3 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 2.9, we can assume $s \in \{1, 2\}$. Corollaries 2.5 and 2.6 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.

$$f(x) = a_0x + a_1x^{q^s} + a_2x^{q^{2s}} - x^{q^{3s}}.$$ 

From (7), the previous $q^s$-polynomial has maximum kernel if and only if $a_0$, $a_1$ and $a_2$ satisfy the following conditions:

$$\left\{\begin{array}{l}
a_1 = -a_0^{q^{s+1}}a_2^{q^s},
a_1^{q^{3s+q^2s+1}}a_2^{q^{2s+q^s}} + a_0^{q^{2s+q^s}}a_0 = 1,
a_2 = -a_0^{q^{2s+q^s+1}}a_2^{q^{3s+q^2s+1}}a_0^{q^{2s+q^s+1}}.
\end{array}\right.$$ 

Arguing as in the case $n = 4$, the previous equations are equivalent to

$$\left\{\begin{array}{l}
N(a_0) = 1,
a_1 = -a_0^{q^{2s+1}}a_2^{q^s},
-a_0^{q^{3s+q^2s+1}}a_2^{q^{2s+q^s}} + a_0a_2^{q^{2s+q^s}} = 1.
\end{array}\right.$$ 

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

$$f(x) = a_0x + a_1x^{q^s} - x^{q^{2s}}.$$ 

By Theorem 2.4 the polynomial $f(x)$ has maximum kernel if and only if its coefficients satisfy

$$\left\{\begin{array}{l}
a_0(a_0^{q^{2s}}a_1^{q^s} + a_1^{q^s}(a_0^{q^{3s}} + a_1^{q^{3s+q^2s}})) = 1,
a_0^{q^{s+1}}(a_0^{q^{3s}} + a_1^{q^{3s+q^2s}}) + a_1 = 0,
\end{array}\right.$$
which is equivalent to

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

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

<table>
<thead>
<tr>
<th>(k)</th>
<th>(s)</th>
<th>Polynomial form</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1,2</td>
<td>(\text{Tr}(\lambda x))</td>
<td>(\lambda \in \mathbb{F}_{q^s}^*)</td>
</tr>
</tbody>
</table>
| 3 | 1,2 | \(a_0x + a_1x^{q^s} + a_2x^{q^2s} - x^{q^3s}\) | \(\begin{cases} N(a_0) = 1 \\
a_1 = -a_0^{q^s+1}a_2^{q^2s} - a_0^{q^{3s}+q^{2s}+q^s}a_2^{q^3s} + a_0a_2^{q^2s+q^s} = 1 \end{cases}\) |
| 2 | 1,2 | \(a_0x + a_1x^{q^s} - x^{q^{2s}}\) | \(\begin{cases} N(a_0) = -1 \\
a_0^{q^s+q^s+1}a_1^{q^3s} - a_1^{q^s+1} = a_0^{q^s} \end{cases}\) |
| 1 | 1,2 | \(a_0x - x^{q^s}\) | \(N(a_0) = 1\) |

### 2.4 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 2.9, we can assume \(s = 1\). Corollaries 2.5 and 2.6 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 2.4, \(f(x)\) has maximum kernel if and only if the coefficients satisfy

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

If \(k = 3\), then \(f(x) = a_0x + a_1x^{q^s} + a_2x^{q^{2s}} - x^{q^{3s}}\), and by Theorem 2.4 it has maximum kernel if and only the coefficients fulfil

\[
\begin{cases}
N(a_0) = 1, \\
\frac{a_0^{q^s+1}}{a_1^{q^s}} = a_2a_0^{q^s} + a_0^{q^{2s}+q^s+1}a_1^{q^{3s}}, \\
\frac{a_2^{q^s+1}}{a_1^{q^s}} = -a_0^{q^{3s}+q^{2s}+q^s+1}a_1^{q^{4s}} - a_1^{q^s}.
\end{cases}
\]
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 $f(x) = a_0 x + a_1 x^q + a_2 x^{q^2} + a_3 x^{q^3} - x^{q^4}$ has maximum kernel if and only if the coefficients satisfy

$$\begin{cases}
    a_0(a_2^{q^2} + a_3^{q_2 + q^*}) = 1, \\
    a_1 = -a_0^{q^* + 1} a_3^{q^2}, \\
    a_2 = -a_0^{q^2 + 1} - a_3^{q^2} a_1^q a_0, \\
    a_3 = -a_1^{q^2} a_0 - a_3^{q^2} a_2^q a_0.
\end{cases}$$

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

<table>
<thead>
<tr>
<th>$k$</th>
<th>polynomial form</th>
<th>conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>$\text{Tr}_{q^5/q}(\lambda x)$</td>
<td>$\lambda \in \mathbb{F}_{q^5}^*$</td>
</tr>
</tbody>
</table>
| 4   | $a_0 x + a_1 x^q + a_2 x^{q^2} + a_3 x^{q^3} - x^{q^4}$ | \begin{align*}
    a_1 &\neq 0 \\
    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{align*} |
| 4   | $\text{Tr}_{q^4/q^3}(\lambda x)$ | $\lambda \in \mathbb{F}_{q^6}^*$ |
| 3   | $a_0 x + a_1 x^q + a_2 x^{q^2} - x^{q^3}$ | \begin{align*}
    a_1 &\neq 0 \\
    a_2 &\neq 0 \\
    N_{q^3/q}(a_0) &= 1 \\
    a_1^{q+1} &= a_2 a_0^{q^2} + a_0^{q^2 + q + 1} a_2^{q^2} \\
    a_2^{q+1} &= -a_0^{q^3 + q^2 + q + 1} a_1^q - a_1^q
\end{align*} |
| 3   | $\text{Tr}_{q^4/q^3}(\lambda x)$ | $\lambda \in \mathbb{F}_{q^6}^*$ |
| 2   | $a_0 x + a_1 x^q - x^{q^2}$ | \begin{align*}
    a_1 &\neq 0 \\
    a_1^{q^4} a_0^{q^3} + a_1^{q^2} (a_0^{q^4} + a_1^{q^4 + q^*}) &= -a_1^{q+1} \\
    (a_0^{q^4} + a_1^{q^4 + 1})^{q^3} &= a_0^{q^5 + q^4 + q^3} (a_0^{q^4} + a_1^{q^4 + 1})
\end{align*} |
| 2   | $a_0 x - x^{q^2}$ | $N_{q^3/q^2}(a_0) = 1$ |
| 1   | $a_0 x - x^q$ | $N_{q^3/q}(a_0) = 1$ |
3 Application

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

**Theorem 3.1.** Let $f(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{k-1}} - x^{q^k} \in \mathbb{F}_{q^n}[x]$ with $a_0 \neq 0$ and let $A$ be defined as in (1). Then the splitting field of $f(x)$ is $\mathbb{F}_{q^m}$ where $m$ is the (multiplicative) order of the matrix $B := AA^q \cdots A^{q^{m-1}}$.

**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 $\mathbb{F}_{q^m}$ is the splitting field of $f(x)$ and let $t$ denote the order of $B$. Then the kernel of the $\mathbb{F}_q$-linear $\mathbb{F}_{q^m} \to \mathbb{F}_{q^m}$ map defined as $x \mapsto f(x)$ has dimension $k$ over $\mathbb{F}_q$ and hence by Theorem 1.2 we have

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

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

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

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

A further application of Theorem 1.2 is the following.

**Theorem 3.2.** 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 $f(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{k-1}} - x^{q^k}$ and $g(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{k-1}} - x^{q^k}$, where $a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}$. The kernel of $f(x)$ considered as a linear transformation of $\mathbb{F}_{q^m}$ has dimension $k$ if and only if the kernel of $g(x)$ considered as a linear transformation of $\mathbb{F}_{q^m}$ has dimension $k$.

**Proof.** Denote by $A$ the matrix associated with $f(x)$ as in (1). By hypothesis, $A \in \mathbb{F}_{q^n}^{k \times k}$ 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 $\mathbb{F}_{q^m}$, has dimension $k$ if and only if

$$AA^q \cdots A^{q^{(nm-1)}} = I_k.$$
Since \( s \equiv t \pmod{m} \), we have
\[
AA^s \cdots A^s(nm-1) = AA^t \cdots A^t(nm-1) = I_k,
\]
and, again by Theorem 1.2, this holds if and only if the kernel of \( g(x) \), considered as a linear transformation of \( \mathbb{F}_{q^m} \), has dimension \( k \). \( \square \)

**Addendum**

During the “Combinatorics 2018” conference, the fourth author presented the results of this paper in his talk entitled “On \( q \)-polynomials with maximum kernel”. In the same conference John Sheekey presented his joint work with Gary McGuire [6] 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.

**References**


[6] **G. McGuire and J. Sheekey**: A Characterization of the Number of Roots of Linearized and Projective Polynomials in the Field of Coefficients, manuscript.


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, Olga Polverino and Ferdinando Zullo
Dipartimento di Matematica e Fisica,
Università degli Studi della Campania “Luigi Vanvitelli”,
I–81100 Caserta, Italy
giuseppe.marino@unicampania.it, olga.polverino@unicampania.it,
gerardzullo@unicampania.it