Revisiting Products of the Form X Times a Linearized Polynomial $L(X)$

Christof Beierle

Ruhr University Bochum, Faculty of Computer Science, Bochum, Germany

Abstract

For a q-polynomial L over a finite field $\mathbb{F}_{q^n}$, we characterize the differential spectrum of the function $f_L \colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto x \cdot L(x)$ and show that, for $n \leq 5$, it is completely determined by the image of the rational function $r_L \colon \mathbb{F}_{q^n}^* \to \mathbb{F}_{q^n}, x \mapsto L(x)/x$. This result follows from the classification of the pairs (L, M) of q-polynomials in $\mathbb{F}_{q^n}[X]$, $n \leq 5$, for which r_L and r_M have the same image, obtained in [B. Csajbók, G. Marino, and O. Polverino. A Carlitz type result for linearized polynomials. Ars Math. Contemp., 16(2):585–608, 2019]. For the case of $n > 5$, we pose an open question on the dimensions of the kernels of $x \mapsto L(x) - ax$ for $a \in \mathbb{F}_{q^n}$.

We further present a link between functions f_L of differential uniformity bounded above by q and scattered q-polynomials and show that, for odd values of q, we can construct CCZ-inequivalent functions f_M with bounded differential uniformity from a given function f_L fulfilling certain properties.

Keywords: linearized polynomial, differential spectrum, differential uniformity, linear set, scattered polynomial (MSC: 11T06, 12E10, 14G50)

1 Introduction and Preliminaries

Let $q = p^m$ for a prime p and a positive integer m and let $\mathbb{F}_{q^n}$ denote the field with q^n elements. A polynomial $L \in \mathbb{F}_{q^n}[X]$ is called a *q-polynomial* if it is of the form

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

There is a one-to-one correspondence of q-polynomials in $\mathbb{F}_{q^n}[X]$ and $\mathbb{F}_q$-linear mappings over $\mathbb{F}_{q^n}$ by means of their evaluation maps.

The version of record of this article, first published in Designs, Codes and Cryptography, is available online at Publisher's website `https://doi.org/10.1007/s10623-024-01511-w`. This is the version prior to copy-editing and typesetting by the publisher.

For a q-polynomial $L \in \mathbb{F}_{q^n}[X]$, we denote $f_L\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto x \cdot L(x)$. Such f_L are exactly the functions of the form

$$x \mapsto \sum_{i=0}^{n-1} a_i x^{q^i+1}, \quad a_i \in \mathbb{F}_{q^n}. \tag{2}$$

Given a function $f\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and $a, b \in \mathbb{F}_{q^n}$, we define

$$D_f(a,b) := \left|\{x \in \mathbb{F}_{q^n} \mid f(x+a) - f(x) = b\}\right|.$$

The *differential spectrum* of f, denoted by $\mathcal{D}_f$, counts the occurrences of $D_f(a,b)$ over all pairs $(a,b) \in \mathbb{F}_{q^n}^* \times \mathbb{F}_{q^n}$, formally,

$$\mathcal{D}_f := (\eta_i)_{i=0,\ldots,q^n},$$

where $\eta_i = |\{(a,b) \in \mathbb{F}_{q^n}^* \times \mathbb{F}_{q^n} \mid D_f(a,b) = i\}|$. The *differential uniformity* ([23]), denoted δ_f, is defined as

$$\delta_f := \max_{a,b \in \mathbb{F}_{q^n}, a \neq 0} D_f(a,b).$$

The differential uniformity, and more generally the differential spectrum of a function can be understood as a measure on the robustness against differential cryptanalysis [8] and its variants when using f as a substitution box in a symmetric cryptographic primitive (see e.g., [9] for a discussion). For p odd, functions reaching the lowest possible differential uniformity $\delta_f = 1$ are called *planar*. For $p = 2$, the lowest possible differential uniformity is 2, and functions reaching this value with equality are called *almost perfect nonlinear (APN)*. Besides the interest in functions with low differential uniformity for cryptographic applications, planar functions and APN functions have strong connections to objects in finite geometry and combinatorics (see [25] for a survey).

The differential uniformity of functions f_L has already been studied in the literature: In [7], Berger et al. showed that a function of the form (2) over a field of characteristic 2 can be APN (i.e., differentially 2-uniform) only if L is a monomial, hence the only APN functions f_L are the Gold APN functions (as defined in [18, 23]).

In the case of odd characteristic p, the planarity of functions f_L was first studied by Kyureghyan and Özbudak in [20]. They showed some sufficient conditions on L for f_L being planar as well as some non-existence results for special types of planar functions f_L. However, all of the constructed planar functions were (CCZ-)equivalent to monomials. This study was continued in [14] and [29] by proving some open conjectures on the non-existence raised in [20].

For L being a trinomial of the form $X^{q^2} + aX^q + bX$, Bartoli and Bonini characterized in [1] all planar functions f_L over $\mathbb{F}_{q^3}$ with the restriction $a, b \in \mathbb{F}_q$. Later, Chen and Mesnager [13] completed the characterization for general $a, b \in \mathbb{F}_{q^3}$.

In [11], Budaghyan et al. introduced the notion of an isotopic shift of a function. Given $g\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and a q-polynomial $L \in \mathbb{F}_{q^n}[X]$, the isotopic shift of g by L is defined as the function mapping $x \in \mathbb{F}_{q^n}$ to $g(x + L(x)) - g(x) - g(L(x))$. Hence, the isotopic shifts of $g(x) = x^2$ are exactly the functions of the form $2 \cdot f_L$. In [10], the authors studied isotopic shifts for constructing planar functions and showed that it is possible to have planar functions f_L inequivalent to monomials, more precisely, they obtained functions corresponding (up to equivalence) to commutative Dickson semifields.

For a q-polynomial $L \in \mathbb{F}_{q^n}[X]$, let

$$\mathcal{V}(L) \coloneqq \{a \in \mathbb{F}_{q^n} \mid x \mapsto L(x) - ax \text{ permutes } \mathbb{F}_{q^n}\}$$

and

$$\mathcal{I}(L) \coloneqq \{\frac{L(x)}{x} \mid x \in \mathbb{F}_{q^n}^*\}.$$

The set $\mathcal{I}(L)$ denotes the image set of the rational function $r_L\colon \mathbb{F}_{q^n}^* \to \mathbb{F}_{q^n}, x \mapsto \frac{L(x)}{x}$ and we have $\mathcal{I}(L) = \mathbb{F}_{q^n} \setminus \mathcal{V}(L)$. Those sets played a central role in the study of planarity of f_L and were also studied in previous papers in the context of finite geometry and coding theory, see, e.g., [20, 22, 17] and the references therein. We would like to point out the geometric interpretation in more detail (see, e.g., [16]): Let W be a 2-dimensional $\mathbb{F}_{q^n}$-vector space and let $\Lambda = \mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(1, q^n)$ be the projective line over $\mathbb{F}_{q^n}$. An $\mathbb{F}_q$-*linear set* $\mathcal{L}_U$ of Λ of rank n is defined as the point set of the non-zero points of an n-dimensional $\mathbb{F}_q$-subspace U of W, i.e.,

$$\mathcal{L}_U \coloneqq \{\langle u \rangle_{\mathbb{F}_{q^n}} \mid u \in U \setminus \{0\}\}.$$

If $L \in \mathbb{F}_{q^n}[X]$ is a q-polynomial, we can take $U = U_L \coloneqq \{(x, L(x)) \mid x \in \mathbb{F}_{q^n}\}$ and denote the corresponding linear set $\mathcal{L}_{U_L}$ by $\mathcal{L}_L$. We then have

$$\mathcal{L}_L = \{\langle (1, L(x)/x) \rangle_{\mathbb{F}_{q^n}} \mid x \in \mathbb{F}_{q^n}^{\star}\} = \{\langle (1, y) \rangle_{\mathbb{F}_{q^n}} \mid y \in \mathcal{I}(L)\}.$$

The study of linear sets has also been successfully applied to the study of APN functions. For instance, in [2] the authors analyze certain classes of $\mathbb{F}_2$-linear sets to prove the existence of APN functions of a specific form.

It is known that the planarity property of a function f_L is completely determined by a property (independent of L) of the set $\mathcal{I}(L)$. Indeed, f_L being planar is equivalent to $x \mapsto aL(x) + xL(a)$ having trivial kernel for all $a \in \mathbb{F}_{q^n}^*$, i.e., $-\frac{L(a)}{a} \notin \mathcal{I}(L)$ for all $a \neq 0$, i.e., $0 \notin \mathcal{I}(L)$ and for all $b \in \mathbb{F}_{q^n}^*$, at most one of $-b, b$ is contained in $\mathcal{I}(L)$ (see [20, Thm. 1]). So, if f_L is planar and M a q-polynomial for which $\mathcal{I}(L) = \mathcal{I}(M)$, also f_M is planar. Clearly, for any planar function over $\mathbb{F}_{q^n}$, there is only one possibility of its differential spectrum, i.e., $\eta_1 = q^n(q^n - 1)$ and $\eta_i = 0$ for $i \neq 1$.

One might ask more generally whether the differential uniformity, or even the differential spectrum, of f_L (not necessarily planar) is completely determined by the set $\mathcal{I}(L)$:

Question 1. *If $\mathcal{I}(L) = \mathcal{I}(M)$ for q-polynomials L, M, do f_L and f_M have identical differential spectra?*

The question for which pairs of q-polynomials $L, M \in \mathbb{F}_{q^n}[X]$ the identity $\mathcal{I}(L) = \mathcal{I}(M)$ holds was studied in [17] and a classification was obtained for the case of $n \leq 5$. To recall this result, we need the notion of $\Gamma\mathrm{L}(2, q^n)$-*equivalence* of two q-polynomials, given below. For a function $f\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, we denote by $\mathcal{G}_f$ the *graph of* f, defined as $\{(x, f(x)) \mid x \in \mathbb{F}_{q^n}\}$. The functions f and g are called *CCZ-equivalent* [12], if there is an affine bijection A over $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ such that $A(\mathcal{G}_f) = \mathcal{G}_g$. An important fact is that the differential spectrum of a function is invariant under CCZ-equivalence.

Definition 1 (see, e.g., [17])**.** *Let $s \in \mathbb{F}_{q^n}$, $0 \leq i \leq n-1$. We denote by $\mu_{s,i}$ the $\mathbb{F}_q$-linear mapping $\mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto sx^{q^i}$. Let*

$$\varphi \coloneqq \begin{pmatrix} \mu_{a,i} & \mu_{b,i} \\ \mu_{c,i} & \mu_{d,i} \end{pmatrix} \tag{3}$$

for some elements $a, b, c, d \in \mathbb{F}_{q^n}$ and $0 \leq i \leq n-1$. We say that φ is admissible *for a q-polynomial $L \in \mathbb{F}_{q^n}[X]$ if and only if $ad - bc \neq 0$ (i.e., φ is invertible) and either $b = 0$ or $-(a/b)^{q^{n-i}} \notin \mathcal{I}(L)$. We say that the q-polynomials $L, M \in \mathbb{F}_{q^n}[X]$ are $\Gamma\mathrm{L}(2, q^n)$-equivalent, if there exists an admissible mapping φ for L as in (3) such that L and M (as linear mappings) are CCZ-equivalent via*

$$\varphi(\mathcal{G}_L) = \mathcal{G}_M.$$

In that case, the linear mappings M and L are related via $M = H_L^{\varphi} \circ (K_L^{\varphi})^{-1}$, where $K_L^{\varphi}(x) = ax^{q^i} + bL(x)^{q^i}$ and $H_L^{\varphi}(x) = cx^{q^i} + dL(x)^{q^i}$. We also write $M = \varphi(L)$.

Clearly (see also [17]), if M and L are $\Gamma\mathrm{L}(2, q)$-equivalent via $M = \varphi(L)$, then $|\mathcal{I}(L)| = |\mathcal{I}(\varphi(L))|$. Further, given L and M with $\mathcal{I}(L) = \mathcal{I}(M)$ and admissible φ as in (3), then $\mathcal{I}(\varphi(L)) = \mathcal{I}(\varphi(M))$.

Given a q-polynomial L in the form of (1), we denote by L^* its adjoint, i.e., the q-polynomial

$$L^* \coloneqq a_0 X + \sum_{i=1}^{n-1} a_i^{q^{n-i}} X^{q^{n-i}}.$$

The induced $\mathbb{F}_q$-linear mappings $x \mapsto L(x)$ and $x \mapsto L^*(x)$ over $\mathbb{F}_{q^n}$ are adjoint relative to the bilinear form $(x, y) \mapsto \mathrm{tr}(xy)$, where $\mathrm{tr}\colon x \mapsto \sum_{i=0}^{n-1} x^{q^i}$ denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. That is, $\mathrm{tr}(xL(y)) = \mathrm{tr}(L^*(x)y)$ holds for all $x, y \in \mathbb{F}_{q^n}$ (see, e.g., [22]).

We have now established the necessary terminology to recall the classification result by Csajbók et al.

Theorem 1 ([17])**.** *Let q be a prime power, $n \leq 5$ a positive integer and let $L, M \in \mathbb{F}_{q^n}[X]$ be q-polynomials with maximum field of linearity $\mathbb{F}_q$ (i.e., L or M is not a q^t-polynomial for $t > 1$) such that $\mathcal{I}(L) = \mathcal{I}(M)$.*

- *If $n \leq 4$, there exists $\lambda \in \mathbb{F}_{q^n}^*$ such that $M(X) = L(\lambda X)/\lambda$ or $M(X) = L^*(\lambda X)/\lambda$.*

- *If $n = 5$, then either*
    - *(i) there exists $\lambda \in \mathbb{F}_{q^n}^*$ such that $M(X) = L(\lambda X)/\lambda$ or $M(X) = L^*(\lambda X)/\lambda$, or*
    - *(ii) there exists an admissible mapping φ for L and M and $a, b \in \mathbb{F}_{q^n}$ such that $\varphi(L)(X) = aX^{q^i}$ and $\varphi(M)(X) = bX^{q^j}$ with $a^{\frac{q^n-1}{q-1}} = b^{\frac{q^n-1}{q-1}}$ and $i, j \in \{1, \ldots, 4\}$.*

Since a q-polynomial $L \in \mathbb{F}_{q^n}[X]$ with maximum field of linearity $\mathbb{F}_{q^t}$ is also a q^t-polynomial in $\mathbb{F}_{{q^t}^{n/t}}[X]$ and for $L, M \in \mathbb{F}_{q^n}[X]$ with $\mathcal{I}(L) = \mathcal{I}(M)$, the fields of linearity of L and M coincide [17, Prop. 2.1], this yields the following corollary.

Corollary 1. *Let q be a prime power, $n \leq 5$ a positive integer and let $L, M \in \mathbb{F}_{q^n}[X]$ be q-polynomials such that $\mathcal{I}(L) = \mathcal{I}(M)$. Then,*

(i) there exists $\lambda \in \mathbb{F}_{q^n}^*$ such that $M(X) = L(\lambda X)/\lambda$ or $M(X) = L^*(\lambda X)/\lambda$, or

(ii) there exists an admissible mapping φ for L and M, some integers $i, j \in \{1, \ldots, n-1\}$, and $a, b \in \mathbb{F}_{q^n}$ such that $\varphi(L)(X) = aX^{q^i}$ and $\varphi(M)(X) = bX^{q^j}$.

1.1 Our Results

In the first part (Section 2), we characterize the differential spectrum of a function f_L for a q-polynomial L (Prop. 1). This characterization yields a sufficient condition on a pair (L, M) of q-polynomials such that f_L and f_M have the same differential spectrum, namely that, for all $a \in \mathbb{F}_{q^n}$, the dimension of the kernel of $x \mapsto L(x) - ax$ is the same as the dimension of the kernel of $x \mapsto M(x) - ax$. While this condition is trivially fulfilled if $M(X) = L(\lambda X)/\lambda$ for $\lambda \neq 0$, we outline that it also holds for the pairs of q-polynomials (L, L^*), (aX^{q^i}, bX^{q^j}) with $\mathcal{I}(aX^{q^i}) = \mathcal{I}(bX^{q^j})$, and $(\varphi(L), \varphi(M))$ for L, M fulfilling the condition above (see Lem. 1, Lem. 2, and Lem. 3, respectively).[1] This yields the following result.

Theorem 2. *Let q be a prime power, $n \leq 5$ a positive integer and let $L, M \in \mathbb{F}_{q^n}[X]$ be q-polynomials such that $\mathcal{I}(L) = \mathcal{I}(M)$. Then, $\mathcal{D}_{f_L} = \mathcal{D}_{f_M}$.*

The case of $n > 5$ is left as an open problem. To settle it, we pose the following interesting open question: If $L, M \in \mathbb{F}_{q^n}[X]$ are q-polynomials with $\mathcal{I}(L) = \mathcal{I}(M)$ and $a \in \mathbb{F}_{q^n}$, does this imply the equality of the dimension of the kernel of $x \mapsto L(x) - ax$ and the dimension of the kernel of $x \mapsto M(x) - ax$ (Question 2)?

[1]While the case of (L, L^*) was known before, the other two cases follow from straightforward adaptions of the arguments given in previous literature such as [17].

In Section 3, we show how to construct CCZ-inequivalent functions f_M with bounded differential uniformity from a given function f_L using $\Gamma\mathrm{L}(2,q^n)$-equivalence (Cor. 3) and we further give a link between functions f_L of differential uniformity bounded above by q and scattered q-polynomials (Cor. 4).

2 On the Differential Spectrum of f_L

Given a q-polynomial $L \in \mathbb{F}_{q^n}[X]$, we denote by $\ker(L)$ the kernel of the $\mathbb{F}_q$-linear map $x \mapsto L(x)$ over $\mathbb{F}_{q^n}$, i.e., the subspace of all elements $y \in \mathbb{F}_{q^n}$ with $L(y) = 0$. For $0 \le k \le n$, let us define

$$\mathcal{V}_k(L) \coloneqq \{a \in \mathbb{F}_{q^n} \mid \dim\ker(L(X) - aX) = k\}.$$

Clearly, $\mathcal{V}_0(L) = \mathcal{V}(L)$ and $\cup_{k=1}^{n}\mathcal{V}_k(L) = \mathcal{I}(L)$. Further, note that, for $1 \le k \le n$, we have

$$\mathcal{V}_k(L) = \{b \in \mathcal{I}(L) \mid b = \frac{L(x)}{x} \text{ for exactly } q^k - 1 \text{ distinct } x \in \mathbb{F}_{q^n}^*\}. \tag{4}$$

The sets $\mathcal{V}_k(L)$ for $0 \le k \le n$ have the following interpretation in terms of linear sets: For a point $P = \langle (x,y)\rangle_{\mathbb{F}_{q^n}} \in \mathrm{PG}(1,q^n)$ with $x, y \in \mathbb{F}_{q^n}$, the *weight* of P with respect to the $\mathbb{F}_q$-linear set $\mathcal{L}_L$, denoted by $w_{\mathcal{L}_L}(P)$, is defined as the dimension of the intersection $U_L \cap \langle (x,y)\rangle_{\mathbb{F}_{q^n}}$ as an $\mathbb{F}_q$-vector space. The set $\mathcal{V}_k(L)$ consists precisely of those $y \in \mathbb{F}_{q^n}$ for which $w_{\mathcal{L}_L}(\langle (1,y)\rangle_{\mathbb{F}_{q^n}}) = k$.

The crucial point for the following discussion is the fact that the differential spectrum of f_L is completely determined by $(\mathcal{V}_k(L))_{k=1,\dots,n}$, which we show in the following characterization. For a set S, we denote by $-S$ the set $\{-a \mid a \in S\}$.

Proposition 1. *Let $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial and $f_L\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto xL(x)$. For the differential spectrum $\mathcal{D}_{f_L} = (\eta_0, \eta_1, \dots, \eta_{q^n})$, we have*

$$\eta_i = \begin{cases} q^{n-k} \cdot \sum_{\ell=1}^{n}(q^\ell - 1) \cdot |\mathcal{V}_\ell(L) \cap -\mathcal{V}_k(L)| & \text{if } i = q^k \\ \sum_{k=1}^{n}(q^n - q^{n-k}) \cdot \sum_{\ell=1}^{n}(q^\ell - 1) \cdot |\mathcal{V}_\ell(L) \cap -\mathcal{V}_k(L)| & \text{if } i = 0 \\ 0 & \text{else} \end{cases}. \tag{5}$$

In particular, if $L, M \in \mathbb{F}_{q^n}[X]$ are q-polynomials such that $\mathcal{V}_k(L) = \mathcal{V}_k(M)$ holds for all $1 \le k \le n$, we have $\mathcal{D}_{f_L} = \mathcal{D}_{f_M}$.

Proof. For any $a \in \mathbb{F}_{q^n}$, the differential mapping $x \mapsto f_L(x+a) - f_L(x) = aL(x) + L(a)x + aL(a)$ is affine, hence the solutions $x \in \mathbb{F}_{q^n}$ of $f_L(x+a) - f_L(x) = d$ (if they exist) form a coset of S_a, where S_a is the vector space of solutions $x \in \mathbb{F}_{q^n}$ of $aL(x) + L(a)x = 0$, i.e., $S_a = \ker(aL(X) + L(a)X)$. The solutions exist if and only if $(d - aL(a)) \in \mathrm{Im}(x \mapsto aL(x) + L(a)x)$. From this, we immediately get $\eta_i = 0$ for $i \neq 0$ not being a power of q, and

$$\begin{aligned}
\eta_{q^k} &= q^{n-k} \cdot |\{a \in \mathbb{F}_{q^n}^* \mid \dim\ker(L(X) + \frac{L(a)}{a}X) = k\}| \\
&= q^{n-k} \cdot |\{a \in \mathbb{F}_{q^n}^* \mid -\frac{L(a)}{a} \in \mathcal{V}_k(L)\}| \\
&= q^{n-k} \cdot \sum_{\ell=1}^{n} (q^\ell - 1) \cdot |\{\frac{L(a)}{a} \in \mathcal{V}_\ell(L) \mid -\frac{L(a)}{a} \in \mathcal{V}_k(L)\}| \\
&= q^{n-k} \cdot \sum_{\ell=1}^{n} (q^\ell - 1) \cdot |\mathcal{V}_\ell(L) \cap -\mathcal{V}_k(L)|,
\end{aligned}$$

where the second to last equality holds because $\dot\bigcup_{\ell=1}^{n} \mathcal{V}_\ell(L) = \mathcal{I}(L)$ and each element in $\mathcal{V}_\ell(L)$ has $q^\ell - 1$ preimages under r_L. The identity for η_0 follows from the fact[2] that $\sum_{i=0}^{q^n} \eta_i = \sum_{i=1}^{q^n} i \cdot \eta_i = q^n(q^n - 1)$. Indeed, since $\eta_i = 0$ for positive i not being a power of q, we get $\eta_0 = \sum_{k=1}^{n} (q^k - 1) \cdot \eta_{q^k}$. $\square$

Corollary 2. *Let $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial and $f_L\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, x \mapsto xL(x)$. Then, $\delta_{f_L} = q^k$, where $k \in \{0, \dots, n\}$ is the largest integer such that $|\mathcal{I}(L) \cap -\mathcal{V}_k(L)| \neq \emptyset$, i.e., such that there exists $a \in \mathbb{F}_{q^n}$ for which $L(X) - aX$ is not permutation polynomial and* $\dim\ker(L(X) + aX) = k$.

Proof. Clearly, the differential uniformity of f_L can only be a power of q. From Prop. 1, the value η_{q^k} is nonzero if and only if $\bigcup_{\ell=1}^{n} (\mathcal{V}_\ell(L) \cap -\mathcal{V}_k(L))$ is not empty. The statement follows from the fact that $\mathcal{I}(L) = \cup_{\ell=1}^{n} \mathcal{V}_\ell(L)$. $\square$

Remark 1. Proposition 1 and Cor. 2 generalize [20, Thm. 1 (c)]. Indeed f_L is planar if and only if $\eta_{q^k} = 0$ holds for all $1 \leq k \leq n$. By Cor. 2, this condition is equivalent to $\mathcal{I}(L) \cap -\mathcal{I}(L) = \emptyset$, i.e., $0 \notin \mathcal{I}(L)$ and for all $b \in \mathbb{F}_{q^n}^*$, at most one of b or $-b$ is contained in $\mathcal{I}(L)$.

It was first proven in [3, Lem. 2.6] that $\mathcal{V}(L) = \mathcal{V}(L^*)$ and $\mathcal{I}(L) = \mathcal{I}(L^*)$. There are various other proofs given in the literature, e.g., in [22], which uses the characterization of permutations by their Walsh transforms. A particularly elegant proof was given in [16, Rem. 3.3], proving the (a priori) more general question of equality of $\mathcal{V}_k(L)$ and $\mathcal{V}_k(L^*), 0 \leq k \leq n$. For completeness, we repeat this proof in the following.

Lemma 1 (see [16])**.** *Let $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial. For all $0 \leq k \leq n$, we have $\mathcal{V}_k(L) = \mathcal{V}_k(L^*)$.*

Proof. For a q-polynomial $L = \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$, let

$$D_L \coloneqq \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1}^q & a_0^q & \dots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \dots & a_0^{q^{n-1}} \end{pmatrix}$$

[2] This identity proved to be quite useful for studying differential spectra of APN monomial functions over finite fields, see, e.g., [27].

denote the corresponding $n \times n$ Dickson matrix over $\mathbb{F}_{q^n}$, so that $\ker(D_L) = \ker(L)$ and $(D_L)^\top = D_{L^*}$ (see [28]). The statement follows since, for any $a \in \mathbb{F}_{q^n}$, we have

$$\begin{aligned}\dim\ker(L(X) - aX) &= \dim\ker(D_L - D_{aX}) = \dim\ker((D_L - D_{aX})^\top) \\ &= \dim\ker(D_{L^*} - D_{aX}) = \dim\ker(L^*(X) - aX).\end{aligned}$$

□

Remark 2. Let $\zeta \in \mathbb{C}$ be a primitive p-th root of unity. The *Walsh transform* of $f\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ at point (a,b), $a, b \in \mathbb{F}_{q^n}$, is defined as

$$\mathcal{W}_f(a,b) \coloneqq \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{tr}_p(ax) + \mathrm{tr}_p(bf(x))} \in \mathbb{C},$$

where $\mathrm{tr}_p(x) \coloneqq \sum_{i=0}^{mn-1} x^{p^i}$ denotes the absolute trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_p$. Let $a \in \mathbb{F}_{q^n}, b \in \mathbb{F}_{q^n}^*$. For the Walsh transform of f_L and f_{L^*}, we get

$$\begin{aligned}\mathcal{W}_{f_L}(a,b) &= \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{tr}_p(ax) + \mathrm{tr}_p(bxL(x))} = \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{tr}_p(ax) + \mathrm{tr}_p(xL^*(bx))} \\ &= \sum_{x \in \mathbb{F}_{q^n}} \zeta^{\mathrm{tr}_p(ab^{-1}x) + \mathrm{tr}_p(b^{-1}xL^*(x))} = \mathcal{W}_{f_{L^*}}(ab^{-1}, b^{-1}).\end{aligned}$$

Since a function f over $\mathbb{F}_{q^n}$ is a permutation if and only if $\mathcal{W}_f(0,b) = 0$ holds for all $b \in \mathbb{F}_{q^n}^*$ (see, e.g., [19, Thm. 1.1]), we immediately get that f_L is a permutation if and only if f_{L^*} is. □

By a folklore argument, we get the following for q-monomials.

Lemma 2. *Let $L = aX^{q^i}$ and $M = bX^{q^j}$, $a, b \in \mathbb{F}_{q^n}$, be q-polynomials in $\mathbb{F}_{q^n}[X]$ such that $\mathcal{V}(L) = \mathcal{V}(M)$. Then, for all $0 \le k \le n$, we have $\mathcal{V}_k(L) = \mathcal{V}_k(M)$. More precisely, if $a, b \in \mathbb{F}_{q^n}^*$, we have $\mathcal{V}(L)_{\gcd(i,n)} = \mathcal{I}(L)$, and $\mathcal{V}_k(L) = \emptyset$ for $k \notin \{0, \gcd(i,n)\}$.*

Proof. If $a = 0$, then also $b = 0$, so that $L = M$. Let us therefore assume $a, b \in \mathbb{F}_{q^n}^*$. It is well known that a monomial function $x \mapsto x^d$ over $\mathbb{F}_{q^n}^*$ is $\gcd(d, q^n - 1)$-to-1. By assumption, we have

$$\mathcal{I}(L) = \{ax^{p^i - 1} \mid x \in \mathbb{F}_{q^n}^*\} = \{bx^{p^j - 1} \mid x \in \mathbb{F}_{q^n}^*\} = \mathcal{I}(M),$$

hence the mappings $x \mapsto x^{q^i - 1}$ and $x \mapsto x^{q^j - 1}$ over $\mathbb{F}_{q^n}^*$ have the same image size and are thus $\gcd(q^i - 1, q^n - 1)$-to-one. By using (4) and the fact that $\gcd(q^i - 1, q^n - 1) = q^{\gcd(i,n)} - 1$, the result follows. □

To settle Thm. 2, we finally show that the property of equality of sets $\mathcal{V}_k(L)$, $\mathcal{V}_k(M)$ is not affected when changing L, M under $\Gamma\mathrm{L}(2, q^n)$-equivalence using the same φ. We can show more generally how the sets $\mathcal{V}_k(L), k = 1, \ldots, n$ are affected under $\Gamma\mathrm{L}(2, q^n)$-equivalence of L.

Lemma 3. *Let $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial and let φ be an admissible mapping for L. Let $1 \leq k \leq n$. The sets $\mathcal{V}_k(L)$ and $\mathcal{V}_k(\varphi(L))$ are related via a bijection $\nu_\varphi \colon \mathcal{I}(\varphi(L)) \to \mathcal{I}(L)$ by*

$$\nu_\varphi^{-1}(\mathcal{V}_k(L)) = \mathcal{V}_k(\varphi(L)).$$

In particular, we have $|\mathcal{V}_k(L)| = |\mathcal{V}_k(\varphi(L))|$, and, for a q-polynomial $M \in \mathbb{F}_{q^n}[X]$ with $\mathcal{I}(M) = \mathcal{I}(L)$ and $\mathcal{V}_k(M) = \mathcal{V}_k(L)$, we have $\mathcal{V}_k(\varphi(M)) = \mathcal{V}_k(\varphi(L))$.

Proof. Let

$$\varphi = \begin{pmatrix} \mu_{a,i} & \mu_{b,i} \\ \mu_{c,i} & \mu_{d,i} \end{pmatrix}$$

be admissible for L and let us fix $k \geq 1$ and let $\gamma \in \mathcal{V}_k(\varphi(L))$. We have

$$\begin{aligned} &|\{x \in \mathbb{F}_{q^n} \mid \varphi(L)(x) - \gamma x = 0\}| = |\{x \in \mathbb{F}_{q^n} \mid H_L^\varphi(x) - \gamma K_L^\varphi(x) = 0\}| \\ =&|\{x \in \mathbb{F}_{q^n} \mid (d-\gamma b)^{q^{n-i}} L(x) - (\gamma a - c)^{q^{n-i}} x = 0\}|, \end{aligned}$$

which is equal to

$$|\{x \in \mathbb{F}_{q^n} \mid L(x) - \left(\frac{\gamma a - c}{d - \gamma b}\right)^{q^{n-i}} x = 0\}|$$

if $d - \gamma b \neq 0$. Since $k \neq 0$, necessarily $d - \gamma b \neq 0$, as otherwise $(d-\gamma b)^{q^{n-i}} L(x) - (\gamma a - c)^{q^{n-i}} x = 0$ would only have one solution $x = 0$ (note that both $d - \gamma b$ and $\gamma a - c$ cannot be simultaneously zero because of the invertibility of φ). Since $ad - bc \neq 0$, the mapping

$$\nu_\varphi \colon x \mapsto \left(\frac{xa - c}{d - xb}\right)^{q^{n-i}}$$

is injective with domain $\mathbb{F}_{q^n} \setminus \{x \in \mathbb{F}_{q^n} \mid d - xb = 0\}$, hence it induces a bijection from $\mathcal{I}(\varphi(L))$ to $\mathcal{I}(L)$. The first part of the assertion follows, as we have shown $\nu_\varphi(\gamma) \in \mathcal{V}_k(L)$. The second part is a trivial corollary. Note that we need $\mathcal{I}(M) = \mathcal{I}(L)$ to ensure that φ is admissible for M. $\square$

The above Lem. 1, Lem. 2, and Lem. 3, together with Thm. 1 imply Thm. 2 and thus completely settle Question 1 for the case of $n \leq 5$.

An interesting open question is whether the sets $\mathcal{V}_k(L)$, $k = 1, \ldots, n$ are completely determined from $\mathcal{I}(L)$ (equivalently from $\mathcal{V}(L)$) in general.

Question 2. *Let $L, M \in \mathbb{F}_{q^n}[X]$ be q-polynomials with $\mathcal{V}(L) = \mathcal{V}(M)$. Does this imply $\mathcal{V}_k(L) = \mathcal{V}_k(M)$ for all $k \in \{1, \ldots, n\}$?*

In terms of linear sets, the question is equivalent to asking whether the weights of $\langle (1,y) \rangle_{\mathbb{F}_{q^n}}$ with respect to the linear set $\mathcal{L}_L$ are completely determined by the points $\langle (1,y) \rangle_{\mathbb{F}_{q^n}}$ of weight $w_{\mathcal{L}_L}(\langle (1,y) \rangle_{\mathbb{F}_{q^n}}) = 0$. Answering this question affirmatively immediately gives a positive answer to Question 1.

Remark 3. Besides the pairs of q-polynomials (L, L^*), (aX^{q^i}, bX^{q^j}) fulfilling $\mathcal{I}(aX^{q^i}) = \mathcal{I}(bX^{q^j})$, and $(\varphi(L), \varphi(M))$ with $\mathcal{I}(L) = \mathcal{I}(M)$, Question 2 also has an affirmative answer when one of L or M corresponds to the trace function $x \mapsto \mathrm{tr}(x)$. This follows immediately from the fact that for a q-polynomial M with $\mathcal{I}(M) = \mathcal{I}(\mathrm{tr}(X))$, we have $M = \mathrm{tr}(\lambda X)/\lambda$ for $\lambda \neq 0$, as proven in [16, Thm. 3.7] (see also [17, Thm. 1.3]).

3 Bounded Differential Uniformity and Scattered q-Polynomials

Using Cor. 2, a simple upper bound on the differential uniformity of f_L can be given based on the emptiness of sets $\mathcal{V}_k(L)$. That is, if $k \in \{1, \ldots, n\}$ is the largest integer such that $\mathcal{V}_k(L) \neq \emptyset$, the differential uniformity of f_L is bounded above by q^k. Moreover, for the case of $p = 2$, we have $-\mathcal{V}_k(L) = \mathcal{V}_k(L) \subseteq \mathcal{I}(L)$. Hence, for $p = 2$, the differential uniformity is *equal* to q^k.

Then, from Lem. 3, it follows that we obtain functions of bounded differential uniformity from f_L if we stay in the same $\Gamma\mathrm{L}(2, q^n)$-equivalence class.

Corollary 3. *Let $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial and let $k \in \{1, \ldots, n\}$ be the largest integer such that $\mathcal{V}_k(L) \neq \emptyset$. For any mapping φ admissible for L, the differential uniformity of $f_{\varphi(L)}$ is bounded above by q^k.*

For odd values of p, this allows us to obtain functions f_M with different differential spectra (hence CCZ-inequivalent to each other), but $\delta_{f_M} \leq q^k$, from M within the $\Gamma\mathrm{L}(2, q^n)$-equivalence class of L (an example is given in Example 1 below). However, in even characteristic, we do not leave the extended-affine equivalence class of f_L (and hence cannot obtain distinct differential spectra), as the following lemma states. Note that two functions $f, g\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ are *extended-affine equivalent (EA-equivalent)* if there exist affine bijections $A, B\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and an affine function $C\colon \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ such that $g = B \circ f \circ A + C$. In case that A and B are also linear and $C = 0$, the functions f and g are called *linear-equivalent*. Since EA-equivalence is a special case of CCZ-equivalence, two EA-equivalent functions have the same differential spectrum.

Lemma 4. *Let $p = 2$ and $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial. Let φ be an admissible mapping for L as in (3). Then, f_L and $f_{\varphi(L)}$ are EA-equivalent.*

Proof. $f_{\varphi(L)}$ corresponds to the mapping $x \mapsto x \cdot H_L^{\varphi}({K_L^{\varphi}}^{-1}(x))$, which is linear-equivalent to $x \mapsto K_L^{\varphi}(x) \cdot H_L^{\varphi}(x)$. Now, we have

$$K_L^{\varphi}(x) \cdot H_L^{\varphi}(x) = (ad + bc) \cdot (xL(x))^{q^i} + ac \cdot x^{2q^i} + bd \cdot L(x)^{2q^i},$$

which is linear-equivalent to

$$xL(x) + (ad + bc)^{-q^{-i}}((ac)^{q^{-i}} \cdot x^2 + (bd)^{q^{-i}} \cdot L(x)^2).$$

Note that, since $p = 2$, we have $ad + bc = ad - bc \neq 0$ because φ is admissible for L. Moreover, since $p = 2$, the mapping $x \mapsto (ad + bc)^{-q^{-i}}((ac)^{q^{-i}} \cdot x^2 + (bd)^{q^{-i}} \cdot L(x)^2)$ is linear, hence $f_{\varphi(L)}$ is EA-equivalent to f_L. $\square$

Remark 4. Let $\gamma \in \mathbb{F}_{q^n}$ and $1 \leq k \leq n$. Then, $\gamma \in \mathcal{I}(\varphi(L))$ and $-\gamma \in \mathcal{V}_k(\varphi(L))$ if and only if $\nu_\varphi(\gamma) \in \mathcal{I}(L)$ and $\nu_\varphi(-\gamma) \in \mathcal{V}_k(L)$. Hence, by Cor. 2, the functions f_L and $f_{\varphi(L)}$ have the same differential uniformity if $\nu_\varphi(-\gamma) = -\nu_\varphi(\gamma)$ holds for all $\gamma \in \mathbb{F}_{q^n}$ with $\gamma \in \mathcal{I}(\varphi(L))$. This condition is equivalent to $ab\gamma^2 - cd = 0$ for all $\gamma \in \mathcal{I}(\varphi(L))$. Hence, a generic choice of φ preserving differential uniformity is such that $a = d = 0$ or $b = c = 0$. But then, f_L and $f_{\varphi(L)}$ are linear-equivalent.

The q-polynomials L such that $\mathcal{V}_k(L) = \emptyset$ for all $k > 1$ are called *scattered q-polynomials* [26]. They are widely studied as they have applications in finite geometry (in terms of *maximum scattered linear sets*) and coding theory (in terms of *rank distance codes* [26]), see [21] and the references therein. It is well known that a q-polynomial $L \in \mathbb{F}_{q^n}[X]$ is scattered if and only if $\mathcal{I}(L)$ is of maximal size, i.e., $|\mathcal{I}(L)| = \frac{q^n-1}{q-1}$. Indeed, $\mathcal{I}(L)$ is of maximal size if and only if each element $\frac{L(y)}{y} \in \mathcal{I}(L)$ has $q-1$ preimages $x = cy$ with $c \in \mathbb{F}_q^*$. This yields an affirmative answer to Question 1 and Question 2 for those L, M for which $\mathcal{V}(L)$ and $\mathcal{V}(M)$ have size $q^n - \frac{q^n-1}{q-1}$. There are only a few known instances and families of scattered q-polynomials, see e.g., the list in [4, Section 1]. The best known family of scattered q-polynomials are the monomials X^{q^s} with $\gcd(s, n) = 1$. Bartoli and Zhou [5] showed that those monomials are the only exceptional scattered (of index 0) monic q-polynomials, i.e., the only monic q-polynomials that are scattered over infinitely many extensions of $\mathbb{F}_q$.

For scattered q-polynomials, we get the following immediate corollaries from Prop. 1 and Cor. 3, respectively.

Corollary 4. *Let $L \in \mathbb{F}_{q^n}[X]$ be a q-polynomial. If L is scattered, the differential uniformity of f_L is bounded above by q and, for $\mathcal{D}_{f_L} = (\eta_i)_{i=0,\dots,q^n}$, we have $\eta_i = 0$ for $i \notin \{0, 1, q\}$ and*

$$\begin{aligned}
\eta_q &= q^{n-1}(q-1) \cdot |\mathcal{I}(L) \cap -\mathcal{I}(L)| \\
\eta_1 &= q^n \cdot (q-1) \cdot |\mathcal{I}(L) \cap -\mathcal{V}(L)| \\
\eta_0 &= q^{n-1}(q-1)^2 \cdot |\mathcal{I}(L) \cap -\mathcal{I}(L)|.
\end{aligned}$$

If $p = 2$, the differential uniformity of f_L is equal to q if and only if L is scattered.

Corollary 5. *Let $L \in \mathbb{F}_{q^n}[X]$ be a scattered q-polynomial and let φ be an admissible mapping for L as in (3). Then, $\delta_{f_{\varphi(L)}} \leq q$.*

This corollary is a consequence of the fact that the property of a q-polynomial in $\mathbb{F}_{q^n}[X]$ being scattered is invariant under $\Gamma\mathrm{L}(2, q^n)$-equivalence.

Example 1. Consider $q = p$ for an odd prime p and let $L = X^{p^s} \in \mathbb{F}_{p^n}[X]$ for s with $\gcd(s, n) = 1$. Then, $f_L \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, x \mapsto x^{p^s+1}$ is planar if and only if n

is odd [15]. Since L is scattered, f_L has differential uniformity of p if n is even. Let $a \in \mathbb{F}_{q^n}^*$. The mapping

$$\varphi := \begin{pmatrix} \mu_{1,0} & 0 \\ \mu_{L(a),0} & \mu_{a,0} \end{pmatrix}$$

is admissible for L. Then, $\varphi(L)(x) = H_L^{\varphi}((K_L^{\varphi})^{-1}(x))$ with $H_L^{\varphi}(x) = ax^{p^s} + a^{p^s}x$ and $K_L^{\varphi}(x) = x$, so $\varphi(L) = aX^{p^s} + a^{p^s}X = f_L(X+a) - f_L(X) - f_L(a)$ (which is also scattered). Hence, the differential uniformity of $f_{\varphi(L)} \colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, x \mapsto ax^{p^s+1} + a^{p^s}x^2$ is bounded above by p. Note that, for each $a \in \mathbb{F}_{q^n}^*$, the function $f_{\varphi(L)}$ is linear-equivalent to $x \mapsto x^{p^s+1} + x^2$. We experimentally checked that, for $p \in \{3,5,7\}$, $n \in \{2,3,4,5\}$ and $\gcd(s,n) = 1$, the differential uniformity of $x \mapsto x^{p^s+1} + x^2$ is indeed equal to p.

In the following example, we illustrate that it is possible to get a variety of distinct differential spectra for $f_{\varphi(L)}$ when L is a scattered q-polynomial and φ and admissible mapping for L (in the case where q is odd).

Example 2. Again, we consider the scattered polynomial $L = X^{p^s} \in \mathbb{F}_{p^n}[X]$, but for $p = n = 3$ and $s = 1$ fixed. Hence, f_L is planar, so the differential spectrum is $\mathcal{D}_{f_L} = (0, 702, 0, 0, 0)$. Generating several admissible mappings φ for L, we obtain the following six additional differential spectra for $f_{\varphi(L)}$: (252,324,126,0,0), (144,486,72,0,0), (288,270,144,0,0), (180,432,90,0,0), (216,378,108,0,0), and (468,0,234,0,0).

In general, it would be interesting to classify all possible differential spectra of $f_{\varphi(L)}$ for admissible mappings φ for L, for a given scattered q-polynomial L and to understand whether a scattered q-polynomial L can yield CCZ-inequivalent planar functions $f_{\varphi(L)}$.

Remark 5. It was proven in [7, Thm. 6] that an APN function f_L for $L = \sum_{i=1}^{n-1} a_i X^{2^i} \in \mathbb{F}_{2^n}[X]$ is APN (i.e., $\delta_{f_L} = 2$) if and only if L is a monomial aX^{2^k} with $\gcd(k,n) = 1$, $a \in \mathbb{F}_{2^n}^*$. To obtain this result, the authors of [7] proved that f_L is APN if and only if r_L is a permutation of $\mathbb{F}_{2^n}^*$, i.e., if and only if $|\mathcal{I}(L)| = 2^n - 1$, i.e., if and only if L is scattered. This is a special case of Cor. 4. They then used the fact that r_L can only be a permutation if L is a monomial, as already proven by Payne [24] and by the authors in [6] using Hermite's criterion.

This means that *any scattered* 2*-polynomial is is necessarily a monomial.* Note that there exist more instances of scattered q-polynomials for q being a larger power of 2, see, e.g., [4].

Acknowledgment. The author thanks the anonymous reviewers for their helpful comments and Daniele Bartoli for a discussion on the problem stated in Question 2.

The author was funded by Deutsche Forschungsgemeinschaft (DFG) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

[1] D. Bartoli and M. Bonini. Planar polynomials arising from linearized polynomials. *J. Algebra Its Appl.*, 21(01):2250002, 2022.

[2] D. Bartoli, M. Calderini, O. Polverino, and F. Zullo. On the infiniteness of a family of APN functions. *J. Algebra*, 598:68–84, 2022.

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

[4] D. Bartoli, G. Longobardi, G. Marino, and M. Timpanella. Scattered trinomials of $\mathbb{F}_{q^6}[x]$ in even characteristic. *Finite Fields Their Appl.*, 97:102449, 2024.

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

[6] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear mappings over $\mathbf{F}_2^n$. In *Proceedings of the 2005 IEEE International Symposium on Information Theory, ISIT 2005, Adelaide, South Australia, Australia, 4-9 September 2005*, pages 2002–2006. IEEE, 2005.

[7] T. P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbf{F}_2^n$. *IEEE Trans. Inf. Theory*, 52(9):4160–4170, 2006.

[8] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *J. Cryptol.*, 4(1):3–72, 1991.

[9] C. Blondeau, A. Canteaut, and P. Charpin. Differential properties of power functions. *Int. J. Inf. Coding Theory*, 1(2):149–170, 2010.

[10] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa. On isotopic shift construction for planar functions. In *IEEE International Symposium on Information Theory, ISIT 2019, Paris, France, July 7-12, 2019*, pages 2962–2966. IEEE, 2019.

[11] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa. Constructing APN functions through isotopic shifts. *IEEE Trans. Inf. Theory*, 66(8):5299–5309, 2020.

[12] C. Carlet, P. Charpin, and V. A. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[13] R. Chen and S. Mesnager. Binomials and trinomials as planar functions on cubic extensions of finite fields. *CoRR*, abs/2303.09229, 2023.

[14] R. S. Coulter and M. Henderson. On a conjecture on planar polynomials of the form $X(\mathrm{tr}_n(X)\text{-}uX)$. *Finite Fields Their Appl.*, 21:30–34, 2013.

[15] R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.

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

[17] B. Csajbók, G. Marino, and O. Polverino. A Carlitz type result for linearized polynomials. *Ars Math. Contemp.*, 16(2):585–608, 2019.

[18] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Trans. Inf. Theory*, 14(1):154–156, 1968.

[19] X. Hou. Permutation polynomials over finite fields - A survey of recent advances. *Finite Fields Their Appl.*, 32:82–119, 2015.

[20] G. M. M. Kyureghyan and F. Özbudak. Planarity of products of two linearized polynomials. *Finite Fields Their Appl.*, 18(6):1076–1088, 2012.

[21] G. Longobardi and C. Zanella. Linear sets and mrd-codes arising from a class of scattered linearized polynomials. *J. Algebr. Comb.*, 53:639–661, 2021.

[22] G. McGuire and J. Sheekey. Linearized polynomials and their adjoints, and some connections to linear sets and semifields. In J. Bajard and A. Topuzoglu, editors, *Arithmetic of Finite Fields - 8th International Workshop, WAIFI 2020, Rennes, France, July 6-8, 2020, Revised Selected and Invited Papers*, volume 12542 of *LNCS*, pages 37–41. Springer, 2020.

[23] K. Nyberg. Differentially uniform mappings for cryptography. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Proceedings*, volume 765 of *LNCS*, pages 55–64. Springer, 1993.

[24] S. E. Payne. A complete determination of translation ovoids in finite desarguian planes. *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti*, 51(5):328–331, 1971.

[25] A. Pott. Almost perfect and planar functions. *Des. Codes Cryptogr.*, 78(1):141–195, 2016.

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

[27] X. Tan and H. Yan. Differential spectrum of a class of APN power functions. *Des. Codes Cryptogr.*, 91(8):2755–2768, 2023.

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

[29] M. Yang, S. Zhu, and K. Feng. Planarity of mappings $x(Tr(x) - \frac{\alpha}{2}x)$ on finite fields. *Finite Fields Their Appl.*, 23:1–7, 2013.