Planar products of linearized polynomials

Gohar Kyureghyan, Ferruh Ozbudak

Planar products of linearized polynomials

Gohar M. Kyureghyan[1] and Ferruh Özbudak[2]

[1] Department of Mathematics, Otto-von-Guericke University of Magdeburg, Universitätsplatz 2, 39106 Magdeburg, Germany
gohar.kyureghyan@ovgu.de

[2] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. Let $L_1(x)$ and $L_2(x)$ be linearized polynomials over $\mathbb{F}_{q^n}$. We determine conditions when the product $L_1(x) \cdot L_2(x)$ is a planar mapping on $\mathbb{F}_{q^n}$. For a linearized polynomial L over $\mathbb{F}_{q^n}$, let $\mathcal{M}(L) = \{\alpha \in \mathbb{F}_{q^n} : L(x) + \alpha \cdot x$ is bijective on $\mathbb{F}_{q^n}\}$. We show that the planarity of the product $L_1(x) \cdot L_2(x)$ is linked with the set $\mathcal{M}(L)$ of a suitable linearized polynomial L. We use this relation to describe some families of such planar mappings and we give some nonexistence results.

Keywords: planar mapping, quadratic mapping, Dembowski-Ostrom polynomial, linearized polynomial, directions defined by linear functions

1 Introduction

Let p be an odd prime number and q a power of p. Given a mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ and a nonzero element $a \in \mathbb{F}_{q^n}$, we call

$$D_{f,a} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \quad x \mapsto f(x+a) - f(x) - f(a)$$

the difference mapping of f defined by a. A mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is called planar (or perfect nonlinear) if all its difference mappings are bijective. Planar mappings were introduced in [7] as a tool to construct projective spaces. In Cryptology planar mappings are called perfectly nonlinear, and they provide the optimal resistance to differential attacks [16]. In [8], [9], planar mappings are used to construct optimal constant-composition codes and signal sets. Planar mappings do not exist in finite fields of even characteristic. A mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called almost perfect nonlinear (APN) if every difference mapping of it has an image set of the maximal possible cardinality 2^{n-1}.

The q-weight of a nonnegative integer m is the sum of the digits in its q-adic representation, i.e. if $m = \sum_i b_i q^i$ then the q-ary weight of m is $\sum_i b_i \in \mathbb{Z}$. Recall, that any mapping of $\mathbb{F}_{q^n}$ can be represented by a polynomial over $\mathbb{F}_{q^n}$ of degree less than q^n. Moreover, different such polynomials define different mappings. This allows us to identify the set of mappings of $\mathbb{F}_{q^n}$ with the set of polynomials over

$\mathbb{F}_{q^n}$ with degree less than q^n. We use the notation $F(X)$ to denote a polynomial, while $F(x)$ is used for the mapping induced by $F(X)$. The algebraic q-degree of a polynomial over $\mathbb{F}_{q^n}$ is the maximal q-weight of the exponents in its terms. We use briefly the term algebraic degree, since q is fixed all over the paper.

The $\mathbb{F}_q$-linear mappings $L : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ are represented by the polynomials of algebraic degree 1 with the zero constant term, that is $L(x) = \sum_{i=0}^{n-1} c_i x^{q^i}$, $c_i \in \mathbb{F}_{q^n}$. Such polynomials are called linearized or q-polynomials. The affine mappings are given by the polynomials of algebraic degree 1.

Two mappings $F, G : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ are called extended affine equivalent (EA-equivalent), if $G = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and an affine mapping A. EA-equivalent non-constant mappings have the same algebraic degree. It is easy to see that EA-equivalence preserves the planarity of mappings.

A mapping is called quadratic if it is represented by a polynomial of algebraic degree 2. The polynomials of algebraic degree 2 with no terms of algebraic degree 1,

$$\sum_{i,j=0}^{n-1} a_{i,j} x^{q^i + q^j}, \ a_{i,j} \in \mathbb{F}_{q^n},$$

are called Dembowski-Ostrom polynomials in [6]. Observe that any quadratic mapping is EA-equivalent to a one represented by a Dembowski-Ostrom polynomial. Dembowski-Ostrom planar polynomials describe finite commutative semifields and vice-versa [7, 5].

In this paper we continue the study of products of linearized polynomials. To our knowledge such polynomials were first considered in [2]. In [2, 12] bijectivness of these polynomials is studied. APN products of linearized polynomials are considered in [3], where it is shown that if $X \cdot L(X)$ is APN with a linearized polynomial $L(X)$ then $L(X)$ must be a monomial. In this paper we investigate the planar products of linearized polynomials. In particular we observe that to contrary to the APN case there are planar polynomials $X \cdot L(X)$ with a non-monomial linearized polynomial $L(X)$.

2 Planar products of linearized polynomials

Proposition 1. *Let L_1, $L_2 \in \mathbb{F}_{q^n}[X]$ be linearized polynomials. If the mapping $L_1 \cdot L_2 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is planar, then necessarily the mappings L_1 and L_2 are bijective on $\mathbb{F}_{q^n}$.*

Proof. Observe that $L_1(X) \cdot L_2(X)$ is a Dembowski-Ostrom polynomial. In [14, 18] it is shown that the only zero of a planar Dembowski-Ostrom polynomial is $X = 0$, which yields the statement. $\square$

The next proposition shows that the study of planar polynomials of shape $L_1(X) \cdot L_2(X)$ can be reduced to the one of shape $X \cdot L(X)$.

Proposition 2. *Let L_1, $L_2 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be $\mathbb{F}_q$-linear. Then $L_1(x) \cdot L_2(x)$ is planar on $\mathbb{F}_{q^n}$ if and only if $x \cdot L_1(L_2^{-1}(x))$ is planar on $\mathbb{F}_{q^n}$, where $L_2^{-1}(x)$ is the inverse mapping of L_2.*

Proof. The mappings $L_1(x) \cdot L_2(x)$ is EA-equivalent to $x \cdot L_1(L_2^{-1}(x))$, since

$$(L_1(x) \cdot L_2(x)) \circ L_2^{-1}(x) = L_1(L_2^{-1}(x)) \cdot L_2(L_2^{-1}(x)) = L_1(L_2^{-1}(x)) \cdot x. \qquad \Box$$

For any linearized polynomial $L(X)$ over $\mathbb{F}_{q^n}$ we define the polynomial Q_L by

$$Q_L(X) := \frac{L(X)}{X}.$$

Lemma 1. *Let $L(X) \in \mathbb{F}_{q^n}[X]$ be a linearized permutation polynomial. The mapping $x \cdot L(x)$ is planar on $\mathbb{F}_{q^n}$ if and only if, for any non-zero $\beta \in \mathbb{F}_{q^n}$, at most one of β or $-\beta$ belongs to the set $\{Q_L(x) : x \in \mathbb{F}_{q^n}^*\}$.*

Proof. Consider

$$D_a(x) = (x+a)L(x+a) - xL(x) - aL(a) = aL(x) + xL(a).$$

Since $D_a(x)$ is a linear mapping, it is bijective if and only if it has a trivial kernel. It remains to note that the condition $aL(x) + xL(a) = 0$ if and only if $x = 0$ is equivalent to

$$\frac{L(x)}{x} \neq -\frac{L(a)}{a}$$

for any non-zero $a, x \in \mathbb{F}_{q^n}$. $\Box$

Further we show that the planarity of $X \cdot L(X)$ is linked with the set

$$\mathcal{M}(L) = \{\alpha \in \mathbb{F}_{q^n} : L(x) + \alpha \cdot x \text{ is bijective on } \mathbb{F}_{q^n}\}.$$

Theorem 1. *Let $L(X) \in \mathbb{F}_{q^n}[X]$ be linearized. The mapping $x \cdot L(x)$ is planar on $\mathbb{F}_{q^n}$ if and only if $0 \in \mathcal{M}(L)$ and at least one of β or $-\beta$ belongs to the set $\mathcal{M}(L)$ for any non-zero $\beta \in \mathbb{F}_{q^n}$.*

Proof. The condition $0 \in \mathcal{M}(L)$ states that $L(x)$ is bijective on $\mathbb{F}_{q^n}$. Using Lemma 1, for any non-zero $\beta \in \mathbb{F}_{q^n}$ it must hold that either β or $-\beta$ is not contained in $\{Q_L(x) : x \in \mathbb{F}_{q^n}^*\}$. The proof now follows from the observation that $\beta \notin \{Q_L(x) : x \in \mathbb{F}_{q^n}^*\}$ if and only if $L(x) - \beta \cdot x$ is bijective on $\mathbb{F}_{q^n}$. $\Box$

Note that the monomial planar mappings x^2 and x^{q^i+1} on $\mathbb{F}_{q^n}$ with $n/\gcd(n,i)$ odd are covered by Theorem 1. The conditions of Theorem 1 are trivially fulfilled for x^2. In the case $x \cdot x^{q^i}$ it is easy to see, that there is no β such that both $x^{q^i} + \beta x$ and $x^{q^i} - \beta x$ are not bijective on $\mathbb{F}_{q^n}$ if and only if -1 is not a $(q^i - 1)$th power in $\mathbb{F}_{q^n}$, or equivalently $n/\gcd(n,i)$ odd.

In [3] it is shown that if $X \cdot L(X)$ is APN with a linearized polynomial $L(X)$ then $L(X)$ must be a monomial. Does a similar result hold for planar products $X \cdot L(X)$? The answer is negative as the following observation shows.

Proposition 3. *Let $1 \leq k \leq n-1$ with $n/\gcd(n,k)$ odd and let $u \in \mathbb{F}_{q^n}$ be not a (q^k-1)st power in $\mathbb{F}_{q^n}$. Then the mapping $F(x) = x \cdot (x^{q^{n-k}} - ux^{q^k})$ is planar on $\mathbb{F}_{q^n}$.*

Proof. We show that $F(x)$ is EA-equivalent to the planar monomial x^{q^k+1}. Indeed,

$$F(x) = x^{q^{n-k}+1} - u\,x^{q^k+1} = (x^{q^{n-k}} - u\,x) \circ x^{q^k+1},$$

and the assumtions on k and u ensure that $x^{q^{n-k}} - u\,x$ is bijective and x^{q^k+1} is planar.

Our next goal is to describe further families of planar products $X \cdot L(X)$ using Theorem 1. To our knowledge the only linearized polynomials L for which the sets $\mathcal{M}(L)$ are known are X, $X^{q^k} - uX$, $Tr(X) = X + X^q + \ldots + X^{q^{n-1}}$ or some natural transformations of these polynomials.

Open Problem. Find new families of linearized permutation polynomials L with $|\{\beta, -\beta\} \cap \mathcal{M}(L)| \geq 1$ for any $\beta \in \mathbb{F}_{q^n}$.

The next result was proved in [10, 11] by different approaches. In [10] it is shown that the mappings of Theorem 2 can be obtained from the mapping $x \mapsto x^2$ via EA-equivalence. We show that this result can be proved by using Theorem 1 as well.

Theorem 2. *Let $u \in \mathbb{F}_{q^2}$. The mapping $F(x) = x^2 + ux^{q+1}$ is planar on $\mathbb{F}_{q^2}$ if and only if $1 - u^{q+1}$ is a square in the subfield $\mathbb{F}_q$.*

Proof. The statement is true for $u = 0$, so let $u \neq 0$. By Proposition 1 if $F(x)$ is planar then $x + ux^q$ is bijective on $\mathbb{F}_{q^2}$, which is equivalent to $u^{q+1} \neq 1$. Further we apply Theorem 1 with $L(x) = x + ux^q$. Let $\beta \in \mathbb{F}_{q^2}$ be such that both $L(x) + \beta x = ux^q + (1+\beta)x$ and $L(x) - \beta x = ux^q + (1-\beta)x$ are not bijective on $\mathbb{F}_{q^2}$. This is the case if and only if the elements $-(1+\beta)/u$ and $-(1-\beta)/u$ are $(q-1)$st powers in $\mathbb{F}_{q^2}$, or equivalently if it holds:

$$\left(\frac{\beta+1}{u}\right)^{q+1} = \left(\frac{\beta-1}{u}\right)^{q+1} = 1.$$

In particular, it must hold $(\beta+1)^{q+1} = (\beta-1)^{q+1}$, which implies $\beta^q = -\beta$. Hence,

$$\left(\frac{\beta+1}{u}\right)^{q+1} = \frac{-\beta^2 - \beta + \beta + 1}{u^{q+1}} = 1,$$

which yields

$$\beta^2 = -u^{q+1} + 1.$$

Note that $1 - u^{q+1}$ is an element in the subfield $\mathbb{F}_q$. Moreover $\beta \notin \mathbb{F}_q$, since $\beta = -\beta^q$. Hence, $F(x)$ is planar on $\mathbb{F}_{q^2}$ only if $1 - u^{q+1}$ is a square in $\mathbb{F}_q$. Finally, we show that this condition is necessary as well. Indeed, let $1 - u^{q+1} \neq 0$

be a non-square in $\mathbb{F}_q$. Suppose, $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $\beta^2 = -u^{q+1} + 1$. Then necessarily $\beta^q = -\beta$, since β and $-\beta$ are the zeros of the irreducible polynomial $X^2 - (1 - u^{q+1})$ in $\mathbb{F}_{q^2}$ and therefor $-\beta$ is the conjugate of β over $\mathbb{F}_q$. To complete the proof it remains to note that for this β it holds

$$\left(\frac{\beta+1}{u}\right)^{q+1} = \left(\frac{\beta-1}{u}\right)^{q+1} = 1.$$

□

In the remaining part of the paper we consider the case $L(X) = Tr(X)$, where $Tr(X)$ is the polynomial describing the trace mapping from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$.

Proposition 4. *[1, 13] For the trace mapping Tr from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ it holds $\mathcal{M}(Tr) = \{\gamma \in \mathbb{F}_{q^n}^* : Tr(\gamma^{-1}) \neq -1\}$.*

Theorem 3. *Let $a \in \mathbb{F}_{q^n}^*$ with $Tr\left((2a)^{-1}\right) \neq -1$. Then $F(X) = X \cdot (Tr(X) + aX)$ is planar on $\mathbb{F}_{q^n}$ if and only if there is no $z \in \mathbb{F}_{q^n}$ such that $Tr(z^{-1}) = -1$ and $Tr((z-2a)^{-1}) = 1$.*

Proof. By Proposition 4 it holds

$$\mathcal{M} := \mathcal{M}(Tr(x) + ax) = \{\alpha \in \mathbb{F}_{q^n} : \alpha \neq -a \text{ and } Tr((a+\alpha)^{-1}) \neq -1\}.$$

By Theorem 1, $F(x)$ is planar if and only if at least one of β or $-\beta$ belongs to $\mathcal{M}$ for any non-zero $\beta \in \mathbb{F}_{q^n}$. First we consider the case that $\beta \in \{-a, a\}$. Note that $a \in \mathcal{M}$ as $a \neq -a$ and $Tr\left((2a)^{-1}\right) \neq -1$. Hence if $\beta \in \{-a, a\}$, then either β or $-\beta$ is contained in $\mathcal{M}$. It remains to show that if $\beta \in \mathbb{F}_{q^n} \setminus \{0, -a, a\}$, then either β or $-\beta$ is contained in $\mathcal{M}$. Assume the contrary and hence we have $\beta \in \mathbb{F}_{q^n} \setminus \{0, -a, a\}$ with $Tr\left((a+\beta)^{-1}\right) = -1$ and $Tr\left((a-\beta)^{-1}\right) = -1$. Putting $z = a+\beta$ we obtain $z \in \mathbb{F}_{q^n}$ with $a - \beta = -(z-2a)$, $Tr\left(z^{-1}\right) = -1$ and $Tr\left((z-2a)^{-1}\right) = -Tr\left((a-\beta)^{-1}\right) = 1$. Using the condition in the statement we complete the proof. □

Remark 1. If $a = 0$ in Theorem 3, then $F(x) = x \cdot (Tr(x))$ is not planar by Proposition 1, since $Tr(x)$ is not bijective. Further let $a \in \mathbb{F}_{q^n}^*$ with $Tr\left((2a)^{-1}\right) = -1$. Then $a \notin \mathcal{M}(Tr(x) + ax)$ and $-a \notin \mathcal{M}(Tr(x) + ax)$. Hence also for such an a the mapping $F(x) = x \cdot (Tr(x) + ax)$ is not planar (see Theorem 1).

Corollaries 1 and 2 show, that the conditions of Theorem 3 are satisfied for $n = 3$ and $a = -1, -2$.

Corollary 1. *The mapping $F(x) = x^{q^2+1} + x^{q+1}$ is planar on $\mathbb{F}_{q^3}$. Equivalently, there is no $z \in \mathbb{F}_{q^3}$ satisfying $Tr\left(\frac{1}{z}\right) = -1$ and $Tr\left(\frac{1}{z+2}\right) = 1$.*

Proof. The statement follows from Proposition 3 and Theorem 3 □

Corollary 2. *The mapping $G(x) = x^{q^2+1} + x^{q+1} - x^2$ is planar on $\mathbb{F}_{q^3}$.*

Proof. Note that $G(x) = x(Tr(x) - 2x)$ and hence we can use Theorem 3 with $a = -2$. Suppose there is $z \in \mathbb{F}_{q^3}$ with

$$Tr\left(\frac{1}{z}\right) = -1 \quad \text{and} \quad Tr\left(\frac{1}{z+4}\right) = 1. \tag{1}$$

Observe that then $z \notin \mathbb{F}_q$. Indeed, for $z \in \mathbb{F}_q$ condition (1)

$$Tr\left(\frac{1}{z}\right) = \frac{3}{z} = -1 \quad \text{and} \quad Tr\left(\frac{1}{z+4}\right) = \frac{3}{z+4} = 1.$$

reduces to $z = -3$ and $z = -1$, which cannot be satisfied. Let $z \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$ which satisfies (1). As in the proof of Corollary 1 already shown the minimal polynomial of z over $\mathbb{F}_q$ is of the following shape

$$M_z(X) = X^3 + a_2X^2 + bX + b.$$

The minimal polynomial of $z + 4$ is $M_{z+4}(X) = M_z(X - 4)$, and hence

$$\begin{aligned} M_{z+4}(X) &= (X-4)^3 + a_2(X-4)^2 + b(X-4) + b \\ &= X^3 + (a_2 - 12)X^2 + (48 - 8a_2 + b)X - 64 + 16a_2 - 3b. \end{aligned}$$

To ensure $Tr((z + 4)^{-1}) = 1$ it must hold

$$48 - 8a_2 + b = 64 - 16a_2 + 3b,$$

and hence $b = 4a_2 - 8$. Substituting this value of b in $M_z(X)$, we get

$$M_z(X) = X^3 + a_2X^2 + (4a_2 - 8)X + 4a_2 - 8,$$

a contradiction, since $X = -2$ is a zero of the latter polynomial. □

Remark 2. Observe that the planar mappings described in Corollaries 1 and 2 are EA-equivalent to the monomial planar mapping x^{q+1}. Indeed, for $F(x)$ this follows from the proof of Proposition 3, and in the case of $G(x)$ from the following equality

$$\left(x^{q^2} + x^q - x\right)^{q+1} = \left(-x^{q^2} + x^q + x\right) \circ G(x).$$

In the following theorem we show that if n is sufficiently large, then there is no $a \in \mathbb{F}_{q^n}$ such that $F(X) = X \cdot (Tr(X) + aX)$ is planar on $\mathbb{F}_{q^n}$. This is a result obtained using Theorem 3 and Remark 1, which is in the oppositive direction of the existence results given above.

Theorem 4. *Let $a \in \mathbb{F}_{q^n}$ and $F(X) = X \cdot (Tr(X) + aX)$. If one the following conditions hold, then $F(X)$ is not planar on $\mathbb{F}_{q^n}$:*

- *$q \geq 23$ and $n \geq 12$,*
- *$q \in \{11, 13, 17, 19\}$ and $n \geq 13$,*

- $q = 9$ *and* $n \geq 14$,
- $q = 7$ *and* $n \geq 15$.
- $q = 5$ *and* $n \geq 16$.
- $q = 3$ *and* $n \geq 19$.

Proof. Using Remark 1, we can assume that $a \neq 0$. Let $f_1(z)$ and $f_2(z)$ be the rational functions in $\mathbb{F}_{q^n}(z)$ given by

$$f_1(z) = \frac{1}{z} \text{ and } f_2(z) = \frac{1}{z - 2a}.$$

We use Theorem 1.1 from [4]. Let p be the characteristic of $\mathbb{F}_{q^n}$. Recall that the set $\{f_1(z), f_2(z)\}$ is *strongly linearly independent over* $\mathbb{F}_q$ (cf. [4]) if there is no $a_1, a_2, \epsilon \in \mathbb{F}_{q^n}$ and $h(z) \in \mathbb{F}_{q^n}(z)$ such that $(a_1, a_2) \neq (0, 0)$ and

$$a_1 f_1(z) + a_2 f_2(z) = h(z)^p - h(z) + \epsilon.$$

We use some simple facts from the theory of algebraic function fields (cf. [17] or [15]). Let P_1 be the place of $\mathbb{F}_{q^n}(z)$ corresponding to the zero of z and let ν_{P_1} denote the normalized discrete valuation corresponding to P_1.

Assume that $a_1 \neq 0$. Then

$$\nu_{P_1}\left(h(z)^p - h(z) + \epsilon\right) = \nu_{P_1}\left(a_1 f_1(z) + a_2 f_2(z)\right) = \nu_{P_1}\left(f_1(z)\right) = -1. \quad (2)$$

Hence $\nu_{P_1}(h(z)) < 0$, indeed otherwise, using the triangle inequality of valuations (cf. [17, Definition 1.1.9]) we get

$$\nu_{P_1}\left(h(z)^p - h(z) + \epsilon\right) \geq \min\left\{\nu_{P_1}(h(z)^p), \nu_{P_1}(h(z)), \nu_{P_1}(\epsilon)\right\} \geq 0,$$

which is a contradiction to (2). As $\nu_{P_1}(h(z)) < 0$, we have $\nu_{P_1}(\epsilon) > \nu_{P_1}(h(z)) > \nu_{P_1}(h(z)^p)$. Then using the strict triangle inequality of valuations (cf. [17, Lemma 1.1.11]) we obtain that $\nu_{P_1}\left(h(z)^p - h(z) + \epsilon\right) = p\nu_{P_1}(h(z)) = p\ell$, where $\ell = \nu_{P_1}(h(z))$ is a negative integer. This is again a contradiction to (2). Therefore we get that $a_1 = 0$. Similarly we show that $a_2 = 0$. This proves that the set $\{f_1(z), f_2(z)\}$ is strongly linearly independent over $\mathbb{F}_q$.

Under the notation of [4, Theorem 1.1] we have $r = 2$, $\deg f_1(z) = \deg f_2(z) = 1 = m$, $t_1 = -1$, $t_2 = 1$, $\ell = 1$. Then there exists a primitive element $\gamma \in \mathbb{F}_{q^n}$ such that $Tr(\gamma^{-1}) = -1$ and $Tr((\gamma - 2a)^{-1}) = 1$ if

$$n > 4\left(2 + \log_q(9.8 \cdot 1 \cdot 2 \cdot 1)\right), \quad (3)$$

where $\log_q$ is the logarithm with respect to base q. It is easy to check the (3) is satisfied if one of the conditions in the statement of the theorem holds. For example if $q \geq 23$, then $4(2 + \log_q(9.8 \cdot 2)) \leq 4(2 + \log_{23}(9.8 \cdot 2)) = 11.7959\ldots$. This completes the proof. $\square$

Acknowledgments

The authors thank anonymous reviewers for their useful comments. A part of this paper was written while the second named author was visiting Department of Mathematics, Otto-von-Guericke University of Magdeburg with a research fellowship from Alexander von Humboldt Foundation. He thanks Otto-von-Guericke University of Magdeburg for hospitality. The second named author is partially supported TÜBİTAK under Grant No. TBAG–109T672.

References

1. A. Blokhuis, A. E. Brouwer, and T. Szőnyi, The number of directions determined by a function f on a finite field, *J. Combin. Theory Ser. A*, 70 (1995) pp. 349–353.
2. A. Blokhuis, R.S. Coulter, M. Henderson and Ch. M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Finite fields and applications (Augsburg, 1999, Springer (2001), pp. 37-42.
3. Th .P. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, *On almost perfect nonlinear functions over* $\mathbb{F}_2^n$, IEEE Trans. Inform. Theory 52(9) (2006), pp. 4160-4170.
4. S. D. Cohen, *Finite field elements with specified order and traces*, Des. Codes Cryptogr. 36 (2005) pp. 331- 340.
5. R. S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math. 217 (2008) pp. 282- 304.
6. R. S. Coulter and R. W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. 10 (1997) pp. 167-184.
7. P. Dembowski and T. Ostrom, *Planes of order n with collineation groups of order* n^2, Math. Z. 103 (1968) pp. 239-258.
8. C. Ding and J. Yin, *Signal sets from functions with optimum nonlinearity*, IEEE Trans. Communications, **55** (2007), 936–940.
9. C. Ding and J. Yuan, *A family of optimal constant-composition codes*,IEEE Trans. Inform. Theory, **51** (2005), 3668–3671.
10. T. Helleseth, G. Kyureghyan, G. J. Ness and A. Pott, *On a family of perfect nonlinear binomials*, in "Boolean Functions in Cryptology and Information Security", B. Preenel and O.A. Logachev (Eds.), IOS Press (2008) pp. 126-139.
11. X.-D. Hou and Ch. Sze, *On certain diagonal equations over finite fields*, Finite Fields Appl .15 (2009) pp. 633-643.
12. Y. Laigle-Chapuy, *A note on a class of quadratic permutations over* $\mathbb{F}_{2^n}$., Applied algebra, algebraic algorithms and error-correcting codes, pp. 130 137, Lecture Notes in Comput. Sci., 4851, Springer, Berlin, 2007.
13. G. Kyureghyan, *Constructing permutations of finite fields via linear translators*, J. Comb. Theory (A), in press.
14. G. Kyureghyan and A. Pott, *Some Theorems on Planar Mappings*, LNCS 5130, WAIFI 2008, pp. 117-122.
15. H. Niederreiter and C. P. Xing, Rational Points on Curves over Finite Fields: Theory and Applications, Cambridge Univ. Press, Cambridge, 2001.
16. K. Nyberg, *Differentially uniform mappings for cryptography*, in Advances in Cryptology-EUROCRYPT 93, Lecture Notes in Computer Science, vol.765. New York: Springer-Verlag, 1994, pp. 134-144.

17. H. Stichtenoth, Algebraic Function Fields and Codes, Second edition, Springer-Verlag, Berlin, 2009.
18. G. Weng, W. Qiu, Z. Wang and Q. Xiang, *Pseudo-Paley graphs and skew Hadamard sets from presemifields*, Des. Codes Cryptogr. 44 (2007) pp. 49-62.