On Commutative Semifields of a Family of Planar Functions

Lilya Budaghyan
University of Bergen
Bergen, Norway
e-mail: Lilya.Budaghyan@ii.uib.no

Tor Helleseth
University of Bergen
Bergen, Norway
e-mail: Tor.Helleseth@ii.uib.no

ABSTRACT

In their recent paper the authors constructed infinite families of planar Dembowski-Ostrom multinomials over $\mathbf{F}_{p^{2k}}$ where p is any odd prime. In the present work we prove that for k odd one of the constructed families of planar functions define new commutative semifields (in part by studying the nuclei of these semifields). This implies that these functions are CCZ-inequivalent to all previously known PN mappings.

Keywords

Commutative semifield, Equivalence of functions, Perfect nonlinear, Planar function.

1. INTRODUCTION

For any positive integer n and any prime p a function F from the field $\mathbf{F}_{p^n}$ to itself is called *differentially δ-uniform* if for every $a \neq 0$ and every b in $\mathbf{F}_{p^n}$, the equation $F(x+a) - F(x) = b$ admits at most δ solutions. Functions with low differential uniformity are of special interest in cryptography (see [3, 16]). Differentially 1-uniform functions are called *perfect nonlinear* (PN) or *planar*. PN functions exist only for p odd. For p even differentially 2-uniform functions, called *almost perfect nonlinear* (APN), are those which have the lowest possible differential uniformity.

There are several equivalence relations of functions for which differential uniformity is invariant. First recall that a function F over $\mathbf{F}_{p^n}$ is called *linear* if

$$F(x) = \sum_{0 \le i < n} a_i x^{p^i}, \qquad a_i \in \mathbf{F}_{p^n}.$$

A sum of a linear function and a constant is called an *affine function*. We say that two functions F and F' are *affine equivalent* (or *linear equivalent*) if $F' = A_1 \circ F \circ A_2$, where the mappings A_1, A_2 are affine (resp. linear) permutations. Functions F and F' are called *extended affine equivalent* (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings A, A_1, A_2 are affine, and where A_1, A_2 are permutations.

Two mappings F and F' from $\mathbf{F}_{p^n}$ to itself are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbf{F}_{p^n}^2$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x, F(x)) \mid x \in \mathbf{F}_{p^n}\}$ and $G_{F'} = \{(x, F'(x)) \mid x \in \mathbf{F}_{p^n}\}$. Differential uniformity is invariant under CCZ-equivalence. EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse. In [4], it is proven that CCZ-equivalence is even more general. However, it is proven in [5, 14], that for PN functions CCZ-equivalence coincides with EA-equivalence.

Almost all known planar functions are DO polynomials. Recall that a function F is called *Dembowski-Ostrom polynomial* (DO polynomial) if

$$F(x) = \sum_{0 \le k,j < n} a_{kj} x^{p^k + p^j}, \quad a_{ij} \in \mathbf{F}_{p^n}.$$

When p is odd the notion of planar DO polynomial is closely connected to the notion of *commutative semifield*. A ring with left and right distributivity and with no zero divisors is called a *presemifield*. A presemifield with a multiplicative identity is called a *semifield*. Any finite presemifield can be represented by $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$, where $(\mathbf{F}_{p^n}, +)$ is the additive group of $\mathbf{F}_{p^n}$ and $x \star y = \phi(x,y)$ with ϕ a function from $\mathbf{F}_{p^n}^2$ onto $\mathbf{F}_{p^n}$, see [8].

Let $\mathbf{S}_1 = (\mathbf{F}_{p^n}, +, \circ)$ and $\mathbf{S}_2 = (\mathbf{F}_{p^n}, +, \star)$ be two presemifields. They are called *isotopic* if there exist three linear permutations L, M, N over $\mathbf{F}_{p^n}$ such that

$$L(x \circ y) = M(x) \star N(y),$$

for any $x, y \in \mathbf{F}_{p^n}$. The triple (M, N, L) is called the *isotopism* between $\mathbf{S}_1$ and $\mathbf{S}_2$. If $M = N$ then $\mathbf{S}_1$ and $\mathbf{S}_2$ are called *strongly isotopic*.

Let $\mathbf{S}$ be a finite semifield. The subsets

$$N_l(\mathbf{S}) = \{\alpha \in \mathbf{S} : (\alpha \star x) \star y = \alpha \star (x \star y) \text{ for all } x, y \in \mathbf{S}\},$$
$$N_m(\mathbf{S}) = \{\alpha \in \mathbf{S} : (x \star \alpha) \star y = x \star (\alpha \star y) \text{ for all } x, y \in \mathbf{S}\},$$
$$N_r(\mathbf{S}) = \{\alpha \in \mathbf{S} : (x \star y) \star \alpha = x \star (y \star \alpha) \text{ for all } x, y \in \mathbf{S}\},$$

are called the *left, middle* and *right nucleus* of $\mathbf{S}$, respectively, and the set $N(\mathbf{S}) = N_l(\mathbf{S}) \cap N_m(\mathbf{S}) \cap N_r(\mathbf{S})$ is called the *nucleus*. These sets are finite fields and, if $\mathbf{S}$ is commutative then $N_l(\mathbf{S}) = N_r(\mathbf{S})$. The nuclei measure how far $\mathbf{S}$ is from being associative. *The orders of the respective nuclei are invariant under isotopism* [8].

Let $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$ be a commutative presemifield which does not contain an identity. To create a semifield from $\mathbf{S}$ choose any $a \in \mathbf{F}_{p^n}^*$ and define a new multiplication $\circ$ by

$$(x \star a) \circ (a \star y) = x \star y$$

for all $x, y \in \mathbf{F}_{p^n}$. Then $\mathbf{S}' = (\mathbf{F}_{p^n}, +, \circ)$ is a commutative semifield isotopic to $\mathbf{S}$ with identity $a \star a$. We say $\mathbf{S}'$ is a commutative semifield *corresponding* to the commutative presemifield $\mathbf{S}$. An isotopism between $\mathbf{S}$ and $\mathbf{S}'$ is a strong isotopism $\big(L_a(x), L_a(x), x\big)$ with a linear permutation $L_a(x) = a \star x$, see [8].

Let F be a planar DO polynomial over $\mathbf{F}_{p^n}$. Then $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$, with

$$x \star y = F(x+y) - F(x) - F(y)$$

for any $x, y \in \mathbf{F}_{p^n}$, is a commutative presemifield. We denote by $\mathbf{S}_F = (\mathbf{F}_{p^n}, +, \circ)$ the commutative semifield corresponding to the commutative presemifield $\mathbf{S}$ with isotopism $\big(L_1(x), L_1(x), x\big)$ and we call $\mathbf{S}_F = (\mathbf{F}_{p^n}, +, \circ)$ the *commutative semifield defined by the planar DO polynomial F*. Conversely, given a commutative presemifield $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$ of odd order, the function given by

$$F(x) = \frac{1}{2}(x \star x)$$

is a planar DO polynomial [8]. It is proven in [5] that for planar DO polynomials CCZ-equivalence coincides with linear equivalence. This implies that two planar DO polynomials F and F' are CCZ-equivalent if and only if the corresponding commutative semifields $\mathbf{S}_F$ and $\mathbf{S}_{F'}$ are strongly isotopic. It is proven in [8] that for the n odd case two commutative presemifields are isotopic if and only if they are strongly isotopic. There are also some sufficient conditions for the n even case when isotopy of presemifields implies their strong isotopy [8]. Thus, in the case n even it is potentially possible that isotopic commutative presemifields define CCZ-inequivalent planar DO polynomials. However, in practice no such cases are known.

Although commutative semifields have been intensively studied for more than a hundred years, up to recently there were only eight distinct cases of commutative semifields of odd order known (see [5]), and only three of them were defined for any odd prime p (the five other known cases were defined only for $p = 3$):

(i) $$x^2$$ over $\mathbf{F}_{p^n}$ which corresponds to the finite field $\mathbf{F}_{p^n}$;

(ii) $$x^{p^t+1}$$ over $\mathbf{F}_{p^n}$, with $n/\gcd(t,n)$ odd, which correspond to Albert's commutative twisted fields [1, 9, 12];

(iii) the functions over $\mathbf{F}_{p^{2k}}$, which correspond to the Dickson semifields [10].

The representations of the Dickson PN functions can be found in [15]. The only known PN functions which are not DO polynomials are the power functions $x^{\frac{3^t+1}{2}}$ over $\mathbf{F}_{3^n}$, where t is odd and $\gcd(t,n) = 1$ [7, 13]. In recent works [5] and [17] other three families of planar DO polynomials defined for any odd prime p have been constructed: for any odd prime p and positive integers s, k and t, and $n = 2k$

(i*) $$(bx)^{p^s+1} - (bx)^{p^k(p^s+1)} + \sum_{i=0}^{k-1} c_i x^{p^i(p^k+1)},$$ over $\mathbf{F}_{p^n}$ where $\sum_{i=0}^{k-1} c_i x^{p^i}$ is a permutation of $\mathbf{F}_{p^n}$ with coefficients in $\mathbf{F}_{p^k}$, $b \in \mathbf{F}_{p^n}^*$, and $\gcd(k+s, 2k) = \gcd(k+s, k)$, $\gcd(p^s+1, p^k+1) \neq \gcd\left(p^s+1, (p^k+1)/2\right)$, see [5];

(ii*) $$bx^{p^s+1} + (bx^{p^s+1})^{p^k} + cx^{p^k+1} + \sum_{i=1}^{k-1} r_i x^{p^{k+i}+p^i},$$ over $\mathbf{F}_{p^n}$ where $b \in \mathbf{F}_{p^n}^*$ is not a square, $c \in \mathbf{F}_{p^n} \setminus \mathbf{F}_{p^k}$, and $r_i \in \mathbf{F}_{p^k}$, $0 \le i < k$, and $\gcd(k+s, n) = \gcd(k+s, k)$, see [5];

(iii*) $$x^{p^s+1} - a^{p^t-1} x^{p^t+p^{2t+s}}$$ over $\mathbf{F}_{p^{3t}}$, where a is primitive in $\mathbf{F}_{p^{3t}}$, $\gcd(3,t) = 1$, $t - s = 0 \bmod 3$, $3t/\gcd(s, 3t)$ is odd, see [17].

In [5] we proved that PN functions (i*) and (ii*) are CCZ-inequivalent to functions (i) and, when $s \neq \pm t$ then also to functions (ii). The present paper is dedicated to the study of the nuclei of the commutative semifields defined by (i*). In particular, we prove that for k odd the commutative semifields defined by functions (i*) are nonisotopic to Dickson semifields. Besides, we prove here that functions (i*) are CCZ-inequivalent to (ii) also when $s = \pm t$ under some conditions on coefficients of (i*). These results imply in particular that for $p \neq 3$ and k odd the PN functions of (i*) are CCZ-inequivalent to the previously known ones and define new commutative semifields.

2. RESULTS

In [5] we proved that PN functions (i*) and (ii*) are CCZ-inequivalent to functions (i) and, when $s \neq \pm t$ then also to functions (ii). In the proposition below we prove that when $s = \pm t$ the family of PN functions (i*) always contains functions CCZ-inequivalent to (ii).

Proposition 1. *Let p be an odd prime, s and k positive integers, $n = 2k$. The function*

$$F(x) = x^{p^s+1} - x^{p^{k+s}+p^s} \pm x^{p^k+1}$$

is CCZ-inequivalent to (ii) *when $s = \pm t$ over $\mathbf{F}_{p^n}$.*

Proof. Assume that F and $G = x^{p^s+1}$ are CCZ-equivalent (that is, $t = s$; the proof for the case $t = -s$ is similar). Since F is a planar DO polynomial then CCZ-equivalence coincides with linear equivalence and, therefore, implies the existence of linear permutations L_1 and L_2, defined by

$$L_1(x) = \sum_{i=0}^{n-1} u_i x^{p^i}, \tag{1}$$

$$L_2(x) = \sum_{i=0}^{n-1} v_i x^{p^i}, \tag{2}$$

such that

$$G\big(L_1(x)\big) + L_2\big(F(x)\big) = 0.$$

We get

$$\begin{aligned} 0 &= \left(\sum_{i=0}^{n-1} u_i x^{p^i}\right)^{p^s+1} \\ &\quad + \sum_{i=0}^{n-1} v_i \left(x^{p^s+1} - x^{p^{k+s}+p^s} \pm x^{p^k+1}\right)^{p^i} \\ &= \sum_{i,j=0}^{n-1} u_i u_j^{p^s} x^{p^i+p^{j+s}} + \sum_{i=0}^{n-1} v_i x^{p^{i+s}+p^i} \\ &\quad - \sum_{i=0}^{n-1} v_i x^{p^{i+s+k}+p^{i+k}} \pm \sum_{i=0}^{n-1} v_i x^{p^{i+k}+p^i}. \end{aligned}$$

Since the latter expression is equal to 0 then the terms of the type x^{2p^i}, $0 \le i < n$, should vanish and we get

$$u_i u_{i-s}^{p^s} = 0, \qquad 0 \le i < n. \tag{3}$$

Considering items with exponents $p^{i+s} + p^i$ and with exponents $p^{i+k} + p^i$, $0 \le i < n$, we get

$$v_i - v_{i+k} + u_i u_i^{p^s} + u_{i+s} u_{i-s}^{p^s} = 0, \tag{4}$$

$$\pm v_i + u_i u_{i+k-s}^{p^s} + u_{i+k} u_{i-s}^{p^s} = 0, \tag{5}$$

respectively. Equality (5) implies

$$\pm v_i = -(u_i u_{i+k-s}^{p^s} + u_{i+k} u_{i-s}^{p^s}) = \pm v_{i+k}. \tag{6}$$

Equalities (4) and (6) imply

$$0 = v_i - v_{i+k} = -(u_i u_i^{p^s} + u_{i+s} u_{i-s}^{p^s}). \tag{7}$$

If $u_i \neq 0$ then $u_{i-s} = 0$ by (3). But if $u_{i-s} = 0$ then $u_i = 0$ by (7). Hence, $L_1 = 0$ which is impossible since L_1 is a permutation. This contradiction shows that the functions F and x^{p^s+1} are CCZ-inequivalent. □

It is proven in [8] that, for any planar DO function F, isotopism between the commutative semifield defined by F and a commutative twisted field, or the finite field, implies strong isotopism. Thus, PN functions (i*) define commutative semifields nonisotopic to the field and to Albert's commutative twisted fields. Due to the theorem below we will see also that the commutative semifields of (i*) are also nonisotopic to Dickson semifields when k is odd and $b \in \mathbf{F}_{p^k}$.

Theorem 1. Let F be a PN function of the family (i*) *with $b \in \mathbf{F}_{p^k}$. Then the middle nucleus of the commutative semifield defined by F has a square order.*

Proof. For any $x, y \in \mathbf{F}_{p^{2k}}$ we denote

$$\begin{aligned} x \star y &= F(x+y) - F(x) - F(y) \\ &= b^{p^s+1}(xy^{p^s} + x^{p^s}y) \\ &\quad -b^{p^k(p^s+1)}(x^{p^k}y^{p^{k+s}} + x^{p^{k+s}}y^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_i(x^{p^i}y^{p^{k+i}} + x^{p^{k+i}}y^{p^i}), \end{aligned} \tag{8}$$

and

$$\begin{aligned} L(x) = 1 \star x &= b^{p^s+1}(x + x^{p^s}) - b^{p^k(p^s+1)}(x^{p^k} + x^{p^{k+s}}) \\ &\quad +\sum_{i=0}^{k-1} c_i(x^{p^i} + x^{p^{k+i}}). \end{aligned} \tag{9}$$

Then the multiplication $\circ$ of the commutative semifield $\mathbf{S}_F$ defined by F is

$$x \circ y = L^{-1}(x) \star L^{-1}(y), \tag{10}$$

for any $x, y \in \mathbf{F}_{p^{2k}}$.
We are going to prove that for any $x, y \in \mathbf{F}_{p^{2k}}$ and any $\alpha \in \mathbf{F}_{p^2}$

$$(x \circ L(\alpha)) \circ y = (y \circ L(\alpha)) \circ x,$$

or, since L is a permutation then, equivalently, we need to prove that

$$\big(L(x) \circ L(\alpha)\big) \circ L(y) = \big(L(y) \circ L(\alpha)\big) \circ L(x),$$

that is,

$$L^{-1}(x \star \alpha) \star y = L^{-1}(y \star \alpha) \star x, \tag{11}$$

due to (10). We have

$$\begin{aligned} L(x)^{p^k} + L(x) &= 2\sum_{i=0}^{k-1} c_i(x^{p^i} + x^{p^{k+i}}), \\ L(x)^{p^k} - L(x) &= 2b^{p^k(p^s+1)}(x^{p^k} + x^{p^{k+s}}) \\ &\quad -2b^{p^s+1}(x + x^{p^s}). \end{aligned}$$

Note that $L(x^{p^k}) = L(x)^{p^k}$. Then applying L^{-1} to both sides of the equalities above we get

$$x^{p^k} + x = 2L^{-1}\Big(\sum_{i=0}^{k-1} c_i(x^{p^i} + x^{p^{k+i}})\Big), \tag{12}$$

$$\begin{aligned} x^{p^k} - x &= 2L^{-1}\Big(b^{p^k(p^s+1)}(x^{p^k} + x^{p^{k+s}}) \\ &\quad -b^{p^s+1}(x + x^{p^s})\Big). \end{aligned} \tag{13}$$

Then, using (12)-(13) and $\alpha^{p^2} = \alpha$,

$$\begin{aligned} L^{-1}(x \star \alpha) &= L^{-1}\Big(b^{p^s+1}(x\alpha^{p^s} + x^{p^s}\alpha) \\ &\quad -b^{p^k(p^s+1)}(x^{p^k}\alpha^{p^{k+s}} + x^{p^{k+s}}\alpha^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_i(x^{p^i}\alpha^{p^{k+i}} + x^{p^{k+i}}\alpha^{p^i})\Big) \\ &= L^{-1}\Big(b^{p^s+1}\big(x\alpha^{p^s} + (x\alpha^{p^s})^{p^s}\big) \\ &\quad -b^{p^k(p^s+1)}\big((x\alpha^{p^s})^{p^k} + (x\alpha^{p^s})^{p^{k+s}}\big)\Big) \\ &\quad +L^{-1}\Big(\sum_{i=0}^{k-1} c_i\big((x\alpha^{p^k})^{p^i} + (x\alpha^{p^k})^{p^{k+i}}\big)\Big) \\ &= -\frac{1}{2}\big((x\alpha^{p^s})^{p^k} - x\alpha^{p^s}\big) + \frac{1}{2}\big(x\alpha^{p^k} + (x\alpha^{p^k})^{p^k}\big) \\ &= \frac{1}{2}(\alpha^{p^s} + \alpha^{p^k})x + \frac{1}{2}(\alpha - \alpha^{p^{k+s}})x^{p^k} \\ &= \begin{cases} \frac{1}{2}(\alpha + \alpha^p)x + \frac{1}{2}(\alpha - \alpha^p)x^{p^k} & \text{if } k+s \text{ is odd}, \\ \alpha x & \text{if } k \text{ and } s \text{ are even}. \end{cases} \end{aligned}$$

Hence, for $k + s$ odd

$$\begin{aligned} L^{-1}(x \star \alpha) \star y &= \frac{1}{2}\Big((\alpha + \alpha^p)x + \frac{1}{2}(\alpha - \alpha^p)x^{p^k}\Big) \star y \\ &= \frac{1}{2}\Big(b^{p^s+1}\big((\alpha + \alpha^p)xy^{p^s} + (\alpha + \alpha^p)x^{p^s}y \\ &\quad +(\alpha - \alpha^p)x^{p^k}y^{p^s} + (\alpha - \alpha^p)^{p^s}x^{p^{k+s}}y\big) \\ &\quad -b^{p^k(p^s+1)}\big((\alpha + \alpha^p)x^{p^k}y^{p^{k+s}} \\ &\quad +(\alpha + \alpha^p)x^{p^{k+s}}y^{p^k} + (\alpha - \alpha^p)^{p^k}xy^{p^{k+s}} \\ &\quad +(\alpha - \alpha^p)^{p^{k+s}}x^{p^s}y^{p^k}\big) \\ &\quad +\sum_{i=0}^{k-1} c_i\big((\alpha + \alpha^p)x^{p^i}y^{p^{k+i}} \\ &\quad +(\alpha + \alpha^p)x^{p^{k+i}}y^{p^i} \\ &\quad +(\alpha - \alpha^p)^{p^i}x^{p^{k+i}}y^{p^{k+i}} \\ &\quad +(\alpha - \alpha^p)^{p^{k+i}}x^{p^i}y^{p^i}\big)\Big) \\ &= L^{-1}(y \star \alpha) \star x. \end{aligned}$$

If k and s are even

$$\begin{aligned} L^{-1}(x \star \alpha) \star y &= b^{p^s+1}(\alpha xy^{p^s} + \alpha x^{p^s}y) \\ &\quad -b^{p^k(p^s+1)}(\alpha x^{p^k}y^{p^{k+s}} + \alpha x^{p^{k+s}}y^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_i(\alpha^{p^i}x^{p^i}y^{p^{k+i}} + \alpha^{p^i}x^{p^{k+i}}y^{p^i}) \\ &= L^{-1}(y \star \alpha) \star x. \end{aligned}$$

Hence, $L(\mathbf{F}_{p^2})$ is contained in the middle nucleus of the semifield $\mathbf{S}_F$ and, therefore, since nuclei of a semifield are finite fields then the middle nucleus must have a square order. □

Corollary 1. If k is odd and $b \in \mathbf{F}_{p^k}$ then the PN function (i*) *defines a commutative semifield non-isotopic to Dickson semifields (and therefore it is CCZ-inequivalent to Dickson PN functions).*

Proof. The middle nuclei of Dickson semifields have the order p^k (see [11]) which is not a square for k odd. Since the orders of the middle nuclei of isotopic semifields are equal then the commutative semifields defined by *(i*)* are non-isotopic to Dickson semifields due to Theorem 1. □

Now we can formulate our main result.

Corollary 2. If $p \neq 3$ and k is odd then the PN functions $F(x) = x^{p^s+1} - x^{p^{k+s}+p^s} \pm x^{p^k+1}$ of family (i*) *are CCZ-inequivalent to all previously known PN functions and define commutative semifields non-isotopic to all previously known semifields.*

The following two propositions give additional information on the nuclei of semifields defined by (i*). Similar results can be obtained also for semifields of (ii*).

Proposition 2. Let F be a PN function of the family (i*) *and p^d be the order of the middle nucleus of the commutative semifield defined by F. Then d is divisible by* $\gcd(s, k)$.

Proof. With notations (8)-(10) we are going to prove that equality (11) takes place for any $x, y \in \mathbf{F}_{p^{2k}}$ and any $\alpha \in$

$\mathbf{F}_{p^{\gcd(s,k)}}$. Indeed, since $\alpha^{p^s} = \alpha^{p^k} = \alpha$ then

$$\begin{aligned} L^{-1}(x \star \alpha) &= L^{-1}\Big(b^{p^s+1}(x\alpha^{p^s} + x^{p^s}\alpha) \\ &\quad -b^{p^k(p^s+1)}(x^{p^k}\alpha^{p^{k+s}} + x^{p^{k+s}}\alpha^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_i(x^{p^i}\alpha^{p^{k+i}} + x^{p^{k+i}}\alpha^{p^i})\Big) \\ &= L^{-1}\Big(b^{p^s+1}\big(x\alpha + (x\alpha)^{p^s}\big) \\ &\quad -b^{p^k(p^s+1)}\big((x\alpha)^{p^k} + (x\alpha)^{p^{k+s}}\big) \\ &\quad +\sum_{i=0}^{k-1} c_i\big((x\alpha)^{p^i} + (x\alpha)^{p^{k+i}}\big)\Big) \\ &= L^{-1}(L(\alpha x)) = \alpha x. \end{aligned} \tag{14}$$

Hence,

$$\begin{aligned} L^{-1}(x \star \alpha) \star y &= b^{p^s+1}(\alpha x y^{p^s} + \alpha x^{p^s} y) \\ &\quad -b^{p^k(p^s+1)}(\alpha x^{p^k} y^{p^{k+s}} + \alpha x^{p^{k+s}} y^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_i(\alpha^{p^i} x^{p^i} y^{p^{k+i}} + \alpha^{p^i} x^{p^{k+i}} y^{p^i}) \\ &= L^{-1}(y \star \alpha) \star x. \end{aligned}$$

Thus, $L(\mathbf{F}_{p^{\gcd(s,k)}})$ is contained in the middle nucleus of the semifield $\mathbf{S}_F$ and, therefore, since nuclei of a semifield are finite fields then d has to be divisible by $\gcd(s,k)$. □

Proposition 3. *Let F be a PN function of the family* (i*) *where $c_i = 0$ for i not divisible by s. If p^d is the order of the left nucleus of the commutative semifield defined by F then d is divisible by* $\gcd(s,k)$.

Proof. With notations (8)-(10) we are going to prove that the equality

$$L^{-1}(x \star \alpha) \star y = L^{-1}(x \star y) \star \alpha \tag{15}$$

takes place for any $x, y \in \mathbf{F}_{p^{2k}}$ and any $\alpha \in \mathbf{F}_{p^{\gcd(s,k)}}$. Indeed, since $\alpha^{p^s} = \alpha^{p^k} = \alpha$ then

$$\begin{aligned} x \star \alpha &= b^{p^s+1}(x\alpha^{p^s} + x^{p^s}\alpha) \\ &\quad -b^{p^k(p^s+1)}(x^{p^k}\alpha^{p^{k+s}} + x^{p^{k+s}}\alpha^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_{is}(x^{p^{is}}\alpha^{p^{k+is}} + x^{p^{k+is}}\alpha^{p^{is}}) \\ &= b^{p^s+1}(x\alpha + x^{p^s}\alpha) \\ &\quad -b^{p^k(p^s+1)}(x^{p^k}\alpha + x^{p^{k+s}}\alpha) \\ &\quad +\sum_{i=0}^{k-1} c_{is}(x^{p^{is}}\alpha + x^{p^{k+is}}\alpha) \\ &= \alpha L(x). \end{aligned}$$

Hence,

$$L^{-1}(x \star y) \star \alpha \;=\; \alpha L\big(L^{-1}(x \star y)\big) = \alpha(x \star y)$$

and using (14) we get

$$\begin{aligned} L^{-1}(x \star \alpha) \star y &= (\alpha x) \star y \\ &= b^{p^s+1}(\alpha x y^{p^s} + \alpha x^{p^s} y) \\ &\quad -b^{p^k(p^s+1)}(\alpha x^{p^k} y^{p^{k+s}} + \alpha x^{p^{k+s}} y^{p^k}) \\ &\quad +\sum_{i=0}^{k-1} c_{is}(\alpha x^{p^{is}} y^{p^{k+is}} + \alpha x^{p^{k+is}} y^{p^{is}}) \\ &= \alpha(x \star y). \end{aligned}$$

This proves equality (15). Thus, $L(\mathbf{F}_{p^{\gcd(s,k)}})$ is contained in the left nucleus of the semifield $\mathbf{S}_F$ and, therefore, d has to be divisible by $\gcd(s,k)$. □

REFERENCES

[1] A. A. Albert. On nonassociative division algebras. *Trans. Amer. Math. Soc.* 72, pp. 296-309, 1952.

[2] A. A. Albert. Generalized twisted fields. Pacific J. Math. 11, pp. 1-8, 1961.

[3] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, vol. 4, No.1, pp. 3-72, 1991.

[4] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

[5] L. Budaghyan and T. Helleseth. New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. *Proceedings of the 5th International Conference of Sequences and Their Applications - SETA 2008*, Springer, Lecture Notes in Computer Science 5203, pp. 401-414, Lexington, KY, USA, Sep. 14-18, 2008.

[6] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[7] R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des., Codes, Cryptogr.*, 10, pp. 167-184, 1997.

[8] R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Advances in Math.* 217, pp. 282-304, 2008.

[9] P. Dembowski and T. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103, pp. 239-258, 1968.

[10] L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc* 7, pp. 514-522, 1906.

[11] L. E. Dickson. Linear algebras with associativity not assumed. *Duke Math. J.* 1, pp. 113-125, 1935.

[12] T. Helleseth, C. Rong and D. Sandberg. New families of almost perfect nonlinear power mappings. *IEEE Trans. in Inf. Theory*, 45, pp. 475-485, 1999.

[13] T. Helleseth and D. Sandberg. Some power mappings with low differential uniformity. *Applic. Alg. Eng., Commun. Comput.*, vol. 8, pp. 363-370, 1997.

[14] G. Kyureghyan and A. Pott. Some theorems on planar mappings. *Proceedings of WAIFI 2008*, Lecture Notes in Computer Science 5130, pp. 115-122, 2008.

[15] K. Minami and N. Nakagawa. On planar functions of elementary abelian p-group type. Submitted.

[16] K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptography, EUROCRYPT'93, LNCS*, 765, pp. 55-64, 1994.

[17] Z. Zha, G. Kyureghyan, X. Wang. Perfect nonlinear binomials and their semifields. Finite Fields and Their Applications, in press doi:10.1016/j.ffa.2008.09.002