New commutative semifields defined by PN multinomials *

Lilya Budaghyan and Tor Helleseth

Department of Informatics
University of Bergen
PB 7803, 5020 Bergen
NORWAY
{Lilya.Budaghyan,Tor.Helleseth}@ii.uib.no

Abstract. We introduce infinite families of perfect nonlinear Dembowski-Ostrom multinomials over $\mathbf{F}_{p^{2k}}$ where p is any odd prime. We prove that for k odd and $p \neq 3$ these PN 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, 24]). 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.

---
* Part of this work was presented at SETA'08 [7]

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 [6], it is proven that CCZ-equivalence is even more general. In the present paper we prove that for PN functions CCZ-equivalence coincides with EA-equivalence (this has been also independently proven in [20]).

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

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

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 [11].

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

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

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* [11].

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 [11].

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 [11]. We prove in Section 4 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 [11] 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 [11]. 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, there are only eight distinct cases of known commutative semifields of odd order (see [11]), and only three of them are defined for any odd prime p. The eight distinct cases of known planar DO polynomials and corresponding commutative semifields are the following:

(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, 13, 18];

(iii) the functions over $\mathbf{F}_{p^{2k}}$, which correspond to the Dickson semifields [14];

(iv)
$$x^{10} \pm x^6 - x^2$$
over $\mathbf{F}_{3^n}$, with n odd, corresponding to the Coulter-Matthews and Ding-Yuan semifields [10, 16];

(v) the function over $\mathbf{F}_{3^{2k}}$, with k odd, corresponding to the Ganley semifield [17];

(vi) the function over $\mathbf{F}_{3^{2k}}$ corresponding to the Cohen-Ganley semifield [9];

(vii) the function over $\mathbf{F}_{3^{10}}$ corresponding to the Penttila-Williams semifield [25];

(viii) the function over $\mathbf{F}_{3^8}$ corresponding to the Coulter-Henderson-Kosick semifield [12].

The representations of the PN functions corresponding to the cases (iii), (v)-(vii), can be found in [21, 22]. 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 $\gcd(t, n) = 1$ [10, 19].

Let p be an odd prime, s and k positive integers, and $n = 2k$. In Sections 2 and 3 of the present paper we introduce the following new infinite classes of perfect nonlinear DO polynomials over $\mathbf{F}_{p^n}$:

(i*)

$$(bx)^{p^s+1} - \left((bx)^{p^s+1}\right)^{p^k} + \sum_{i=0}^{k-1} c_i x^{p^i(p^k+1)},$$

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

(ii*)

$$bx^{p^s+1} + (bx^{p^s+1})^{p^k} + cx^{p^k+1} + \sum_{i=1}^{k-1} r_i x^{p^{k+i}+p^i},$$

where $b \in \mathbf{F}_{p^n}^*$ is not a square, $c \in \mathbf{F}_{p^n} \setminus \mathbf{F}_{p^k}$, and $r_i \in \mathbf{F}_{p^k}$, $0 \leq i < k$, and $\gcd(k + s, n) = \gcd(k + s, k)$.

Another case of new planar DO polynomials is the family of PN binomials* which have been constructed in [26] by extending the family of APN binomials of [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.

In Section 5 we prove that the introduced PN functions (i*) and (ii*) are CCZ-inequivalent to the functions (i) and (ii). It means that (i*) and (ii*) define commutative semifields non-isotopic to finite fields and to Albert's commutative twisted fields.

Section 6 is dedicated to the study of the nuclei of the commutative semifields defined by (i*) and (ii*). In particular, we prove that for k odd the commutative semifields defined by the functions (i*) are CCZ-inequivalent to Dickson semifields. The results of Sections 5 and 6 imply in particular that for $p \neq 3$ and k odd the PN functions of (i*) define new commutative semifields.

This paper is an extended version of the work presented at SETA'08 [7]. Proposition 4 and all results of Section 6 are the new contributions of this article.

* The paper [26] became publicly available only after the submission of the paper [7].

2 A new family of PN multinomials

In [23] Ness gives a list of planar DO trinomials over $\mathbf{F}_{p^n}$ for $p \leq 7$, $n \leq 8$ which were found with a computer. Investigation of these functions has led us to the following family of planar DO polynomials.

Theorem 1. *Let p be an odd prime, s and k positive integers such that* $\gcd(p^s+1, p^k+1) \neq \gcd\big(p^s+1, (p^k+1)/2\big)$ *and* $\gcd(k+s, 2k) = \gcd(k+s, k)$. *Let also $n = 2k$, $b \in \mathbf{F}_{p^n}^*$, and $\sum_{i=0}^{k-1} c_i x^{p^i}$ be a permutation over $\mathbf{F}_{p^n}$ with coefficients in $\mathbf{F}_{p^k}$. Then the function*

$$F(x) = (bx)^{p^s+1} - \left((bx)^{p^s+1}\right)^{p^k} + \sum_{i=0}^{k-1} c_i x^{p^i(p^k+1)}$$

is PN over $\mathbf{F}_{p^n}$.

Proof. Since F is DO polynomial then it is PN if for any $a \in \mathbf{F}_{p^n}^*$ the equation $F(x+a) - F(x) - F(a) = 0$ has only 0 as a solution. We have

$$\begin{aligned} \Delta(x) &= F(x+a) - F(x) - F(a) \\ &= b^{p^s+1}(ax^{p^s} + a^{p^s}x) - b^{p^k(p^s+1)}(a^{p^k}x^{p^{k+s}} + a^{p^{k+s}}x^{p^k}) \\ &\quad + \sum_{i=0}^{k-1} c_i(a^{p^i}x^{p^{k+i}} + a^{p^{k+i}}x^{p^i}). \end{aligned}$$

Any solution of the equation $\Delta(x) = 0$ is also a solution of $\Delta(x) + \Delta(x)^{p^k} = 0$ and $\Delta(x) - \Delta(x)^{p^k} = 0$, that is, a solution of

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

$$b^{p^s+1}(ax^{p^s} + a^{p^s}x) = b^{p^k(p^s+1)}(a^{p^k}x^{p^{k+s}} + a^{p^{k+s}}x^{p^k}). \tag{2}$$

Since $\sum_{i=0}^{k-1} c_i x^{p^i}$ is a permutation then (1) implies

$$ax^{p^k} = -a^{p^k}x. \tag{3}$$

Now we can substitute ax^{p^k} in (2) by $-a^{p^k}x$ and then obtain

$$b^{p^s+1}(ax^{p^s} + a^{p^s}x) = -b^{p^k(p^s+1)}(a^{p^{k+s}+p^k-p^s}x^{p^s} + a^{p^{k+s}+p^k-1}x),$$

that is,

$$(b^{p^s+1}a + b^{p^k(p^s+1)}a^{p^{k+s}+p^k-p^s})x^{p^s} = -(b^{p^s+1}a^{p^s} + b^{p^k(p^s+1)}a^{p^{k+s}+p^k-1})x,$$

and since $a, b \neq 0$ then for $x \neq 0$

$$x^{p^s-1} = -\frac{b^{p^s+1}a^{p^s} + b^{p^k(p^s+1)}a^{p^{k+s}+p^k-1}}{b^{p^s+1}a + b^{p^k(p^s+1)}a^{p^{k+s}+p^k-p^s}} = -a^{p^s-1}, \tag{4}$$

when

$$b^{(p^k-1)(p^s+1)} a^{p^{k+s}+p^k-p^s-1} \neq -1. \tag{5}$$

Now assume that for some nonzero a inequality (5) is wrong, that is, $(ba)^{(p^k-1)(p^s+1)} = -1$. Then -1 is a power of $(p^k-1)(p^s+1)$ which is in contradiction with $\gcd(p^s+1, p^k+1) \neq \gcd\left(p^s+1, (p^k+1)/2\right)$ since -1 is a power of $(p^n-1)/2$.

From (3) and (4) we get

$$y^{p^k-1} = y^{p^s-1} = -1, \tag{6}$$

where $y = x/a$. Since $n = 2k$ then the first equality in (6) implies $y^{p^{k+s}} = y$, that is, $y \in \mathbf{F}_{p^{k+s}}$. Thus, if $\gcd(k+s, 2k) = \gcd(k+s, k)$ then $y \in \mathbf{F}_{p^{\gcd(k+s,k)}}$ which contradicts the second equality in (6), that is, $y^{p^k-1} = 1 \neq -1$, for any $y \neq 0$. Therefore, the only solution of $\Delta(x) = 0$ is $x = 0$.

3 Another family of PN multinomials

In this section we show that one of the ways to construct PN mappings is to extend a known family of APN functions over $\mathbf{F}_{2^n}$ to a family of PN functions over $\mathbf{F}_{p^n}$ for odd primes p. Below we construct a class of PN functions by following the pattern of APN multinomials over $\mathbf{F}_{2^{2k}}$ presented in [4].

Theorem 2. *Let p be an odd prime, s and k positive integers, $n = 2k$, and $\gcd(k+s, n) = \gcd(k+s, k)$. If $b \in \mathbf{F}_{p^n}^*$ is not a square, $c \in \mathbf{F}_{p^n} \setminus \mathbf{F}_{p^k}$, and $r_i \in \mathbf{F}_{p^k}$, $0 \leq i < k$, then the function*

$$F(x) = \mathrm{Tr}_k^{2k}(bx^{p^s+1}) + cx^{p^k+1} + \sum_{i=1}^{k-1} r_i x^{p^{k+i}+p^i}$$

is PN over $\mathbf{F}_{p^n}$.

Proof. We have to show that for any $a \in \mathbf{F}_{p^n}^*$ the equation $\Delta(x) = 0$ has only 0 as a solution when

$$\begin{aligned} \Delta(x) &= F(x+a) - F(x) - F(a) \\ &= \mathrm{Tr}_k^{2k}\left(b(x^{p^s}a + xa^{p^s})\right) + c(x^{p^k}a + xa^{p^k}) + \sum_{i=1}^{k-1} r_i(x^{p^{k+i}}a^{p^i} + x^{p^i}a^{p^{k+i}}). \end{aligned}$$

After replacing x by ax we get

$$\begin{aligned} \Delta_1(x) = \Delta(ax) = \mathrm{Tr}_k^{2k}\left(ba^{p^s+1}(x^{p^s} + x)\right) + ca^{p^k+1}(x^{p^k} + x) \\ + \sum_{i=1}^{k-1} r_i a^{p^{k+i}+p^i}(x^{p^{k+i}} + x^{p^i}). \end{aligned}$$

Since $\Delta_1(x) = 0$ then $\Delta_1(x) - \Delta_1(x)^{p^k} = 0$, that is, $(ca^{p^k+1} - c^{p^k} a^{p^k+1})(x^{p^k} + x) = 0$. Thus, $(c - c^{p^k})a^{p^k+1}(x^{p^k} + x) = 0$ and, therefore,

$$x^{p^k} = -x$$

since $c \in \mathbf{F}_{p^{2k}} \setminus \mathbf{F}_{p^k}$.

Substituting $x^{p^k} = -x$ in $\Delta_1(x) = 0$ we obtain

$$\begin{aligned}\Delta_1(x) &= ba^{p^s+1}(x^{p^s} + x) + b^{p^k} a^{p^{s+k}+p^k}(x^{p^{s+k}} + x^{p^k}) \\ &= (ba^{p^s+1} - b^{p^k} a^{p^{s+k}+p^k})(x^{p^s} + x).\end{aligned}$$

Hence, if

$$ba^{p^s+1} \neq b^{p^k} a^{p^{s+k}+p^k} \tag{7}$$

then

$$x^{p^s} = -x.$$

Assume that $ba^{p^s+1} = b^{p^k} a^{p^{s+k}+p^k}$ for some nonzero a. Then we get equalities

$$b^{p^k-1} = a^{p^s+1-p^{s+k}-p^k} = a^{-(p^s+1)(p^k-1)} = a^{(p^{k+s}-1)(p^k-1)}$$

which imply that b is a power of $\gcd(p^s+1, p^k+1)$ and of $\gcd(p^{s+k}-1, p^k+1)$. Thus, inequality (7) holds for any $a \neq 0$ if b is not a power of $\gcd(p^s+1, p^k+1)$ or a power of $\gcd(p^{s+k}-1, p^k+1)$. Since $\gcd(p^s+1, p^k+1)$ and $\gcd(p^{s+k}-1, p^k+1)$ are even then we cannot have inequality (7) for any nonzero b but we have this inequality, in particular, when b is not a square in $\mathbf{F}_{p^n}^*$.

Since $x^{p^k} = -x$ and $x^{p^s} = -x$ then $x^{p^k} = x^{p^s}$ and then by taking the p^k-th power we get $x^{p^{k+s}} = x$. Hence, if $\gcd(k+s, 2k) = \gcd(k+s, k)$ then $x \in \mathbf{F}_{p^{\gcd(k+s,k)}}$ and $x^{p^{\gcd(k+s,k)}} = x$. But $x^{p^k} = -x$, which implies $x = 0$.

4 On the equivalence of PN functions

We prove below that for PN functions CCZ-equivalence coincides with EA-equivalence. In particular it means that PN functions are never permutations.

Proposition 1. *Let F be a PN function and F' be CCZ-equivalent to F. Then F and F' are EA-equivalent.*

Proof. If functions F and F' are CCZ-equivalent then there exists an affine permutation $\mathcal{L}$ over $\mathbf{F}_{p^n}^2$ such that $\mathcal{L}(G_F) = G_{F'}$ where $G_F = \{(x, F(x)) \mid x \in \mathbf{F}_{p^n}\}$ and $G_{F'} = \{(x, F'(x)) \mid x \in \mathbf{F}_{p^n}\}$. The function $\mathcal{L}$ in this case can be introduced as $\mathcal{L}(x,y) = \big(L_1(x,y), L_2(x,y)\big)$ where $L_1, L_2 : \mathbf{F}_{p^n}^2 \to \mathbf{F}_{p^n}$ are affine and $L_1(x, F(x))$ is a permutation (see [6]). Let us see whether there exists such a function L_1 when F is PN. For some linear functions $L, L' : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ and some $b \in \mathbf{F}_{p^n}^*$ we have $L_1(x,y) = L(x)+L'(y)+b$. If $L_1(x, F(x))$ is a permutation then for any nonzero a

$$L(x) + L'(F(x)) + b \neq L(x+a) + L'(F(x+a)) + b,$$

that is, $L'(F(x+a) - F(x)) \neq -L(a)$. Since F is PN then $F(x+a) - F(x)$ is a permutation. Thus, the inequality above implies $L'(c) \neq L(a)$ for any c and any nonzero a. First of all we see that L is a permutation since otherwise $L(a') = 0 = L'(0)$ for some nonzero a' and so we get the inequality $L' \circ L^{-1}(c) \neq a$ for any c and any nonzero a which in its turn means $L' \circ L^{-1} = 0$, that is, $L' = 0$.

By the definition of CCZ-equivalence and by the data obtained above we get for CCZ-equivalent functions F and F' that $F' = F_2 \circ F_1^{-1}$, where

$$F_1(x) = L_1(x, F(x)) = L(x) + b,$$

$$F_2(x) = L_2(x, F(x)) = L''(x) + L'''(F(x)) + b'$$

with $b, b' \in \mathbf{F}_{p^n}$, L, L'', L''' linear and L a permutation. Note that

$$F'(x) = L''\big(F_1^{-1}(x)\big) + L'''\Big(F\big(F_1^{-1}(x)\big)\Big) + b' = A(x) + A_1 \circ F \circ A_2(x)$$

where $A_2(x) = F_1^{-1}(x)$ is an affine permutation, $A = L'' \circ F_1^{-1}$ is affine, and we show below that the linear function $A_1 = L'''$ is a permutation. Indeed, the affine function $\mathcal{L}(x,y) = \big(L(x)+b, L''(x) + L'''(y) + b'\big)$ is a permutation, that is, the system of two equations $L(x) = 0$ and $L''(x) + L'''(y) = 0$ has the only solution $(0,0)$, and then $L'''(y) = 0$ should have the only solution 0 which implies that L''' is a permutation. Thus, F and F' are EA-equivalent.

From the result above we get the following obvious corollaries.

Corollary 1. *If a PN function F is CCZ-equivalent to a DO polynomial F' then F is also DO polynomial.*

Corollary 2. *Perfect nonlinear DO polynomials F and F' are CCZ-equivalent if and only if they are linear equivalent.*

Now it is obvious that CCZ-equivalence of two DO planar functions implies strong isotopism of the corresponding commutative semifields.

It is also obvious that DO polynomials cannot be CCZ-equivalent to the PN functions $x^{(3^t+1)/2}$ over $\mathbf{F}_{3^n}$ with $\gcd(n,t) = 1$, t odd. Indeed, $x^{(3^t+1)/2}$ is not DO polynomial because $\frac{3^t+1}{2} = 2 + \sum_{i=1}^{t-1} 3^{t-i}$.

5 On the inequivalence of the introduced PN functions with known PN mappings

Note that the functions of (i*) and (ii*) are defined over $\mathbf{F}_{p^{2k}}$ for any odd prime p. Obviously, we can say the same only about PN functions of the cases (i), (ii) and (iii), while the cases (v)-(viii) are defined only for $p = 3$ and cannot cover all the functions of Theorems 1 and 2. So when proving CCZ-inequivalence to the previously known PN functions we mainly concentrate our attention on the functions (i), (ii), and (iii).

In the proposition below we show that any function which is CCZ-equivalent to x^2 should have some monomial of the form x^{2p^t} for some t, $0 \le t < n$, in its polynomial representation.

Proposition 2. *Let p be an odd prime and n be a positive integer. Any function F of the form*

$$F(x) = \sum_{0 \le k < j < n} a_{kj} x^{p^k + p^j}$$

over $\boldsymbol{F}_{p^n}$ is CCZ-inequivalent to x^2.

Proof. Since x^2 is a planar DO polynomial then, by Corollary 2, CCZ-equivalence of F to x^2 implies the linear equivalence, that is, the existence of linear permutations L_1 and L_2 such that

$$\big(L_1(x)\big)^2 + L_2\big(F(x)\big) = 0. \tag{8}$$

Let

$$L_1(x) = \sum_{i=0}^{n-1} u_i x^{p^i}, \tag{9}$$

$$L_2(x) = \sum_{i=0}^{n-1} v_i x^{p^i}. \tag{10}$$

Then equality (8) implies

$$0 = \left(\sum_{i=0}^{n-1} u_i x^{p^i}\right)^2 + \sum_{i=0}^{n-1} v_i \left(\sum_{0 \le k < j < n} a_{kj} x^{p^k + p^j}\right)^{p^i}$$

$$= \sum_{i=0}^{n-1} u_i^2 x^{2p^i} + 2 \sum_{0 \le i < j < n} u_i u_j x^{p^i + p^j} + \sum_{0 \le k < j < n, 0 \le i < n} v_i a_{kj}^{p^i} x^{p^i (p^k + p^j)}.$$

Since the identity above takes place for any $x \in \mathbf{F}_{p^n}$ then obviously $u_i^2 = 0$ for all $0 \le i < n$, that is, $L_1(x) = 0$. This contradicts the condition that L_1 is a permutation. Hence F is CCZ-inequivalent to x^2.

Corollary 3. *The functions* (i*) *and* (ii*) *are CCZ-inequivalent to x^2 and define commutative semifields non-isotopic to a finite field.*

Proof. By Proposition 2 the functions (i*) and (ii*) are CCZ-inequivalent to x^2 and, therefore, by Corollary 3.10 of [11] they define commutative semifields non-isotopic to a finite field.

We give below a sufficient condition on DO polynomials to be CCZ-inequivalent to the PN functions of the case (ii).

Proposition 3. *Let p be an odd prime number, n, n' and t positive integers such that $n' < n$ and $n/\gcd(n,t)$ is odd. Let a function $F: \boldsymbol{F}_{p^n} \to \boldsymbol{F}_{p^n}$ be such that*

$$F(x) = \sum_{i=0}^{n'} A_i(x^{p^{s_i}+1}),$$

where $0 < s_i < n$ and $s_i \neq s_j$, for all $i \neq j$, $0 \leq i,j \leq n'$, and the functions A_i, $0 \leq i \leq n'$, are linear. If $t \neq s_i$ and $t \neq n - s_i$ for all $0 \leq i \leq n'$ then the PN function $G(x) = x^{p^t+1}$ is CCZ-inequivalent to F.

Proof. Assume that F and G are CCZ-equivalent. Since G is planar DO polynomial then, by Corollary 2, CCZ-equivalence implies the existence of linear permutations L_1 and L_2, defined by (9)-(10), such that $G\big(L_1(x)\big) + L_2\big(F(x)\big) = 0$. We get

$$\begin{aligned} 0 &= \left(\sum_{i=0}^{n-1} u_i x^{p^i}\right)^{p^t+1} + \sum_{i=0}^{n-1} v_i \left(\sum_{i=0}^{n'} A_i(x^{p^{s_i}+1})\right)^{p^i} \\ &= \sum_{i,j=0}^{n-1} u_i u_j^{p^t} x^{p^i+p^{j+t}} + \sum_{i=0}^{n'} A'_i(x^{p^{s_i}+1}), \end{aligned}$$

where A'_i, $0 \leq i \leq n'$, are some linear functions. Since the latter expression is equal to 0 then the terms of the type x^{2p^i}, $0 \leq i < n$, should vanish and we get

$$u_i u_{i-t}^{p^t} = 0, \qquad 0 \leq i < n. \tag{11}$$

Since $t \neq s_i$ and $t \neq n - s_i$ for all $0 \leq i \leq n'$ then canceling all terms of the type $x^{p^i(p^t+1)}$, $0 \leq i < n$, we get

$$u_i u_i^{p^t} = -u_{i+t} u_{i-t}^{p^t}, \qquad 0 \leq i < n. \tag{12}$$

Equalities (13) and (14) imply $L_1 = 0$. Indeed, if $u_i \neq 0$ for some i then from (13) we get $u_{i-t} = 0$ while from (14) we get $u_{i-t} \neq 0$. But L_1 is a permutation and cannot be constantly 0. This contradiction shows that the functions F and x^{p^t+1} are CCZ-inequivalent.

From proposition above and Corollary 3.9 of [11] we get the following straightforward corollaries.

Corollary 4. *The functions* (i*) *and* (ii*) *are CCZ-inequivalent to x^{p^t+1} when $s \neq \pm t$.*

Corollary 5. *The functions* (i*) *and* (ii*) *are CCZ-inequivalent to all the functions* (ii) *and define commutative semifields non-isotopic to all Albert's commutative twisted fields when $2k/\gcd(2k,s)$ is even.*

Further we can prove that, under some conditions on coefficients, the functions (i*) are CCZ-inequivalent also to x^{p^s+1}.

Proposition 4. *If F is a functions of* (i*) *with $b=1$, $c_0=\pm 1$ and $c_i=0$ for $1\le i<k$ then it is CCZ-inequivalent to $G(x)=x^{p^s+1}$.*

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

Assume that F and G are CCZ-equivalent. Since G is planar DO polynomial then CCZ-equivalence implies the existence of linear permutations L_1 and L_2 (defined by (9) and (10)) such that $G\big(L_1(x)\big)+L_2\big(F(x)\big)=0$. We get

$$\begin{aligned}0&=\left(\sum_{i=0}^{n-1}u_ix^{p^i}\right)^{p^s+1}+\sum_{i=0}^{n-1}v_i\left(x^{p^s+1}-x^{p^{k+s}+p^s}\pm x^{p^k+1}\right)^{p^i}\\&=\sum_{i,j=0}^{n-1}u_iu_j^{p^t}x^{p^i+p^{j+t}}+\sum_{i=0}^{n-1}v_ix^{p^{i+s}+p^i}-\sum_{i=0}^{n-1}v_ix^{p^{i+s+k}+p^{i+k}}\pm\sum_{i=0}^{n-1}v_ix^{p^{i+k}+p^i},\end{aligned}$$

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

$$u_iu_{i-s}^{p^s}=0,\qquad 0\le i<n. \tag{13}$$

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

$$v_i-v_{i+k}+u_iu_i^{p^s}+u_{i+s}u_{i-s}^{p^s}=0, \tag{14}$$
$$\pm v_i+u_iu_{i+k-s}^{p^s}+u_{i+k}u_{i-s}^{p^s}=0 \tag{15}$$

Equality (15) implies

$$\pm v_i=-(u_iu_{i+k-s}^{p^s}+u_{i+k}u_{i-s}^{p^s})=\pm v_{i+k}. \tag{16}$$

Equalities (14) and (16) imply

$$0=v_i-v_{i+k}=-(u_iu_i^{p^s}+u_{i+s}u_{i-s}^{p^s}) \tag{17}$$

If $u_i\ne 0$ then $u_{i-s}=0$ by (13). But if $u_{i-s}=0$ then $u_i=0$ by (17). 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.

Corollary 6. *If $b=1$, $c_0=\pm 1$ and $c_i=0$ for $1\le i<k$ then the functions* (i*) *are CCZ-inequivalent to all the functions* (ii) *and define commutative semifields non-isotopic to all Albert's commutative twisted fields.*

6 Nuclei of the new semifields

Theorem 3. *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 squire order.*

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

$$\begin{aligned} x \star y &= F(x+y) - F(x) - F(y) \\ &= b^{p^s+1}(xy^{p^s} + x^{p^s}y) - b^{p^k(p^s+1)}(x^{p^k}y^{p^{k+s}} + x^{p^{k+s}}y^{p^k}) \\ &\quad + \sum_{i=0}^{k-1} c_i(x^{p^i}y^{p^{k+i}} + x^{p^{k+i}}y^{p^i}). \end{aligned} \tag{18}$$

and

$$L(x) = 1 \star x = b^{p^s+1}(x + x^{p^s}) - b^{p^k(p^s+1)}(x^{p^k} + x^{p^{k+s}}) + \sum_{i=0}^{k-1} c_i(x^{p^i} + x^{p^{k+i}}). \tag{19}$$

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

$$x \circ y = L^{-1}(x) \star L^{-1}(y), \tag{20}$$

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,

$$L^{-1}(x \star \alpha) \star y = L^{-1}(y \star \alpha) \star x. \tag{21}$$

We have

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

Since $L(x^{p^k}) = L(x)^{p^k}$ then applying L^{-1} to both sides of the equalities above we get

$$x^{p^k} + x = 2L^{-1}\Big(\sum_{i=0}^{k-1} c_i(x^{p^i} + x^{p^{k+i}})\Big), \tag{22}$$

$$x^{p^k} - x = 2L^{-1}\Big(b^{p^k(p^s+1)}(x^{p^k} + x^{p^{k+s}}) - b^{p^s+1}(x + x^{p^s})\Big). \tag{23}$$

Then, using (22)-(23) and $\alpha^{p^2}=\alpha$,

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

Hence, for $k+s$ odd

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

If k and s are even

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

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 7. *If k is odd and $b \in \boldsymbol{F}_{p^k}$ 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 [15]) 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 3.

Hence, we can formulate the following result.

Corollary 8. *If k is odd, $b \in \boldsymbol{F}_{p^k}$ and $p \geq 5$ then the PN functions* (i*) *define commutative semifields non-isotopic to all previously known commutative semifields (and therefore these functions are CCZ-inequivalent to all previously known PN functions).*

Further we prove some specific properties of the nuclei of the commutative semifields defined by (i*) and (ii*).

Proposition 5. *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 (18)-(20) we are going to prove that equality (21) 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

$$\begin{aligned} L^{-1}(x \star \alpha) &= L^{-1}\Big(b^{p^s+1}(x\alpha^{p^s} + x^{p^s}\alpha) - b^{p^k(p^s+1)}(x^{p^k}\alpha^{p^{k+s}} + x^{p^{k+s}}\alpha^{p^k}) \\ &\quad + \sum_{i=0}^{k-1} c_i(x^{p^i}\alpha^{p^{k+i}} + x^{p^{k+i}}\alpha^{p^i})\Big) \\ &= L^{-1}\Big(b^{p^s+1}\big(x\alpha + (x\alpha)^{p^s}\big) - b^{p^k(p^s+1)}\big((x\alpha)^{p^k} + (x\alpha)^{p^{k+s}}\big) \\ &\quad + \sum_{i=0}^{k-1} c_i\big((x\alpha)^{p^i} + (x\alpha)^{p^{k+i}}\big)\Big) \\ &= L^{-1}(L(\alpha x)) = \alpha x. \end{aligned} \tag{24}$$

Hence,

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

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 6. *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 (18)-(20) we are going to prove that the equality

$$L^{-1}(x \star \alpha) \star y = L^{-1}(x \star y) \star \alpha \tag{25}$$

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

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

Hence,

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

and using (24) we get

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

This proves equality (25). 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 $\gcd(s,k)$.

Proposition 7. *Let F be a PN function of the family* (ii*). *Then the order of the middle nucleus of the commutative semifield defined by F is divisible by* $\gcd(s,k)$.

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

$$\begin{aligned} x \star y &= F(x+y) - F(x) - F(y) \\ &= b(xy^{p^s} + x^{p^s}y) + b^{p^k}(x^{p^k}y^{p^{k+s}} + x^{p^{k+s}}y^{p^k}) \\ &\quad + c(xy^{p^k} + x^{p^k}y) + \sum_{i=0}^{k-1} r_i(x^{p^i}y^{p^{k+i}} + x^{p^{k+i}}y^{p^i}). \end{aligned} \tag{26}$$

and

$$L(x) = 1\star x = b(x+x^{p^s})+b^{p^k}(x^{p^k}+x^{p^{k+s}})+c(x+x^{p^k})+\sum_{i=0}^{k-1} r_i(x^{p^i}+x^{p^{k+i}}). \quad (27)$$

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

$$x \circ y = L^{-1}(x) \star L^{-1}(y), \quad (28)$$

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 $\alpha \in \mathbf{F}_{p^{\gcd(s,k)}}$

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

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

$$L^{-1}(x \star \alpha) \star y = L^{-1}(y \star \alpha) \star x. \quad (29)$$

Indeed, since $\alpha^{p^s} = \alpha^{p^k} = \alpha$ then

$$\begin{aligned} L^{-1}(x \star \alpha) &= L^{-1}\Big(b(x\alpha^{p^s} + x^{p^s}\alpha) + b^{p^k}(x^{p^k}\alpha^{p^{k+s}} + x^{p^{k+s}}\alpha^{p^k}) \\ &\quad +c(x\alpha^{p^k} + x^{p^k}\alpha) + \sum_{i=0}^{k-1} r_i(x^{p^i}\alpha^{p^{k+i}} + x^{p^{k+i}}\alpha^{p^i})\Big) \\ &= L^{-1}\Big(b\big(x\alpha + (x\alpha)^{p^s}\big) + b^{p^k}\big((x\alpha)^{p^k} + (x\alpha)^{p^{k+s}}\big) \\ &\quad +c\big(x\alpha + (x\alpha)^{p^k}\big) + \sum_{i=0}^{k-1} r_i\big((x\alpha)^{p^i} + (x\alpha)^{p^{k+i}}\big)\Big) \\ &= L^{-1}(L(\alpha x)) = \alpha x. \end{aligned} \quad (30)$$

Hence,

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

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

Proposition 8. *Let F be a PN function of the family* (ii*) *where $r_i = 0$ 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 (26)-(28) we are going to prove that equality (25) 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

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

Hence,

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

and using (30) we get

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

This proves equality (25). 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 $\gcd(s, k)$.

The functions of the family (iii*) define commutative semifields with similar properties.

Proposition 9. *Let F be a PN function of the family* (iii*)*. Then the orders of the middle and left nuclei of the commutative semifield defined by F are the* $\gcd(s,t)$*-th powers.*

Proof. For any $x, y \in \mathbf{F}_{p^{3t}}$ we denote

$$\begin{aligned} x \star y &= F(x+y) - F(x) - F(y) \\ &= xy^{p^s} + x^{p^s}y - a^{p^t-1}(x^{p^t}y^{p^{2t+s}} + x^{p^{2t+s}}y^{p^t}). \end{aligned} \tag{31}$$

and

$$L(x) = 1 \star x = x + x^{p^s} - a^{p^t-1}(x^{p^t} + x^{p^{2t+s}}). \tag{32}$$

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

$$x \circ y = L^{-1}(x) \star L^{-1}(y), \tag{33}$$

for any $x, y \in \mathbf{F}_{p^{3t}}$.

We are going to prove that for any $x, y \in \mathbf{F}_{p^{3t}}$ and any $\alpha \in \mathbf{F}_{p^{\gcd(s,t)}}$

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

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

$$L^{-1}(x \star \alpha) \star y = L^{-1}(y \star \alpha) \star x, \tag{34}$$
$$L^{-1}(x \star \alpha) \star y = L^{-1}(x \star y) \star \alpha. \tag{35}$$

Since $\alpha^{p^s} = \alpha^{p^t} = \alpha$ then

$$\begin{aligned} x \star \alpha &= x\alpha^{p^s} + x^{p^s}\alpha - a^{p^t-1}(x^{p^t}\alpha^{p^{2t+s}} + x^{p^{2t+s}}\alpha^{p^t}) \\ &= x\alpha + (x\alpha)^{p^s} - a^{p^t-1}\big((x\alpha)^{p^t} + (x\alpha)^{p^{2t+s}}\big) \\ &= L(\alpha x) = \alpha L(x). \end{aligned}$$

Thus,

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

and therefore

$$\begin{aligned} L^{-1}(x \star \alpha) \star y = (\alpha x) \star y &= \alpha x y^{p^s} + \alpha x^{p^s} y - a^{p^t-1}(\alpha x^{p^t} y^{p^{2t+s}} + \alpha x^{p^{2t+s}} y^{p^t}) \\ &= \alpha(x \star y) = L^{-1}(y \star \alpha) \star x = L^{-1}(x \star y) \star \alpha, \end{aligned}$$

which proves equalities (34) and (35).

Hence, $L(\mathbf{F}_{p^{\gcd(s,t)}})$ is contained in the left and middle nuclei of the semifield $\mathbf{S}_F$. Therefore, if p^{d_l} and p^{d_m} are the orders of the left and middle nuclei of $\mathbf{S}_F$, respectively, then d_l and d_m are divisible by $\gcd(s,t)$.

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. C. Bracken, E. Byrne, N. Markin, G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. To appear in *Finite Fields and Applications*, 2008.
5. L. Budaghyan, C. Carlet, G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 4218-4229, Sept. 2008.

6. 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.
7. L. Budaghyan and T. Helleseth. New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. *Proceedings of SETA 2008*, Lecture Notes in Computer Science 5203, pp. 401-414, 2008.
8. 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.
9. S. D. Cohen and M. J. Ganley. Commutative semifields, two-dimensional over there middle nuclei. *J. Algebra* 75, pp. 373-385, 1982.
10. R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des., Codes, Cryptogr.*, 10, pp. 167-184, 1997.
11. R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Advances in Math.* 217, pp. 282-304, 2008.
12. R. S. Coulter, M. Henderson, P. Kosick. Planar polynomials for commutative semifields with specified nuclei. *Des. Codes Cryptogr.* 44, pp. 275-286, 2007.
13. P. Dembowski and T. Ostrom. Planes of order n with collineation groups of order n^2. *Math. Z.*, 103, pp. 239-258, 1968.
14. L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc* 7, pp. 514-522, 1906.
15. L. E. Dickson. Linear algebras with associativity not assumed. *Duke Math. J.* 1, pp. 113-125, 1935.
16. C. Ding and J. Yuan. A new family of skew Paley-Hadamard difference sets. *J. Comb. Theory Ser. A*, 133, pp. 1526-1535, 2006.
17. M. J. Ganley. Central weak nucleus semifields. *European J. Combin.* 2, pp. 339-347, 1981.
18. 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.
19. T. Helleseth and D. Sandberg. Some power mappings with low differential uniformity. *Applic. Alg. Eng., Commun. Comput.*, vol. 8, pp. 363-370, 1997.
20. G. Kyureghyan and A. Pott. Some theorems on planar mappings. *Proceedings of WAIFI 2008*, Lecture Notes in Computer Science 5130, pp. 115-122, 2008.
21. K. Minami and N. Nakagawa. On planar functions of elementary abelian p-group type. Submitted.
22. N. Nakagawa. On functions of finite fields. Available at http://www.math.is.tohoku.ac.jp/ taya/sendaiNC/2006/report/nakagawa.pdf
23. G. J. Ness. Correlation of sequences of different lengths and related topics. PhD dissertation. University of Bergen, Norway, 2007
24. K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptography, EUROCRYPT'93, LNCS*, 765, pp. 55-64, 1994.
25. T. Penttila and B. Williams. Ovoids of parabolic spaces. *Geom. Dedicata* 82, pp. 1-19, 2000.
26. 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