On isotopisms of commutative presemifields and CCZ-equivalence of functions

Lilya Budaghyan and Tor Helleseth

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

Abstract. A function F from $\mathbf{F}_{p^n}$ to itself is planar if for any $a \in \mathbf{F}_{p^n}^*$ the function $F(x+a)-F(x)$ is a permutation. CCZ-equivalence is the most general known equivalence relation of functions preserving planar property. This paper considers two possible extensions of CCZ-equivalence for functions over fields of odd characteristics, one proposed by Coulter and Henderson and the other by Budaghyan and Carlet. We show that the second one in fact coincides with CCZ-equivalence, while using the first one we generalize one of the known families of PN functions. In particular, we prove that, for any odd prime p and any positive integers n and m, the indicators of the graphs of functions F and F' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ are CCZ-equivalent if and only if F and F' are CCZ-equivalent. We also prove that, for any odd prime p, CCZ-equivalence of functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$, is strictly more general than EA-equivalence when $n \geq 3$ and m is greater or equal to the smallest positive divisor of n different from 1.

Keywords: Commutative semifield, CCZ-equivalence, EA-equivalence, isotopism of presemifields, Perfect nonlinear, Planar function.

1 PN and APN functions

Let p be any prime number and n any positive integer. A function F from the field $\mathbf{F}_{p^n}$ to itself is called **planar** if all the equations

$$F(x+a)-F(x)=b, \qquad \forall a,b \in \mathbf{F}_{p^n}, a \neq 0, \tag{1}$$

have exactly one solution, that is, if for any non-zero element a of $\mathbf{F}_{p^n}$ the function $D_aF(x)=F(x+a)-F(x)$, called the **derivative of F in the direction of a**, is a permutation. Planar functions were introduced in 1968 by Dembowski and Ostrom [19] in context of finite geometry to describe projective planes with specific properties. Since 1991 planar functions have attracted interest also from cryptography as functions with optimal resistance to differential cryptanalysis. In this context they were first considered in the work of Nyberg [35] where they were given a new name "**perfect nonlinear**" (PN) which described their important cryptographic property of being as far as possible from being linear (in certain sense). However, it is obvious that planar or PN functions exist only for p odd since if p is even and x_0 is a solution of (1) then $x_0 + a$ is a solution too, and the functions, whose derivatives D_aF, $a \in \mathbf{F}_{p^n}^*$, are 2-to-1 mappings, possess the best possible resistance to differential cryptanalysis and are called **almost perfect nonlinear** (APN).

There are several equivalence relations of functions for which PN and APN properties are invariant. Due to these equivalence relations, having only one PN (or APN) function one can generate a huge class of PN (resp. APN) functions. The terminology for these equivalence relations was introduced in 2005 in [11] while the ideas behind this terminology go back to the works of Nyberg [36] and Carlet, Charpin and Zinoviev [14]. To continue we need first to recall the following definitions:

Definition 1. *A function F from $\mathbf{F}_{p^n}$ to itself is called*

- ***linear*** *if*
$$F(x) = \sum_{0 \le i < n} a_i x^{p^i}, \qquad a_i \in \mathbf{F}_{p^n};$$
- ***affine*** *if F is a sum of a linear function and a constant;*
- ***Dembowski-Ostrom polynomial*** *(DO polynomial) if*
$$F(x) = \sum_{0 \le k \le j < n} a_{kj} x^{p^k + p^j}, \quad a_{ij} \in \mathbf{F}_{p^n}; \tag{2}$$
- ***quadratic*** *if it is a sum of a DO polynomial and an affine function.*

Definitions for equivalences below are given for functions from $\mathbf{F}_{p^n}$ to itself. However they can be naturally extended to functions from A to B where A and B are arbitrary groups [11].

Definition 2. *Two functions F and F' from $\mathbf{F}_{p^n}$ to itself are called*

- ***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 of $\mathbf{F}_{p^n}$;*
- ***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 of $\mathbf{F}_{p^n}$;*
- ***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 $G_{F'} = \{(x, F'(x)) \mid x \in \mathbf{F}_{p^n}\}$.*

Although different these equivalence relations are connected to each other. It is obvious that linear equivalence is a particular case of affine equivalence, and

that affine equivalence is a particular case of EA-equivalence. As shown in [14] EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. For quite a long time it was believed that CCZ-equivalence class of an arbitrary function F can be completely described by means of EA-equivalence and of the inverses of permutations EA-equivalent to F. In [7, 11], it is proven to be false: CCZ-equivalence is much more general. As proven in [8], CCZ-equivalence is strictly more general than EA-equivalence for functions from $\mathbf{F}_{2^n}$ to $\mathbf{F}_{2^m}$ when $n \geq 5$ and m is greater or equal to the smallest positive divisor of n different from 1. In Section 6 of the present paper we prove a similar result for any odd prime p: CCZ-equivalence of functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$, is strictly more general than EA-equivalence when $n \geq 3$ and m is greater or equal to the smallest positive divisor of n different from 1.
However, there are particular cases of functions for which CCZ-equivalence can be reduced to EA-equivalence. For instance, CCZ-equivalence coincides with

- EA-equivalence for planar functions [12, 29];
- linear equivalence for DO planar functions [12];
- EA-equivalence for all functions whose derivatives are surjective [13];
- EA-equivalence for all Boolean functions [8];
- EA-equivalence for all vectorial bent functions with p even [9].

It is useful to know cases where CCZ- and EA-equivalences coincide because in general it is very difficult to determine whether two functions are CCZ-equivalent or not while EA-equivalence is much simpler and has a nice invariant, algebraic degree of a function.

Nowadays, CCZ-equivalence is the most general known equivalence relation of functions preserving PN and APN properties and it is appealing to find a more general equivalence for which PN and APN properties are invariants. The most intriguing possibility for such generalization is connected with isotopisms of commutative presemifields and is discussed in Sections 2 and 4 of the present paper. Other attempts in this direction were made in [8, 24]. In [8] the first author and Carlet consider two functions F and F' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ equivalent if the indicators of the graphs of F and F' are CCZ-equivalent. Recall that for a given function F from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ the indicator 1_{G_F} of its graph G_F is

$$1_{G_F}(x, y) = \begin{cases} 1 & \text{if} \quad y = F(x) \\ 0 & \text{otherwise} \end{cases} .$$

However, as proven in [8], for p even that equivalence coincides with original CCZ-equivalence of functions, and we prove in Section 5 of this paper that it coincides with CCZ-equivalence for p odd as well. In [24] Edel and Pott present so-called "switching construction" which is proven to be an appropriate method for constructing APN functions (see also [38] for the case of PN functions). Basing on this construction they define an equivalence relation, called switching equivalence, over APN functions. But when considered over all functions switching equivalence does not preserve APN property, that is, if two functions are switching equivalent and one of them is APN the second is not necessarily APN.

2 Commutative presemifields and semifields

As shown in [19, 17] quadratic planar functions have important connection with commutative semifields. 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 p is a prime, n is a positive integer, $(\mathbf{F}_{p^n}, +)$ 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 [17, 28]. The prime p is called the **characteristic** of $\mathbf{S}$. Any finite field is a semifield. A semifield which is not a field is called **proper**.

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**.

The investigation of commutative semifields was launched by Dickson [20, 21] in 1906, shortly after the classification of finite filds, and the first family of proper commutative semifields was constructed by him in 1935.

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 $N_l(\mathbf{S}) = N_r(\mathbf{S}) \subseteq N_m(\mathbf{S})$. The nuclei measure how far $\mathbf{S}$ is from being associative. *The orders of the respective nuclei are invariant under isotopism* [17].

Every commutative presemifield can be transformed into a commutative semifield. Indeed, 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 [17].

Every commutative presemifield defines a planar DO polynomial and vice versa [17]. Let F be a quadratic PN function 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 quadratic PN function** 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 [17].

We have the following known facts on connection between CCZ-equivalence, isotopisms and strong isotopisms:

- 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 [12];

- two commutative presemifields of order p^n with n odd are isotopic if and only if they are strongly isotopic [17];

- any commutative presemifield can generate at most two equivalence classes of planar DO polynomials [17];

- if $\mathbf{S}_1$ and $\mathbf{S}_2$ are isotopic commutative semifields of characteristic p with the order of the middle nuclei and nuclei p^m and p^k, respectively, then one of the following statements must hold
  (a) m/k is odd and $\mathbf{S}_1$ and $\mathbf{S}_2$ are strongly isotopic,
  (b) m/k is even and either $\mathbf{S}_1$ and $\mathbf{S}_2$ are strongly isotopic or the only isotopisms between $\mathbf{S}_1$ and $\mathbf{S}_2$ are of the form $(\alpha \star N, N, L)$ where α is a non-square element of $N_m(\mathbf{S}_1)$ [17] ;

- there exist two commutative semifields of order 3^6 which are isotopic but not strongly isotopic [41].

Thus, in the case n even it is possible that isotopic commutative presemifields define CCZ-inequivalent quadratic PN functions. However, isotopisms define an equivalence relation only over quadratic PN functions, and it is an open question whether this can be extended to an equivalence relation over all functions (from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ for any positive integers n, m, and any prime p) preserving differential properties.

3 Known cases of planar functions and commutative semifields

Almost all known planar functions are DO polynomials. The only known non-quadratic PN functions are the power functions

$$x^{\frac{3^t+1}{2}}$$

over $\mathbf{F}_{3^n}$, where t is odd and $\gcd(t,n)=1$ [16, 27]. Although commutative semifields have been intensively studied for more than a hundred years there are only a few cases of commutative semifields of odd order known (see [12, 17]):

(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, 19, 26];

(iii) the functions over $\mathbf{F}_{p^{2k}}$, which correspond to the Dickson semifields [21];

(iv) the functions over $\mathbf{F}_{p^{2k}}$

$$(ax)^{p^s+1} - (ax)^{p^k(p^s+1)} + \sum_{i=0}^{k-1} c_i x^{p^i(p^k+1)}, \tag{3}$$

$$bx^{p^s+1} + (bx^{p^s+1})^{p^k} + cx^{p^k+1} + \sum_{i=1}^{k-1} r_i x^{p^{k+i}+p^i}, \tag{4}$$

where $a, b \in \mathbf{F}^*_{p^{2k}}$, b is not a square, $c \in \mathbf{F}_{p^{2k}} \setminus \mathbf{F}_{p^k}$, $r_i \in \mathbf{F}_{p^k}$, $0 \le i < k$, $\sum_{i=0}^{k-1} c_i x^{p^i}$ is a permutation of $\mathbf{F}_{p^k}$ with coefficients in $\mathbf{F}_{p^k}$, $\gcd(k+s, 2k) = \gcd(k+s, k)$, and for (3) also $\gcd(p^s+1, p^k+1) \ne \gcd\big(p^s+1, (p^k+1)/2\big)$ (see [12, 13]);

(v) the function over $\mathbf{F}_{p^{2m}}$ for $m = 2k+1$ (see [30, 4])

$$\begin{aligned} F(x) = \; & x^2 + x^{2p^m} + \sum_{i=0}^{k} (-1)^i x^{p^{2i}(p^2+1)} + \sum_{j=0}^{k-1} (-1)^{k+j} x^{p^{2j+1}(p^2+1)} \\ & - \Big(\sum_{i=0}^{k} (-1)^i x^{p^{2i}(p^2+1)} + \sum_{j=0}^{k-1} (-1)^{k+j} x^{p^{2j+1}(p^2+1)} \Big)^{p^m}; \end{aligned}$$

(vi) $$x^{p^s+1} - a^{p^t-1} x^{p^t+p^{2t+s}}$$

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 [40]);

(vii)
$$x^{p^s+1} - a^{p^t-1}x^{p^{3t}+p^{t+s}}$$
over $\mathbf{F}_{p^{4t}}$, where a is primitive in $\mathbf{F}_{p^{4t}}$, $p^s \equiv p^t \equiv 1 \bmod 4$, $2t/\gcd(s,2t)$ is odd (see [3]);

(viii)
$$x^{10} \pm x^6 - x^2$$
over $\mathbf{F}_{3^n}$, with n odd, corresponding to the Coulter-Matthews and Ding-Yuan semifields [16, 23];

(ix) the function over $\mathbf{F}_{3^{2k}}$, with k odd, corresponding to the Ganley semifield [25];

(x) the function over $\mathbf{F}_{3^{2k}}$ corresponding to the Cohen-Ganley semifield [15];

(xi) the function over $\mathbf{F}_{3^{10}}$ corresponding to the Penttila-Williams semifield [37];

(xii) the function over $\mathbf{F}_{3^8}$ corresponding to the Coulter-Henderson-Kosick semifield [18];

(xiii)
$$x^2 + x^{90}$$
over $\mathbf{F}_{3^5}$ (see [39]).

The first seven cases above are defined for any odd prime p while the last six are defined only for $p = 3$. The polynomial representations of functions (iii), (viii)-(x) can be found in [32]. Note that PN functions (4) of family (iv) and families (vi) and (vii) were constructed by following patterns of some known families of APN functions over fields of even characteristic, see [6, 10]. In Section 4 we present a generalization of the function F of (v) for k odd case:

(v*) the function over $\mathbf{F}_{p^{2m}}$ for $m = 2k+1$, k odd, $a \in \mathbf{F}_{p^2}^*$,
$$\begin{aligned} F'(x) = \ & a^{1-p}x^2 + x^{2p^m} + a^{1-p}\sum_{i=0}^{k}(-1)^i x^{p^{2i}(p^2+1)} + \sum_{j=0}^{k-1}(-1)^{k+j}x^{p^{2j+1}(p^2+1)} \\ & -\Big(\sum_{i=0}^{k}(-1)^i x^{p^{2i}(p^2+1)} + a^{p-1}\sum_{j=0}^{k-1}(-1)^{k+j}x^{p^{2j+1}(p^2+1)}\Big)^{p^m} \end{aligned}$$
is PN.

We construct F' by using isotopisms. Hence, F' and F define isotopic semifields. Moreover, F and F' coincide for $a \in \mathbf{F}_p^*$. Nevertheless, for $a \in \mathbf{F}_{p^2} \setminus \mathbf{F}_p$, the functions F and F' are CCZ-inequivalent in general.

Further we have the following results on classification of commutative pre-semifields:

- any semifield of order p^2 is a finite field [28];

- any semifield of order p^3 is either a finite field or Albert's commutative twisted field [31];

- a commutative presemifield which is three dimensional over its middle nucleus is necessarily isotopic to Albert's commutative twisted field [31];

- Albert's commutative twisted fields have left and middle nuclei of order $p^{\gcd(t,n)}$ [2];

- Dickson semifields have middle nuclei of order p^k [22];

- for $a \in \mathbf{F}_{p^k}$ the commutative semifields corresponding to the functions (3) of the family (iv) have middle nuclei of order p^d where d is even and divisible by $\gcd(s,k)$ [9];

- a DO polynomial (2) is CCZ-inequivalent to the planar function x^2 if $a_{jj} = 0$ for all j [12];

- a DO polynomial (2) is CCZ-inequivalent to the planar function x^{p^t+1}, with $n/\gcd(t,n)$ odd, if $a_{kj} = 0$ for all k and $j = k \pm t \bmod n$ [12];

- for $p = 3$ and $n = 6$ semifield (v) is isotopic but not strongly isotopic one of the semifields (iv) [41].

4 On isotopisms of commutative presemifields

As mentioned in Section 2, under some condition on n, Coulter and Henderson proved in [17] that commutative presemifields of order p^n are isotopic if and only if they are strongly isotopic. However, there are cases when isotopic commutative presemifields define CCZ-inequivalent quadratic PN functions, as shown in [41] by using function (v) with parameters $p = 3$ and $k = 1$. Below we show that this example is generalizable for any odd prime p and any odd positive integer k. In particular, we extend the family of functions (v) to the family of the functions F' below with larger CCZ-equivalence class.

Let F be function (v) with k odd. Let "$*$" denotes the multiplication of $\mathbf{S}_F$, and $a \in \mathbf{F}_{p^2}^*$. Then we have

$$\begin{aligned} x * a = \; & F(x+a) - F(x) - F(a) \\ = \; & 2ax + 2a^p x^{p^m} + \sum_{i=0}^{k} (-1)^i (ax^{p^{2(i+1)}} + ax^{p^{2i}}) \\ & + \sum_{j=0}^{k-1} (-1)^{k+j} (a^p x^{p^{2(j+1)+1}} + a^p x^{p^{2j+1}}) \\ & - \Big(\sum_{i=0}^{k} (-1)^i (ax^{p^{2(i+1)}} + ax^{p^{2i}}) \end{aligned}$$

$$
\begin{aligned}
&+\sum_{j=0}^{k-1}(-1)^{k+j}(a^p x^{p^{2(j+1)+1}}+a^p x^{p^{2j+1}})\Big)^{p^m}\\
=\;& 2ax+2a^p x^{p^m}+(ax-ax^{p^{m+1}})+(-a^p x^p-a^p x^{p^m})\\
&-\Big((ax-ax^{p^{m+1}})+(-a^p x^p-a^p x^{p^m})\Big)^{p^m}\\
=\;& 4ax.
\end{aligned}
$$

And

$$
\begin{aligned}
F'(x) =\;& (x*a)*x=(4ax)*x\\
=\;& 4\Big(2ax^2+2a^p x^{2p^m}+2a\sum_{i=0}^{k}(-1)^i x^{p^{2i}(p^2+1)}\\
&+2a^p\sum_{j=0}^{k-1}(-1)^{k+j}x^{p^{2j+1}(p^2+1)}\\
&-\Big(2a\sum_{i=0}^{k}(-1)^i x^{p^{2i}(p^2+1)}+2a^p\sum_{j=0}^{k-1}(-1)^{k+j}x^{p^{2j+1}(p^2+1)}\Big)^{p^m}\Big)\\
=\;& 8a^p\Big(a^{1-p}x^2+x^{2p^m}+a^{1-p}\sum_{i=0}^{k}(-1)^i x^{p^{2i}(p^2+1)}\\
&+\sum_{j=0}^{k-1}(-1)^{k+j}x^{p^{2j+1}(p^2+1)}\\
&-\Big(\sum_{i=0}^{k}(-1)^i x^{p^{2i}(p^2+1)}+a^{p-1}\sum_{j=0}^{k-1}(-1)^{k+j}x^{p^{2j+1}(p^2+1)}\Big)^{p^m}\Big).
\end{aligned}
$$

Obviously, $\mathbf{S}_F$ and $\mathbf{S}_{F'}$ are isotopic by construction. According to Theorem 2.4 of [17], $\mathbf{S}_F$ and $\mathbf{S}_{F'}$ can be potentially non-strongly isotopic if $a \in N_m(\mathbf{S}_F)\setminus N(\mathbf{S}_F)$. It can be easily checked that $(x*a)*y=(4ax)*y=(4ay)*x=(y*a)*x$ for any $x,y\in\mathbf{F}_{p^{2m}}$. That is, $\mathbf{F}_{p^2}$ is a subset of $N_m(\mathbf{S}_F)$. On the other hand, $a*(x*y)=4a(x*y)$, and if $(4ax)*y=4a(x*y)$ for any $x,y\in\mathbf{F}_{p^{2m}}$, then the coefficient of the monomial $x^{p^m}y^{p^m}$ would be the same in $(4ax)*y$ and $4a(x*y)$, while it is $8a^p$ in the first one and $8a$ in the second. Hence, $a\in N_m(\mathbf{S}_F)\setminus N(\mathbf{S}_F)$ for $a\in\mathbf{F}_{p^2}\setminus\mathbf{F}_p$. According to [41], if $p=3$ and $m=3$ then $\mathbf{S}_F$ and $\mathbf{S}_{F'}$ are not strongly isotopic. Hence the function F' is a generalization of family (v): it coincides with F for $a\in\mathbf{F}_p^*$ and, in general, it is CCZ-inequivalent to F for $a\in\mathbf{F}_{p^2}\setminus\mathbf{F}_p$. Note that the function F' is constructed for k odd. However, for k even and $a\in\mathbf{F}_{p^2}\setminus\mathbf{F}_p$ the function F' may be PN as well (as checked for small values of p and k).

5 On CCZ-equivalence of the indicators of the graphs of functions of odd characteristics

The following natural generalization of CCZ-equivalence of functions was considered in [8]. Let n and m be any positive integers, p any prime. Two functions F and F' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ are considered equivalent if their graphs 1_{G_F} and $1_{G'_F}$ are CCZ-equivalent. However, as proven in [8], for p even this equivalence coincides with original CCZ-equivalence of functions. Below we prove that it coincides with CCZ-equivalence for p odd as well. First we need some auxiliary results.

Lemma 1. *Let p be an odd prime, n a positive integer, $a \in \mathbf{F}_{p^n}$ and f any function from $\mathbf{F}_{p^n}$ to itself with the image set $\{0, a\}$. If the function $F(x) = x + f(x)$ is a permutation of $\mathbf{F}_{p^n}$ then $x - f(x)$ is its inverse.*

Proof. Denoting $F'(x) = x - f(x)$ we get

$$F' \circ F(x) = x + f(x) - f(x + f(x)).$$

If $f(x) = 0$ then obviously $F' \circ F(x) = x$.
If $f(x) = a$ then $F' \circ F(x) = x + a - f(x + a)$. Moreover, we have $f(x + a) = a$ since otherwise $F(x + a) = F(x)$ which contradicts F being a permutation. Hence, when $f(x) = a$, we have also $F' \circ F(x) = x$. Therefore, $F^{-1} = F'$. □

As mentioned in [11], CCZ-equivalence can be considered not only for functions from $\mathbf{F}_{p^n}$ to itself but also for functions between arbitrary groups H_1 and H_2. In the following proposition we consider CCZ-equivalence of functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_2$.

Proposition 1. *Let p be an odd prime and n a positive integer. Two functions f and f' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_2$ are CCZ-equivalent if and only if $f' = f \circ A$ for some affine permutation A of $\mathbf{F}_{p^n}$.*

Proof. Let the functions f and f' be CCZ-equivalent. Then there exists an affine permutation $\mathcal{L}$ of $\mathbf{F}_{p^n} \times \mathbf{F}_2$ such that $\mathcal{L}(G_f) = G_{f'}$. Without loss of generality we can assume that $\mathcal{L}$ is linear. Then there exist linear functions $L : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$, $\phi : \mathbf{F}_2 \to \mathbf{F}_{p^n}$, $l : \mathbf{F}_{p^n} \to \mathbf{F}_2$ and an element $a \in \mathbf{F}_2$ such that

$$\mathcal{L}(x, y) = \big(L(x) + \phi(y), l(x) + ay\big),$$

and for

$$F_1(x) = L(x) + \phi \circ f(x),$$
$$F_2(x) = l(x) + af(x),$$

F_1 is a permutation of $\mathbf{F}_{p^n}$ and

$$f'(x) = F_2 \circ F_1^{-1}(x).$$

Note that any linear function l from $\mathbf{F}_p^n$ to $\mathbf{F}_2$ must be 0 since otherwise it is balanced which is impossible since p^n is an odd number. Hence, we have $l(x) = 0$ and, since $\mathcal{L}$ is a permutation, $a = 1$, that is, $F_2(x) = f(x)$. Besides, if $\phi \circ f = 0$ then obviously L is a permutation and $f' = f \circ L^{-1}$ and we can take $A = L^{-1}$. Hence we assume that ϕ has the image set $\{0, b\}$ where $b \neq 0$ and $\phi \circ f$ is not a zero function.
Since F_1 is a permutation and the image of $\phi \circ f$ consists of 2 elements then the function L must have at most 2 zeros, and, since $p \geq 3$ and L is a linear function from $\mathbf{F}_{p^n}$ to itself then it has exactly one zero, that is, L is a permutation. Hence,

$$F_1(x) = L\big(x + L^{-1} \circ \phi \circ f(x)\big),$$

where the function $F_1^*(x) = x + L^{-1} \circ \phi \circ f(x)$ is a permutation too, and therefore, by Lemma 1 its inverse is $F_1^{*-1}(x) = x - L^{-1} \circ \phi \circ f(x)$. We get

$$F_1^{-1}(x) = F_1^{*-1} \circ L^{-1}(x)$$

and then

$$f' \circ L(x) = F_2 \circ F_1^{*-1}(x) = f\big(x - L^{-1} \circ \phi \circ f(x)\big).$$

If $f(x) = 0$ then $f' \circ L(x) = 0 = f(x)$.
If $f(x) = 1$ then we have $f(x - L^{-1}(b)) = 1 = f(x)$. Indeed, if $f(x) = 1$ and $f(x - L^{-1}(b)) = 0$ then

$$F^{*-1}\big(x - L^{-1}(b)\big) = x - L^{-1}(b) - L^{-1} \circ \phi \circ f\big(x - L^{-1}(b)\big) = x - L^{-1}(b),$$
$$F^{*-1}(x) = x - L^{-1} \circ \phi \circ f(x) = x - L^{-1}(b),$$

which contradict F^{*-1} being a permutation. Hence, $f' \circ L(x) = f(x)$ and we can take $A = L^{-1}$. □

Now we can proof the main result of this section:

Theorem 1. *Let n and m be any positive integers, p any prime, and F and F' any functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$. Then F and F' are CCZ-equivalent if and only if the indicators of their graphs 1_{G_F} and $1_{G_{F'}}$ are CCZ-equivalent.*

Proof. For the case p even this theorem states Corollary 1 of [8]. Let p be odd. Since 1_{G_F} and $1_{G_{F'}}$ are functions from $\mathbf{F}_{p^n} \times \mathbf{F}_{p^m}$ to $\mathbf{F}_2$ then according to Proposition 1 they are CCZ-equivalent if and only if there exists an affine permutation A of $\mathbf{F}_{p^n} \times \mathbf{F}_{p^m}$ that $1_{G_{F'}} = 1_{G_F} \circ A$, that is, if and only if F and F' are CCZ-equivalent. □

6 Relation between CCZ-equivalence and EA-equivalence for functions of odd characteristics

Let p be any prime and n any positive integer. Any function $F : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ is uniquely represented as a univariate polynomial over $\mathbf{F}_{p^n}$ of degree smaller than p^n

$$F(x) = \sum_{i=0}^{p^n-1} c_i x^i, \quad c_i \in \mathbf{F}_{p^n}.$$

If m is a divisor of n then a function F from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ can be viewed as a function from $\mathbf{F}_{p^n}$ to itself and, therefore, it admits a univariate polynomial representation. More precisely, if $\mathrm{tr}_n(x)$ denotes the trace function from $\mathbf{F}_{p^n}$ into $\mathbf{F}_p$, and $\mathrm{tr}_n^m(x)$ denotes the trace function from $\mathbf{F}_{p^n}$ into $\mathbf{F}_{p^m}$, that is,

$$\mathrm{tr}_n(x) = x + x^p + x^{p^2} + ... + x^{p^{n-1}},$$
$$\mathrm{tr}_n^m(x) = x + x^{p^m} + x^{p^{2m}} + ... + x^{p^{(n/m-1)m}},$$

then F can be represented in the form $\mathrm{tr}_n^m(\sum_{i=0}^{p^n-1} c_i x^i)$ (and in the form $\mathrm{tr}_n(\sum_{i=0}^{p^n-1} c_i x^i)$ for $m = 1$). Indeed, there exists a function G from $\mathbf{F}_{p^n}$ to itself (for example $G(x) = aF(x)$, where $a \in \mathbf{F}_{p^n}$ and $\mathrm{tr}_n^m(a) = 1$) such that F equals $\mathrm{tr}_n^m(G(x))$.

Let k be an integer such that $0 \le k < p^n$. Then $k = \sum_{s=0}^{n-1} p^s k_s$ for some $0 \le k_s < p$. We call the integer $w_p(k) = \sum_{s=0}^{n-1} k_s$ th p-weight of k. The algebraic degree of a function $F : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$ is equal to the maximum p-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$, that is,

$$d^\circ(F) = \max_{0 \le i < p^n,\ c_i \neq 0} w_p(i).$$

The algebraic degree of a function (if it is not linear) is invariant under EA-equivalence but it is not preserved by CCZ-equivalence.

For functions of even characteristics the following theorem is proven in [8]:

Theorem 2. [8] *Let $n \ge 5$ and $k > 1$ be the smallest divisor of n. Then for any $m \ge k$ CCZ-equivalence for functions from $\mathbf{F}_{2^n}$ to $\mathbf{F}_{2^m}$ is strictly more general than EA-equivalence.*

We are going to obtain an analogue of this theorem for functions of odd characteristics.

Proposition 2. *Let p be an odd prime, $n \ge 3$, and $m > 1$ be a divisor of n. Then there exist functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ for which CCZ-equivalence is strictly more general than EA-equivalence.*

Proof. The linear permutation of $\mathbf{F}_{p^n} \times \mathbf{F}_{p^m}$

$$\mathcal{L}(x, y) = (x + \mathrm{tr}_m(y),\ y)$$

maps the graph of a quadratic function $F : \mathbf{F}_{p^n} \to \mathbf{F}_{p^m}$

$$F(x) = \mathrm{tr}_n^m(x^2 - x^{p+1})$$

to the graph of a cubic function

$$F'(x) = \mathrm{tr}_n^m(x^2 - x^{p+1}) + \mathrm{tr}_n(x^2 - x^{p+1})\mathrm{tr}_n^m(x^p - x).$$

That is, the functions F and F' are CCZ-equivalent but EA-inequivalent.

Indeed, $\mathcal{L}$ is obviously a permutation since $(0,0)$ is the only solution of the system

$$\begin{aligned} x + \mathrm{tr}_m(y) &= 0, \\ y &= 0. \end{aligned}$$

The function

$$F_1(x) = x + \mathrm{tr}_m(F(x)) = x + \mathrm{tr}_n(x^2 - x^{p+1})$$

is a permutation of $\mathbf{F}_{p^n}$ since for any $a \in \mathbf{F}_{p^n}^*$

$$\begin{aligned} F(x+a) - F(x) = {} & x + a + \mathrm{tr}_n(x^2 + 2ax + a^2 - x^{p+1} - ax^p - a^p x - a^{p+1}) \\ & -x - \mathrm{tr}_n(x^2 - x^{p+1}) \\ = {} & a + \mathrm{tr}_n(a^2 - a^{p+1}) - \mathrm{tr}_n(x(a^p + a^{p^{n-1}} - 2a)) \end{aligned}$$

and the equality $F(x+a) = F(x)$ would imply $a + \mathrm{tr}_n(a^2 - a^{p+1}) = \mathrm{tr}_n(x(a^p + a^{p^{n-1}} - 2a))$, that is, $a \in \mathbf{F}_p^*$, that is, $a = 0$, a contradiction. Note further that the inverse of the function F_1 is

$$F_1^{-1}(x) = x - \mathrm{tr}_n(x^2 - x^{p+1})$$

since

$$\begin{aligned} F_1^{-1} \circ F_1(x) = {} & x + \mathrm{tr}_n(x^2 - x^{p+1}) - \mathrm{tr}_n\Big(x^2 + 2x\ \mathrm{tr}_n(x^2 - x^{p+1}) \\ & + \mathrm{tr}_n(x^2 - x^{p+1})^2 - x^{p+1} - x^p\ \mathrm{tr}_n(x^2 - x^{p+1}) \\ & - x\ \mathrm{tr}_n(x^2 - x^{p+1})^p - \mathrm{tr}_n(x^2 - x^{p+1})^{p+1}\Big) \\ = {} & x - \mathrm{tr}_n(x^2 - x^{p+1})\ \mathrm{tr}_n(x - x^p) = x. \end{aligned}$$

Hence, for $F_2(x) = F(x)$ we get

$$\begin{aligned} F_2 \circ F_1^{-1}(x) &= \mathrm{tr}_n^m\Big(\big(x - \mathrm{tr}_n(x^2 - x^{p+1})\big)^2 - \big(x - \mathrm{tr}_n(x^2 - x^{p+1})\big)^{p+1}\Big) \\ &= \mathrm{tr}_n^m(x^2 - x^{p+1}) + \mathrm{tr}_n(x^2 - x^{p+1})\mathrm{tr}_n^m(x^p - x) = F'(x). \end{aligned}$$

It is easy to check that for $m \geq 2$ and $n \geq 3$ the term x^{2p+1} has coefficient -2 in the polynomial representation of F'. Hence, F' has algebraic degree 3. By construction F and F' are CCZ-equivalent but they are EA-inequivalent because of the difference of their algebraic degrees. $\square$

Next proposition was proven in [8] for p even case but the proof works for any prime p.

Proposition 3. [8] *Let p be a prime, n and m any positive integers. If there exist CCZ-equivalent functions F and F' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ which are EA-inequivalent then for any positive integer k the functions $H(x) = (F(x), 0)$ and $H'(x) = (F'(x), 0)$ from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^{m+k}}$ are also CCZ-equivalent and EA-inequivalent.*

Proposition 2 and Proposition 3 give

Theorem 3. *Let p be an odd prime, $n \geq 3$ and $k > 1$ the smallest divisor of n. Then for any $m \geq k$, CCZ-equivalence of functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ is strictly more general than their EA-equivalence.*

Acknowledgments

We thank Claude Carlet and Alexander Pott for useful comments.

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. J. Bierbrauer. New semifields, PN and APN functions. Designs, Codes and Cryptography, v. 54, pp. 189 - 200, 2010.
4. J. Bierbrauer. New commutative semifields from projection mappings. Manuscript, 2010.
5. E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology **4**, no. 1, pp. 3-72, 1991.
6. C. Bracken, E. Byrne, N. Markin, G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. Finite Fields and Their Applications **14**(3), pp. 703-714, 2008.
7. L. Budaghyan. The Simplest Method for Constructing APN Polynomials EA-Inequivalent to Power Functions. Proceedings of First International Workshop on Arithmetic of Finite Fields, WAIFI 2007, Lecture Notes in Computer Science **4547**, pp. 177-188, 2007.
8. L. Budaghyan and C. Carlet. CCZ-equivalence of single and multi output Boolean functions. "Contemporary Mathematics" of American Mathematical Society, 2010, (to appear).
9. L. Budaghyan and C. Carlet. On CCZ-equivalence and its use in secondary constructions of bent functions. Preproceedings of International Workshop on Coding and Cryptography WCC 2009, pp. 19-36, 2009.
10. L. Budaghyan, C. Carlet, G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inform. Theory **54**, no. 9, pp. 4218-4229, 2008.
11. L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. IEEE Trans. Inform. Theory **52**, no. 3, pp. 1141-1152, 2006.
12. L. Budaghyan and T. Helleseth. New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. Proceedings of International Conference on Sequences and Their Applications SETA 2008, Lecture Notes in Computer Science **5203**, pp. 401-414, 2008.
13. L. Budaghyan and T. Helleseth. New commutative semifields defined by new PN multinomials. Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences, 2010, (to appear).
14. 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.

15. S. D. Cohen and M. J. Ganley. Commutative semifields, two-dimensional over there middle nuclei. J. Algebra **75**, pp. 373-385, 1982.
16. R. S. Coulter and R. W. Matthews. Planar functions and planes of Lenz-Barlotti class II. Des., Codes, Cryptogr. **10**, pp. 167-184, 1997.
17. R. S. Coulter and M. Henderson. Commutative presemifields and semifields. Advances in Math. **217**, pp. 282-304, 2008.
18. R. S. Coulter, M. Henderson, P. Kosick. Planar polynomials for commutative semifields with specified nuclei. Des. Codes Cryptogr. **44**, pp. 275-286, 2007.
19. P. Dembowski and T. Ostrom. Planes of order n with collineation groups of order n^2. Math. Z. **103**, pp. 239-258, 1968.
20. L. E. Dickson. Linear algebras in which division is always uniquely possible. Trans. Amer. Math. Soc **7**, pp. 370-390, 1906.
21. L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. Trans. Amer. Math. Soc **7**, pp. 514-522, 1906.
22. L. E. Dickson. Linear algebras with associativity not assumed. Duke Math. J. **1**, pp. 113-125, 1935.
23. C. Ding and J. Yuan. A new family of skew Paley-Hadamard difference sets. J. Comb. Theory Ser. A **133**, pp. 1526-1535, 2006.
24. Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications **3**, no. 1, pp. 59-81, 2009.
25. M. J. Ganley. Central weak nucleus semifields. European J. Combin. **2**, pp. 339-347, 1981.
26. 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.
27. T. Helleseth and D. Sandberg. Some power mappings with low differential uniformity. Applic. Alg. Eng., Commun. Comput. **8**, pp. 363-370, 1997.
28. D. E. Knuth. Finite semifields and projective planes. J. Algebra **2**, pp. 182-217, 1965.
29. G. Kyureghyan and A. Pott. Some theorems on planar mappings. Proceedings of International Workshop on Arithmetic of Finite Fields, WAIFI 2008, Lecture Notes in Computer Science **5130**, pp. 115-122, 2008.
30. G. Lunardon, G. Marino, O. Polverion, R. Trombetti. Symplectic spreads and quadric Veroneseans. Manuscript, 2009.
31. G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. J. Algebra **47**, pp. 400-410, 1977.
32. K. Minami and N. Nakagawa. On planar functions of elementary abelian p-group type. Submitted.
33. N. Nakagawa. On functions of finite fields. Available at http://www.math.is.tohoku.ac.jp/ taya/sendaiNC/2006/report/nakagawa.pdf
34. G. J. Ness. Correlation of sequences of different lengths and related topics. PhD dissertation. University of Bergen, Norway, 2007.
35. K. Nyberg. Perfect nonlinear S-boxes. Advances in Cryptography, EUROCRYPT'91, Lecture Notes in Computer Science **547**, pp. 378-386, 1992.
36. K. Nyberg. Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science **765**, pp. 55-64, 1994.
37. T. Penttila and B. Williams. Ovoids of parabolic spaces. Geom. Dedicata **82**, pp. 1-19, 2000.
38. A. Pott and Y. Zhou. Switching Construction of Planar Functions on Finite Fields. Proceedings of WAIFI 2010, LNCS, v. 6087/2010, pp. 135-150, 2010.

39. G. Weng. Private communications, 2007.
40. Z. Zha, G. Kyureghyan, X. Wang. Perfect nonlinear binomials and their semifields. Finite Fields and Their Applications **15**(2), pp. 125-133, 2009.
41. Y. Zhou. A note on the isotopism of commutative semifields. Preprint, 2010.