On Isotopic Shift Construction for Planar Functions

(An extended abstract)

Lilya Budaghyan, Marco Calderini
Department of Informatics
University of Bergen
Bergen, NORWAY
Email: {lilya.budaghyan, marco.calderini}@uib.no

Claude Carlet
LAGA, University of Paris 8,
Paris, FRANCE
and Department of Informatics
University of Bergen
Bergen, NORWAY
Email: claude.carlet@gmail.com

Robert Coulter
University of Delaware,
Newark, Delaware USA
Email: coulter@udel.edu

Irene Villa
Department of Informatics
University of Bergen
Bergen, NORWAY
Email: irene.villa@uib.no

Abstract—**CCZ-equivalence is the most general currently known equivalence relation for functions over finite fields preserving planarity and APN properties. However, for the particular case of quadratic planar functions isotopic equivalence is more general than CCZ-equivalence. A recent construction method for APN functions over fields of even characteristic, so-called isotopic shift construction, was instigated by the notion of isotopic equivalence. In this paper we discuss possible applications of the idea of isotopic shift for the case of planar functions. We show that, surprisingly, some of the known planar functions are actually isotopic shifts of each other. This confirms practically the pertinence of the notion of isotopic shift not only for APN functions but also for planar maps.**

I. Introduction

Let p be a prime number and n a positive integer. Then $\mathbb{F}_{p^n}$ denotes the finite field with p^n elements and $\mathbb{F}_{p^n}^\star = \mathbb{F}_{p^n} \setminus \{0\}$ is its multiplicative group. Throughout the paper, ζ denotes a primitive element of $\mathbb{F}_{p^n}$, in particular $\mathbb{F}_{p^n}^\star = \langle \zeta \rangle$. Any map F defined from $\mathbb{F}_{p^n}$ to itself can be represented as a univariate polynomial of degree at most $p^n - 1$, $F \in \mathbb{F}_{p^n}[x]$

$$F(x) = \sum_{j=0}^{p^n-1} a_j x^j, \qquad a_j \in \mathbb{F}_{p^n}.$$

Given a function F we set $\ker(F)$ to be the set of zeros of F over $\mathbb{F}_{p^n}$.

Based on its structure, a function F is called

- *linear* if $F(x) = \sum_{i=0}^{n-1} c_i x^{p^i}$;
- *affine* if it is the sum of a linear function and a constant;
- *DO* (Dembowski-Ostrom) *polynomial* if $F(x) = \sum_{0 \leq i \leq j < n} a_{ij} x^{p^i + p^j}$, with $a_{ij} \in \mathbb{F}_{p^n}$ (for $p = 2$ there is a restriction $i \neq j$);
- *quadratic* if it is the sum of a DO polynomial and an affine function.

If for any $a \in \mathbb{F}_{p^n}^\star$ and $b \in \mathbb{F}_{p^n}$ the equation $F(x+a) - F(x) = b$ admits at most δ solutions, for δ a positive integer, then the function F is called *differentially δ-uniform.* When F is used as an S-box inside a cryptosystem, the differential uniformity measures its resistance to the differential attack [4]. Small values of δ lead to a better contribution of F used as S-box in a cryptosystem to the resistance against this attack. In this sense, 1-uniform functions are optimal and they are called *perfect nonlinear* or PN. Hence, defining $D_aF(x) = F(x+a) - F(x)$ the *derivative of F in the direction of a*, a given function F is PN if and only if, for any nonzero a, the function $D_aF(x)$ is a bijection. PN functions are also called *planar.* In even characteristic such functions do not exist. In this case, the best resistance belongs to functions that are differentially 2-uniform, these functions are called *almost perfect nonlinear* or APN. Notice that PN and APN functions have been also employed to construct message authentication codes (see for instance [10], [15]).

There are several equivalence relations of functions for which the PN and APN properties are preserved. Two functions F and F' from $\mathbb{F}_{p^n}$ to itself are called:

- affine equivalent if $F' = A_1 \circ F \circ A_2$ where $A_1, A_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ are affine permutations;
- EA-equivalent if $F' = F'' + A$, where the map $A : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is affine and F'' is affine equivalent to F;
- CCZ-equivalent if there exists some affine permutation $\mathcal{L}$ of $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ such that the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$, where $G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$ and $G_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{p^n}\}$.

CCZ-equivalence is the most general known equivalence relation for functions which preserves PN and APN properties while affine and EA-equivalences are its particular cases. However, for the particular case of quadratic planar functions so-called isotopic equivalence is more general than CCZ-equivalence [9]. Inspired by the notion of isotopic equivalence, a new construction method for APN functions, called isotopic shift, was introduced in [5]. Given a function $F \in \mathbb{F}_{p^n}[x]$ and a linear map $L \in \mathbb{F}_{p^n}[x]$ the *isotopic shift* of F by L is defined as the map

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)). \qquad (1)$$

In [5], it is proved that if F and G are isotopic equivalent quadratic PN functions, then G is EA-equivalent to an isotopic shift of F by some linear permutation L. We will show below that the converse does not hold, that is, an isotopic shift of a quadratic planar function by a linear permutation does not necessarily produce an isotopic equivalent function (and it is not always planar either).

As we have shown in [5], for the case $p = 2$, an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original function. In particular, all quadratic APN functions over $\mathbb{F}_{2^6}$ can be obtained from x^3 by isotopic shift, and a new family of quadratic APN functions is constructed over $\mathbb{F}_{2^n}$ for n divisible by 3 by isotopic shift of Gold functions [5]. Some generalizations of the isotopic shift for the case of APN functions over a field of characteristic 2 are discussed in [6].

In this work we will extend the isotopic shift construction of APN functions given in [5] for the even charecteristics to the case of odd charecteristics for PN functions. For a Gold-like PN functions (i.e x^{p^i+1}) we will also generalize the result obtained in [6], that is we study the PN property for some particular functions of the type

$$F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i},$$

with L_1 and L_2 linearized polynomials. From the latter construction we obtain some results on PN functions of the type $xL(x)$ with L linear. Some PN functions of this type are also studied in [19], [20] . In the last part we report some computational results and conclusions.

II. On the linear shifts in fields of odd characteristic

As shown in [5], with the isotopic shift of an APN function it is possible to obtain a CCZ-inequivalent APN function. This is also true for the case of PN function. For example, consider the planar quadratic function $F(x) = x^2$, defined over any finite field of odd characteristic. Consider its isotopic shift by the linear permutation $L(x) = x^{p^j}$.

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)) = 2x^{p^j+1}.$$

Now, F_L is PN over $\mathbb{F}_{p^n}$ if and only if $\frac{n}{\gcd(n,j)}$ is odd. Therefore we have an example of isotopic shift F_L that is not PN and also an example of isotopic shift that is PN and isotopic inequivalent to F.

Proposition II.1. *Given $F, L \in \mathbb{F}_{p^n}[x]$, where L is a linear function which is not a permutation, the map F_L is not PN.*

Proof. Without loss of generality assume $F(0) = 0$. Given $F_L(x)$ as in (1), the function is PN if and only if for any element $e \neq 0$ $D_e F_L(x) = F_L(x+e) - F_L(x)$ is a permutation. Equivalently we can consider $\Delta_e(x) = D_e F_L(x) - F_L(e)$ to be a permutation. Since L is not a permutation, there exists $z \neq 0$ such that $L(z) = 0$. Then, $\Delta_z(z) = F_L(2z) - 2F_L(z) = 0 = \Delta_z(0)$ since $F_L(2z) = F_L(z) = 0$. □

Remark II.2. *If F is not PN, then it is still possible to construct a planar isotopic shift F_L. Consider the finite field $\mathbb{F}_{3^4}$ and the non-PN function $F(x) = x^{3+1} = x^4$. With the linear permutation $L(x) = x^{27} + \zeta^4 x^3$ we construct*

$$F_L(x) = x^3 L(x) + x L(x)^3 = x^{30} + \zeta^4 x^6 + x^2 + \zeta^{12} x^{10},$$

that is PN. This function is CCZ-equivalent to the Dickson function $L(t^2(x)) + \frac{1}{2}x^2$ with $L(x) = \frac{1}{8}(x^3 - x)$ and $t(x) = x^{3^2} - x$.

Similarly to the case of finite fields with even characteristic we have the following proposition.

Proposition II.3. *For a monomial DO polynomial $F(x)$ and a linear function $L(x) = \sum_{j=0}^{n-1} b_j x^{p^j}$, the isotopic shift $F_L(x)$ is affine equivalent to the isotopic shift $F_M(x)$ constructed with the linear function*

$$M(x) = \sum_{j=0}^{n-1} (b_j \zeta^{k(p^j-1)})^{p^t} x^{p^j},$$

where k and t can be any integers. Moreover, for any function F, if L is a permutation, then $F_L(x)$ is affine equivalent to $F_{L^{-1}}(x)$.

Proof. Without loss of generality let $F(x) = x^{p^i+1}$. Then, we have

$$F_M(x) = \sum_{j=0}^{n-1} [(b_j \zeta^{k(p^j-1)})^{p^t} x^{p^i+p^j} + (b_j \zeta^{k(p^j-1)})^{p^{i+t}} x^{p^{j+i}+1}]$$

and

$$\begin{aligned}
&(\zeta^{kp^t(1+p^i)} F_M(\zeta^{-kp^t} x^{p^t}))^{p^{-t}} = \\
=&\zeta^{k(1+p^i)} [\zeta^{-kp^i} x^{p^i} M(\zeta^{-kp^t} x^{p^t}))^{p^{-t}} \\
&+ \zeta^{-k} x M(\zeta^{-kp^t} x^{p^t}))^{p^{i-t}}] \\
=&\zeta^{k(1+p^i)} \sum [\zeta^{-kp^i} x^{p^i} b_j \zeta^{k(p^j-1)} \zeta^{-kp^j} x^{p^j} + \\
&+ \zeta^{-k} x b_j^{p^i} \zeta^{k(p^j-1)p^i} \zeta^{-kp^j p^i} x^{p^j p^i}] \\
=&\zeta^{k(1+p^i)} \sum [\zeta^{-k(p^i+1)} b_j x^{p^j+p^i} + \zeta^{-k(p^i+1)} b_j^{p^i} x^{p^j p^i+1}] \\
=&\sum [b_j x^{p^j+p^i} + b_j^{p^i} x^{p^{j+i}+1}] = F_L(x).
\end{aligned}$$

For the last part, it is easy to check that if L is a permutation, then $F_L(L^{-1}(x)) = F_{L^{-1}}(x)$. □

A. Comparison on linear shifts in odd and even characteristic

Assume F is a quadratic polynomial satisfying $F(0) = 0$ and L a linear function over $\mathbb{F}_{p^n}$ where p is odd. Let $\Delta(y, x)$ be the symmetric bilinear operator

$$\Delta(y, x) = F(x + y) - F(x) - F(y).$$

Then

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)) = \Delta(L(x), x)$$

is an isotopic shift of a quadratic polynomial and then is a DO polynomial itself, and its differential property is given by $\Delta(c, L(x)) + \Delta(L(c), x)$ for $c \neq 0$. Indeed, since $\Delta(y, x)$ is symmetric and bilinear we have

$$\begin{aligned}
&F_L(x + c) - F_L(x) - F_L(c) = \\
=&\Delta(L(x + c), x + c) - \Delta(L(x), x) - \Delta(L(c), c) \\
=&\Delta(L(x), x) + \Delta(L(c), x) + \Delta(L(x), c) + \\
&\Delta(L(c), c) - \Delta(L(x), x) - \Delta(L(c), c) \\
=&\Delta(c, L(x)) + \Delta(L(c), x).
\end{aligned}$$

In order F_L to be PN we want that

$$\text{for any } c \neq 0 \qquad |\mathfrak{Im}(\Delta(c, L(x)) + \Delta(L(c), x))| = p^n,$$

where $\mathfrak{Im}(\cdot)$ is the image set. In particular we have the following.

Proposition II.4. *Given $F, L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ where F is a quadratic polynomial satisfying $F(0) = 0$ and L is a linear map, consider the isotopic shift of F by L, F_L defined as in* (1). *If the map F_L is PN then for any element $c \neq 0$ we have*

$$ker(\Delta(c, L(x))) \cap ker(\Delta(L(c), x)) = \{0\}.$$

Moreover, L is a permutation.

In the following table we compare the characteristics of the linear functions L for the case p even and p odd.

	p **even**
if	F_L is APN
then	
$\forall c \in \mathbb{F}^{\star}_{p^n}$	$\Delta(c, L(x)) + \Delta(L(c), x)$ 2-to-1
	L 1-to-1 or 2-to-1
	if $ker(L) = \{0, z\}$ then $\Delta(z, L(c)) \neq 0$ $\forall c \neq 0, z$
	$ker(\Delta(c, L(x))) \cap ker(\Delta(L(c), x)) = \{0, c\}$

	p **odd**
if	F_L is PN
then	
$\forall c \in \mathbb{F}^{\star}_{p^n}$	$\Delta(c, L(x)) + \Delta(L(c), x)$ 1-to-1
	L 1-to-1
	$\Delta(c, L(c)) \neq 0$ $(F_L(c) \neq 0)$
	$ker(\Delta(c, L(x))) \cap ker(\Delta(L(c), x)) = \{0\}$

III. Generalized isotopic shift for PN maps over fields of odd characteristic

In this section we extend the result obtained in [6] to the case of PN functions. Let us consider two linear maps

$$L_1(x) = \sum_{j=0}^{k-1} A_j x^{p^{jm}} \text{ and } L_2(x) = \sum_{j=0}^{k-1} B_j x^{p^{jm}}$$

defined over the finite field $\mathbb{F}_{p^{km}}$ and construct the function

$$F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i}.$$

A necessary condition for F' to be PN is the following.

Proposition III.1. *Over $\mathbb{F}_{p^{km}}$, for two integer m, k, consider the function*

$$F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i},$$

where $L_1, L_2 \in \mathbb{F}_{p^{km}}[x]$ are p^m-linear polynomial. Then F can be PN only if $\frac{m}{\gcd(i,m)}$ is odd.

Proof. Since F is PN then for any $e \in \mathbb{F}^{\star}_{p^{km}}$ the function $\Delta_e(x) = F(x + e) - F(x) - F(e)$ is a permutation. In particular, for any $e \in \mathbb{F}^{\star}_{p^m}$ we have

$$\Delta_e(1) = (L_1(1)^{p^i} + L_2(1))(e^{p^i} + e).$$

Since $\Delta_e(0) = 0$, in order to be PN $\Delta_e(1)$ must be different from 0, implying that $e^{p^i} \neq -e$, for any $e \in \mathbb{F}^{\star}_{p^m}$. This implies that $\frac{m}{\gcd(i,m)}$ is odd. □

Remark III.2. *Note that for this construction, the necessary condition $\frac{m}{\gcd(i,m)}$ odd implies that x^{p^i+1} is PN over the subfield $\mathbb{F}_{p^m}$, but it could be not PN over $\mathbb{F}_{p^{km}}$.*

As for the case of even characteristic, let $W = \{y\zeta^j : y \in U, 0 \leq j \leq d' - 1\}$, where $U = \langle \zeta^{d'(p^m-1)} \rangle$, $d = \gcd(p^m - 1, \frac{p^{km}-1}{p^m-1})$ and d' is an integer with the same prime factor as d, each being raised at the power as in $\frac{p^{km}-1}{p^m-1}$ (hence such that $\gcd(p^m - 1, \frac{p^{km}-1}{d'(p^m-1)}) = 1$). We obtain the following result. (The proof use similar ideas as in [5]).

Theorem III.3. *Over $\mathbb{F}_{p^{km}}$, where k and m are positive integers, let i be a positive integer such that $\frac{m}{\gcd(m,i)}$ is odd and consider two p^m-linear polynomials L_1, L_2. Then the function $F(x) = L_1(x)^{p^i} x + L_2(x) x^{p^i}$ is PN if and only if the following conditions are satisfied:*

(i) *for any $t \in W$ $F(t) \neq 0$;*
(ii) *for any $t, v \in W$ if $L_1(t)^{p^i} v + L_2(v) t^{p^i} = 0$ then $L_1(v)^{p^i} t + L_2(t) v^{p^i} \neq 0$;*
(iii) *for any $t, v \in W$ and any $r \in \mathbb{F}^{\star}_{p^m}$ if $L_1(t)^{p^i} v + L_2(v) t^{p^i} \neq 0$ then $\frac{L_1(v)^{p^i} t + L_2(t) v^{p^i}}{L_1(t)^{p^i} v + L_2(v) t^{p^i}} \neq (r)^{p^i-1}$.*

Sketch of proof. To be PN, we need that for any $e \in \mathbb{F}^{\star}_{p^{km}}$ the function $\Delta_e(x) = F(x + e) - F(x) - F(e)$ is a permutation (or equivalently 0 is the only root of $\Delta_e(x)$). Since $\mathbb{F}^{\star}_{p^{km}} = W \times \mathbb{F}^{\star}_{p^m}$ then we can rewrite $e = st$ and $x = uv$ with $s, u \in \mathbb{F}^{\star}_{p^m}$ and $t, v \in W$. Hence,

$$\begin{aligned} \Delta_e(x) =& us[s^{p^i-1}(L_1(t)^{p^i} v + L_2(v) t^{p^i}) \\ &+ u^{p^i-1}(L_1(v)^{p^i} t + L_2(t) v^{p^i})]. \end{aligned}$$

If $v = t$, then $\Delta_e(x) \neq 0$ is equivalent to (i).
For the case $v \neq t$, when $L_1(t)^{p^i} v + L_2(v) t^{p^i} = 0$, $\Delta_e(x) \neq 0$ if and only if (ii) holds. While, if $L_1(t)^{p^i} v + L_2(v) t^{p^i} \neq 0$ then Condition (iii) is equivalent to having $\Delta_e(x) \neq 0$. □

A. The particular case of x^2

If we consider the particular case of x^2, we will obtain the function

$$F(x) = L_1(x)x + L_2(x)x = xL(x),$$

where $L(x) = L_1(x) + L_2(x)$.

Some existence results on PN functions of type $xL(x)$ are discussed in [19], [20]. In particular, we have that

Proposition III.4 ([19]). *Let $L_1, L_2 : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be $\mathbb{F}_q$-linear mappings. If the mapping $L_1(x) \cdot L_2(x)$ is PN, then the maps L_1 and L_2 are bijective.*

This proposition implies that it is sufficient to study PN function of type $xL(x)$ where L is a bijection.

Remark III.5. *The fact that L is bijective can be obtained also from the previous section. Indeed, we can consider the isotopic shift of x^2 with a linear function L, obtaining the function $F(x) = 2xL(x)$. If F is PN then the function L needs to be a permutation.*

The PN property of functions of type $x(x^q+ux)$ over $\mathbb{F}_{q^2}$ and $x(tr_n(x)+ax)$ over $\mathbb{F}_{q^n}$ is studied in [19], [20] (where tr_n denotes the trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$).
We can restate Theorem III.3 for the case of x^2 as follows.

Theorem III.6. *Let k and m be positive integers. Consider a p^m-linear polynomial L over $\mathbb{F}_{p^{km}}$. Then the function $F(x) = xL(x)$ is PN if and only if the following conditions are satisfied:*

- *for any $t \in W$ $F(t) \neq 0$;*
- *for any $t, v \in W$, $\frac{L(v)}{v} \neq -\frac{L(t)}{t}$.*

For the case $k = 3$ it is possible to obtain the following results on polynomials of the type $xL(x)$ with L a p^m-linear polynomial.

Proposition III.7. *Over $\mathbb{F}_{p^{3m}}$, consider the isotopic shift of x^2 by the linear permutation $L(x) = ax^{p^{2m}}+bx^{p^m}+x$, $F_L(x) = 2(ax^{p^{2m}+1}+bx^{p^m+1}+x)$. Denoting by N the norm function from $\mathbb{F}_{p^{3m}}$ to $\mathbb{F}_{p^m}$, assume that $a = \frac{2e^{p^{2m}+1}}{N(e)+1}$ and $b = \frac{2e^{p^{2m}}}{N(e)+1}$, where e is such that $N(e) \neq \pm 1$ and $ex^{p^{2m}}+x^{p^m}+e^{p^m+1}x$ is a permutation. Then $F_L(x)$ is PN and affine equivalent to x^2.*

Proof. Let $A_1(x) = \frac{e^{2p^{2m}}}{1-N(e)^2}(x^{p^{2m}} - e^2x)$ and $A_2(x) = \frac{1}{e}(ex^{p^2m}+x^{p^m}+e^{p^m+1}x)$. The map A_1 is a permutation since $x^{p^{2m}-1} = e^2$ would imply $1 = N(x)^{(p^m+1)(p^m-1)} = N(e)^2$, and $A_2(x)$ is a permutation by hypothesis. Now, it is easy to verify that $A_1 \circ x^2 \circ A_2 = F_L(x)/2$. □

Proposition III.8. *Over $\mathbb{F}_{p^{3m}}$ consider the isotopic shift of x^2 by the linear permutation $L(x) = ax^{p^{2m}} + bx^{p^m} + x$, $F_L(x) = 2(ax^{p^{2m}+1} + bx^{p^m+1} + x^2)$. Denoting by N the norm function from $\mathbb{F}_{p^{3m}}$ to $\mathbb{F}_{p^m}$, assume that $a = 1/b^{p^{2m}}$, $N(b) \neq 1$, and $x^{p^{2m}} + b^{p^{2m}+1}x^{p^m} + b^{p^{2m}}x$ is a permutation. Then $F_L(x)$ is PN and affine equivalent to x^{p^m+1}.*

Proof. Let $A_1(x) = \frac{b^{p^m+1}}{N(b)-1}(x^{p^{2m}} - \frac{1}{b^{p^m}}x)$ and $A_2(x) = \frac{1}{b^{p^{2m}}}(x^{p^{2m}} + b^{p^{2m}+1}x^{p^m} + b^{p^{2m}}x)$. $A_1(x)$ is a permutation since $x^{p^{2m}-1} = \frac{1}{b^{p^m}}$ would imply $1 = N(x)^{(p^m+1)(p^m-1)} = 1/N(b)^{p^m} = 1/N(b)$ and $A_2(x)$ is a permutation by hypothesis. Then, $A_1 \circ x^{p^m+1} \circ A_2 = F_L(x)/2$. □

IV. Computational results over $\mathbb{F}_{p^n}$

In this section we report some computational results obtained on the linear shift for odd characteristics in small dimensions.

As seen before, from the linear shift of x^2 by a linear monomial we can obtain the Albert functions x^{p^t+1} [2] (for any $t \geq 1$). For any p odd, over $\mathbb{F}_{p^n}$ with $n \leq 3$, these are the only PN functions possible.

A. The case $p = 3$

We consider the isotopic shift of x^2 by a linear function L, that is the function $2xL(x)$ with L a linear permutation.

Over $\mathbb{F}_{3^4}$ from the shift of x^2 we can obtain with $L(x) = ax^{27} + bx^9 + cx^3 + dx$ (for some a, b, c, d) PN maps CCZ-equivalent to $x^{28} + x^{10} + \zeta^{20}x^4 + \zeta^5x^2$, which is equivalent to the Dickson function [14] $L(t^2(x)) + \frac{1}{2}x^2$ with $L(x) = \frac{1}{8}(x^p - x)$ and $t(x) = x^{p^2} - x$.
Over $\mathbb{F}_{3^5}$, from the shift of x^2 we can obtain the PN functions x^4, and x^{10} (Albert case).
From the shift of $F(x) = x^{90} + x^2$ (PN function [3]), for $L(x) = x^{81} + x^9 + 2x^3 + x$ we obtain that F_L is equivalent to $x^{10} - x^6 - x^2$ [16].
Over $\mathbb{F}_{3^6}$ from the shift of x^2 we can obtain the PN function x^{10} (Albert case). Due to the number of linear permutations over $\mathbb{F}_{3^6}$, our program was still running at the time of writing.

B. The case $p = 5$

Over $\mathbb{F}_{5^4}$, from the shift of x^2 with $L = ax^{125} + bx^5 + cx$ and $L = ax^{125} + bx^{25} + cx^5 + dx$ (for some a, b, c, d) we can obtain PN maps equivalent to $x^{126} + \zeta^{12}x^6 + \zeta^2x^2$, which is CCZ-equivalent to the Dickson function $L(t^2(x)) + \frac{1}{2}x^2$ with $L(x) = \frac{1}{8}(x^p - x)$ and $t(x) = x^{p^2} - x$. As for the case $\mathbb{F}_{3^6}$, our program was still running at the time of writing.

C. Isotopic shifts by a linear monomial

Starting from an Albert like function x^{p^t+1} over $\mathbb{F}_{p^n}$ by a linear monomial $L(x) = ax^{p^i}$ we obtain the map

$$F_L(x) = a^{p^t}x^{p^{t+i}+1} + ax^{p^t+p^i}.$$

When $t = 0$ we get that $F_L(x) = 2ax^{p^i+1}$ is PN if and only if $n/\gcd(n, i)$ is odd. For $t \neq 0$ we performed some computations over small dimension.

- For $p = 3$ and $3 \leq n \leq 9$ no PN maps were constructed.
- Over $\mathbb{F}_{3^6}$ the only maps constructed were for $t = 1$ and $i = 3$ (the maps found are affine equivalent to x^{p^2+1}).
- Over $\mathbb{F}_{5^3}$, $\mathbb{F}_{5^5}$, $\mathbb{F}_{5^7}$ no PN maps were constructed.
- Over $\mathbb{F}_{5^4}$ the only maps constructed were for $t = 1$, $i = 1$ and $i = 3$ (the maps found for $L(x) = \zeta x^5$ and $L = \zeta x^{5^3}$ are affine equivalent to Dickson's map).
- Over $\mathbb{F}_{5^6}$ the only maps constructed were for $t = 1$ and $i = 3$ (the found PN maps are affine equivalent to x^{p^2+1}).
- Over $\mathbb{F}_{7^3}$ with $t = 1$, $i = 1$ and $i = 2$ the map is affine equivalent to x^{p^2+1} ($L = \zeta^j x^7$ for $(j-1)$ not multiple of 3 and $L = \zeta^j x^{7^2}$ for $(j-2)$ not multiple of 3).
- Over $\mathbb{F}_{7^4}$, $\mathbb{F}_{7^5}$ no PN maps were constructed.

D. Isotopic shift with q-polynomials

We report some computational results, done in characteristic 3, for the (generalized) isotopic shift constructed in Section III.

Consider the field $\mathbb{F}_{3^6}$, in Table I we list all known isotopic inequivalent planar functions,

Considering $k = 2$ and $m = 3$, a p^m-polynomial is of the form $L(x) = ax^{3^3} + bx$. With $F(x) = x^{p+1}$ (it is not PN over $\mathbb{F}_{3^6}$) the isotopic shift with $L(x) = \zeta^2x^{3^3} + x$ (i.e. the case $L_1(x) = L_2(x)$),

$$F_L(x) = \zeta^6x^{82} + \zeta^2x^{30} + 2x^4$$

is PN and affine equivalent to the ZP function.

Table I

All known isotopic inequivalent planar functions over $\mathbb{F}_{3^6}$

x^2	Finite Field
x^{p^2+1}	Albert
$\frac{1}{8}(x^{2p^4}+x^{2p}-2x^{p^4+p}-x^{2p^3}-x^2+2x^{p^3+1})+\frac{1}{2}x^2$	Dickson [14]
$\zeta^{27}x^{270}+\zeta x^{28}+\zeta x^{10}$	BH [9]
$2x^{270}+x^{246}+2x^{90}+x^{82}+x^{54}+2x^{30}+x^{10}+x^2$	LMPTB [18]
$\zeta^{336}x^{270}+\zeta^{700}x^{244}+\zeta^{350}x^{162}+\zeta^{350}x^{84}+$ $+x^{54}+\zeta^{700}x^{36}+x^{28}+\zeta^{336}x^{10}+\zeta^{350}x^6$	Ganley [17]
$2x^{486}+2x^{252}+\zeta^{294}x^{162}+\zeta^{294}x^{84}+$ $+\zeta^{28}x^{54}+\zeta^{28}x^{28}+2x^{18}+\zeta^{294}x^6+\zeta^{84}x^2$	Cohen-Ganley [11]
$\zeta^{140}x^{324}+\zeta^{504}x^{246}+\zeta^{284}x^{108}+\zeta^{504}x^{90}+\zeta^{674}x^{82}+$ $+\zeta^{506}x^{54}+\zeta^{726}x^{30}+\zeta^{225}x^{28}+\zeta^{140}x^{12}+\zeta^{388}x^4+\zeta^{532}x^2$	ZP [22]
x^{122}	CM [12]

We searched for similar structures in other even dimensions. Over $\mathbb{F}_{3^{2m}}$ with $L(x) = ax^{p^m} + x$ and $F(x) = x^{p^i+1}$ we obtained the following results:

- with $m = 3$ over $\mathbb{F}_{3^6}$ the following PN maps are constructed
  - $F(x) = x^{3+1}$ and $L(x) = ax^{3^3} + x$ ($a = \zeta^2, \zeta^6, \zeta^{18}, \zeta^{28}, \zeta^{32}, \ldots$), the functions obtained are all affine equivalent to the ZP function.
- with $m = 4, 5$ no PN maps are constructed;
- with $m = 6$, over $\mathbb{F}_{3^{12}}$ the following PN maps are constructed
  - $F(x) = x^{3^2+1}$ and $L(x) = ax^{3^6} + x$ ($a = \zeta^{22}, \zeta^{56}, \zeta^{66}, \zeta^{168}, \zeta^{198}, \ldots$),
  - $F(x) = x^{3^4+1}$ and $L(x) = ax^{3^6} + x$ ($a = \zeta^{22}, \zeta^{56}, \zeta^{66}, \zeta^{168}, \zeta^{198}, \ldots$).

For these last functions it is not currently possible to check with MAGMA CCZ-equivalence to the known families.

Over $\mathbb{F}_{3^6}$ we consider also the generalized isotopic shift with $L_2(x) = -L_1(x)$. For the PN function $F(x) = x^{p^2+1}$, putting $k = 2$ and $m = 3$, and thus $L_1(x) = ax^{3^3} + bx$, we have

$$F'(x) = a^{p^2}x^{p^5+1} - ax^{p^3+p^2} + (b^{p^2} - b)x^{p^2+1}.$$

With coefficients restricted to the subfield $\mathbb{F}_{3^3}$ the following results are obtained:

- when $L_1(x) = ax$, ($a \notin \mathbb{F}_{p^2}$) F' is affine equivalent to F,
- when $L_1(x) = ax^{3^3} + bx$, F' is affine equivalent to the ZP function.

Putting $k = 3$ and $m = 2$, then L_1 is a p^2-polynomial, $L_1(x) = ax^{p^4} + bx^{p^2} + cx$, and

$$F'(x) = ax^{p^2(p^2+1)}+bx^{2p^2}-a^{p^2}x^2-b^{p^2}x^{p^4(p^2+1)}+(c-c^{p^2})x^{p^2+1}.$$

All PN functions constructed are affine equivalent to $x^{10} = x^{p^2+1}$.

V. Conclusions

We investigate further the isotopic shift construction introduced in [5] applying it to PN functions in odd characteristic. We show that isotopic shift of a PN function can lead to PN functions isotopic inequivalent to the original function. Moreover, we extend the construction through q-polynomials also at the PN case. In the last years, known classes of APN functions over fields of even characteristic were used for constructing new classes of PN mappings over fields of odd characteristics (see for instance [9], [21]). It would be interesting to investigate more whether the isotopic shift construction can determine new classes of PN mappings and, in particular, whenever the functions given in Theorem III.3 can be CCZ-inequivalent to the known ones.

References

[1] A.A. Albert, *Finite division algebras and finite planes*, Combinatorial Analysis: Proceedings of the 10th Symposium in Applied Mathematics (Providence), Symposia in Applied Mathematics, vol. 10, American Mathematical Society, 1960, pp. 53-70.

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

[3] N. At, S.D. Cohen, :*A new tool for assurance of perfect nonlinearity*. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 415–419. Springer, Heidelberg (2008)

[4] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol., vol. 4, no. 1, pp. 3-72, 1991.

[5] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, *Constructing APN functions through isotopic shifts*. submitted

[6] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, I.: *Generalized Isotopic Shift of Gold Functions*. In proceedings of WCC 2019

[7] L. Budaghyan, C. Carlet, and G. Leander, *Constructing New APN Functions from Known Ones*, Finite Fields and Their Applications, **15** (2009), pp. 150–159

[8] L. Budaghyan, C. Carlet, and G. Leander, *On a Construction of Quadratic APN Functions.*, Proceedings of IEEE Information Theory workshop ITW'09, Oct. 2009, pp. 374–378 .

[9] L. Budaghyan, T. Helleseth: *New perfect nonlinear multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p*. In: Sequences and Their Applications - SETA 2008. Lecture Notes in Computer Science, vol. 5203, pp. 403–414. Springer, Berlin (2008).

[10] C. Carlet, C. Ding, H. Niederreiter, *Authentication schemes from highly nonlinear functions*. In: 2006 IEEE International Symposium on Information Theory. IEEE, 2006. p. 739-743.

[11] S. Cohen, M. Ganley, *Commutative semifields, two-dimensional over their middle nuclei*. Journal of Algebra 75, 373–385 (1982)

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

[13] E. Edel and A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), 59–81.

[14] L. Dickson, *On commutative linear algebras in which division is always uniquely possible*. Transaction of the American Mathematical Society 7, 514–522 (1906)

[15] C. Ding, H. Niederreiter, *Systematic authentication codes from highly nonlinear functions*. IEEE Transactions on Information Theory, 50(10), 2421-2428, 2004.

[16] C. Ding, J. Yuan, J. *A family of skew Hadamard difference sets*. J. Comb. Theory Ser. A 113(7), 1526–1535 (2006)

[17] M. Ganley, *Central weak nucleus semifields*. European Journal of Combinatorics 2, 339–347 (1981)

[18] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, R.: *Symplectic spreads and quadric veroneseans*. Manuscript, also presented at Finite Fields 2009, Dublin, Ireland (2009)

[19] G. Kyureghyan, F. Özbudak. *Planarity of products of two linearized polynomials*. Finite Fields and Their Applications 18 1076–1088 (2012).

[20] M. Yang, S. Zhu, K. Feng. *Planarity of mappings $x(Tr(x) - \alpha/2x)$ on finite fields*. Finite Fields and Their Applications 23 1–7 (2013).

[21] Z. Zha, G. Kyureghyan, X. Wang. *Perfect nonlinear binomials and their semifields*. Finite Fields and Their Applications 15(2), pp. 125–133, 2009.

[22] Y. Zhou, A. Pott, *A new family of semifields with 2 parameters* Advances in Mathematics, Vol. 234, pp. 43–60, 2013.