Generalized Isotopic Shift of Gold Functions

Lilya Budaghyan[1], Marco Calderini[1], Claude Carlet[1,2], Robert Coulter[3], and Irene Villa[1]

[1] University of Bergen, Bergen, Norway
[2] LAGA, University of Paris 8, Paris, France
[3] The University of Delaware, Newark, Delaware USA

Abstract. In the present paper we present several generalizations of the isotopic shift construction when the starting function is a Gold function. In particular we derive a general family of APN functions which produces 15 new APN functions for $n = 9$.

Keywords: APN functions · Isotopic shift · Boolean functions.

1 Introduction

For a prime p and a positive integer n let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. We will denote by $\mathbb{F}_{p^n}^\star$ its multiplicative group. Throughout the paper, ζ denotes a primitive element of $\mathbb{F}_{p^n}$, so that $\mathbb{F}_{p^n}^\star = \langle\zeta\rangle$. A map from the field to itself admits a unique representation as a 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 $\mathbb{F}_{p^n}$.

The function F is

- *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 $F(x) = \sum_{0\le i\le j<n} a_{ij} x^{p^i+p^j}$, with $a_{ij} \in \mathbb{F}_{p^n}$;
- *quadratic* if it is the sum of a DO polynomial and an affine function.

Let δ be a positive integer, the function F is called *differentially δ-uniform* if for any pairs $a, b \in \mathbb{F}_{p^n}$, with $a \neq 0$, the equation $F(x + a) - F(x) = b$ admits at most δ solutions. When F is used as an S-box inside a cryptosystem, the differential uniformity measures its contribution to the resistance to the differential attack [2]. The smaller δ is the better is the resistence of F to this attack. So, 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*, for a PN function for any non-zero a the function $D_aF(x)$ is a permutation. 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.

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

$$F_L(x) = F(x + L(x)) - F(x) - F(L(x)).$$

This notion was introduced in [3] (see also [4]) and is inspired by the notion of isotopic equivalence of pre-semifields [1]. As we have shown in [3], for the case $p = 2$, an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original function. Moreover, all quadratic APN functions with $n = 6$ (which are all known) can be obtained from x^3 by isotopic shift, and a new infinite family of quadratic APN functions is constructed for n divisible by 3 by isotopic shift of Gold functions [3].

In the present paper we consider different generalizations of isotopic shift construction when the starting function is a monomial with a Gold exponent. In particular, instead of the expression

$$xL(x)^{2^i} + x^{2^i} L(x) \tag{1}$$

provided by the isotopic shift of x^{2^i+1} by a linear function L we consider $xL_1(x)^{2^i} + x^{2^i} L_2(x)$ where both L_1 and L_2 are linear. This leads us to a general family of APN functions which, for $n = 9$, provides 15 new APN functions and covers the only known unclassified example of APN functions, that is, function 8.1 in [5, Table 11], which is given by the polynomial $x^3 + x^{10} + \zeta^{438} x^{136}$. Further we discuss the case when in (1) the function x^{2^i+1} is not necessarily APN. And finally, we consider the case when in (1) the function L is not necessarily linear.

2 On the generalized linear shift over $\mathbb{F}_{2^n}$

Let $n = km$ for any positive integers m and k. An $\mathbb{F}_{2^m}$-polynomial is linear map given by $L(x) = \sum_{j=0}^{k-1} A_j x^{2^{jm}}$, for some $A_j \in \mathbb{F}_{2^n}$. We studied in [3, Theorem 6.3] the linear shift of the Gold function $\mathcal{G}_i = x^{2^i+1}$, defined over a finite field $\mathbb{F}_{2^n}$, by a $\mathbb{F}_{2^m}$-polynomial, that is,

$$\mathcal{G}_{i,L}(x) = xL(x)^{2^i} + x^{2^i} L(x).$$

For the case $n = 3m$ this construction leads to an infinite family of APN functions, providing, in particular, a new APN function for $n = 9$.

In the following we will generalize the isotopic shift construction. This generalization produces further new APN functions, as will be shown below.

Denote $d = \gcd(2^m - 1, \frac{2^{km}-1}{2^m-1})$ and let d' be the positive integer with the same prime factors as in d and satisfying $\gcd(2^m - 1, \frac{2^{km}-1}{(2^m-1)d'}) = 1$. Now denote

$U = \langle \zeta^{d'(2^m-1)} \rangle$ the multiplicative subgroup of $\mathbb{F}_{2^n}^\star$ of order $\left(\frac{2^{km}-1}{2^m-1}\right)/d'$. Note that it is possible to write every element $x \in \mathbb{F}_{2^n}^\star$ as $x = ut$ with $u \in W$ and $t \in \mathbb{F}_{2^m}^\star$, where $W = \{\zeta^s y : y \in U,\ 0 \le s \le d'-1\}$.
Then it is possible to obtain the following generalization of [3, Theorem 6.3]. The proof use similar ideas as the proof of the theorem mentioned above, and so we omit it.

Theorem 1. *Let $n = km$ for $m > 1$ and set $q = 2^n$. Let $L_1(x) = \sum_{j=0}^{k-1} A_j x^{2^{jm}}$ and $L_2(x) = \sum_{j=0}^{k-1} B_j x^{2^{jm}}$ be two $\mathbb{F}_{2^m}$-polynomials. Then, let i be such that $\gcd(i,m) = 1$ and $F \in \mathbb{F}_q[x]$ given by*

$$F(x) = xL_1(x)^{2^i} + x^{2^i} L_2(x) \tag{2}$$

is APN over $\mathbb{F}_q$ if and only if the following statements hold for any $v \in W$:

- $(\frac{L_1(v)}{v})^{2^i} \neq \frac{L_2(v)}{v}$.
- *If $u \in W \setminus \{1\}$ and $(\frac{L_1(uv)}{uv})^{2^i} = \frac{L_2(v)}{v}$, then $(\frac{L_1(v)}{v})^{2^i} \neq \frac{L_2(uv)}{uv}$.*
- *If $u \in W \setminus \{1\}$ and $(\frac{L_1(uv)}{uv})^{2^i} \neq \frac{L_2(v)}{v}$, then $\frac{L_1(v)^{2^i}(uv) + L_2(uv)v^{2^i}}{L_1(uv)^{2^i} v + L_2(v)(uv)^{2^i}} \notin \mathbb{F}_{2^m}^\star$.*

The obtained APN function (2) is of the form

$$F(x) = (A_0^{2^i} + B_0)x^{2^i+1} + \sum_{j=1}^{k-1} [A_j^{2^i} x^{2^{i+jm}+1} + B_j x^{2^{jm}+2^i}]$$

For the linear functions L_1 and L_2 we obtain also the following properties.

Proposition 1. *Let n, q, L_1, L_2 and F be as in Theorem 1. If F is APN over $\mathbb{F}_q$, then the following statements hold:*

(i) $\ker(L_1(x) + rx) \cap \ker(L_2(x) + r^{2^i} x) = \{0\}$ *for any* $r \in \mathbb{F}_{2^n}$.
(ii) $|\ker(L_1(x)^{2^i} + rx) \cap \ker(L_2(x) + w^{2^i} x^{2^i})| \le 2$ *for any* $r, w \in \mathbb{F}_{2^n}$.
(iii) If $\ker(L_1) \cap \ker(L_2(x) + x) \neq \{0\}$, *then* $\ker(L_1(x) + x) \cap \ker(L_2) = \{0\}$.
(iv) $\ker(L_1(x) + rx^{2^j}) \cap \ker(L_2(x) + r^{2^i} x^{(2^j-1)2^i+1}) = \{0\}$ *for any* $r \in \mathbb{F}_{2^n}$ *and* $j \ge 0$.

Proof. For any nonzero a we define the function $\Delta_a(x) = F(x+a) + F(x) + F(a)$. Suppose there exists a non-zero $a \in \ker(L_1(x) + rx) \cap \ker(L_2(x) + r^{2^i} x)$. As

$$\Delta_a(x) = aL_1(x)^{2^i} + xL_1(a)^{2^i} + x^{2^i} L_2(a) + a^{2^i} L_2(x),$$

we clearly have $a\mathbb{F}_{2^m} \subseteq \ker(\Delta_a)$, but since $m > 1$, this contradicts $|\ker(\Delta_a)| = 2$. This establishes (i).

For (ii), suppose $\{0, a, b\} \subset \ker(L_1(x)^{2^i} + rx) \cap \ker(L_2(x) + w^{2^i} x^{2^i})$. Then

$$\Delta_a(b) = a(rb) + b(ra) + a^{2^i}(w^{2^i} b^{2^i}) + b^{2^i}(w^{2^i} a^{2^i}) = 0.$$

Next suppose $a \in \ker(L_1) \cap \ker(L_2(x)+x)$. Then we have $\Delta_a(x) = a(L_1(x)+x)^{2^i} + a^{2^i} L_2(x)$. Clearly any $b \in \ker(L_1(x)+x) \cap \ker(L_2)$ satisfies $\Delta_a(b) = 0$. Since f is APN, $\ker(\Delta_a) = \{0, a\}$, so that $\ker(L_1(x)+x) \cap \ker(L_2) \subset \{0, a\}$. However, $\ker(L_1) \cap \ker(L_1(x)+x) = \{0\}$, so that no non-zero element of $\mathbb{F}_q$ can lie in both $\ker(L_1) \cap \ker(L_2(x)+x)$ and $\ker(L_1(x)+x) \cap \ker(L_2)$. This establishes (iii).

For (iv), suppose $a \in \ker(L_1(x) + rx^{2^j}) \cap \ker(L_2(x) + r^{2^i} x^{(2^j-1)2^i+1})$ is non-zero. Then for any $t \in \mathbb{F}_{2^m}$ we have

$$\begin{aligned} \Delta_a(ta) &= ar^{2^i} t^{2^i} a^{2^{j+i}} + tar^{2^i} a^{2^{j+i}} + (ta)^{2^i} r^{2^i} a^{(2^j-1)2^i+1} + a^{2^i} r^{2^i} ta^{(2^j-1)2^i+1} \\ &= r^{2^i} a^{2^{j+i}+1} \left(t^{2^i} + t + t^{2^i} + t \right) = 0, \end{aligned}$$

so that $a\mathbb{F}_{2^m} \subseteq \ker(\Delta_a)$, a contradiction. □

For the case $k = m = 3$ we consider generalized linear shift as (2) with L_1 and L_2 having coefficients in the subfield $\mathbb{F}_{2^3}$. In Table 1 we list all the known APN functions for $n = 9$, as reported in [3, Table I]. In Table 2, we list all new APN functions obtained from Theorem 1. We see that the family of Theorem 1 covers the only known example of APN functions for $n = 9$, function 8.1 of Table 11 in [5], which has not previously been identified as a part of an APN family. Hence, currently we do not have any known example of APN functions for $n = 9$ which would not be covered by an APN family. Finally, Table 2 indicates 15 new APN functions all obtained from Theorem 1.

Table 1. Known CCZ-inequivalent APN polynomials over $\mathbb{F}_{2^9}$

Functions	Families	no. Table 11 in [5]
x^3	Gold	1.1
x^5	Gold	2.1
x^{17}	Gold	3.1
x^{13}	Kasami	4.1
x^{241}	Kasami	6.1
x^{19}	Welch	5.1
x^{255}	Inverse	7.1
$Tr_1^9(x^9) + x^3$	[6]	1.2
$Tr_3^9(x^{18} + x^9) + x^3$	[7]	1.3
$Tr_3^9(x^{36} + x^{18}) + x^3$	[7]	1.4
$x^3 + x^{10} + \zeta^{438} x^{136}$	–	8.1
$\zeta^{337} x^{129} + \zeta^{424} x^{66} + \zeta^2 x^{17} + \zeta x^{10} + \zeta^{34} x^3$	[3]	–

We conclude this section with the observation that the isotopic shift can lead to an APN function also starting from a non-APN function.

Table 2. APN polynomials over $\mathbb{F}_{2^9}$ derived from Theorem 1. All are either new or correspond to the one known but unclassified case.

i, L_1, L_2	Function	Eq. to known ones
$i=1$, $L_1=\zeta^{365}x^{64}+\zeta^{146}x^8+x$ $L_2=\zeta^{292}x^{64}+\zeta^{219}x^8$	$\zeta^{219}x^{129}+\zeta^{292}x^{66}+\zeta^{292}x^{17}+\zeta^{219}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{438}x^{64}+\zeta^{438}x^8+x$ $L_2=\zeta^{292}x^{64}+\zeta^{73}x^8$	$\zeta^{365}x^{129}+\zeta^{292}x^{66}+\zeta^{365}x^{17}+\zeta^{73}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{438}x^{64}+\zeta^{73}x^8+x$ $L_2=\zeta^{365}x^{64}+\zeta^{365}x^8$	$\zeta^{365}x^{129}+\zeta^{365}x^{66}+\zeta^{146}x^{17}+\zeta^{365}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{438}x^{64}+\zeta^{146}x^8$ $L_2=\zeta^{219}x^{64}+\zeta^{73}x^8+x$	$\zeta^{365}x^{129}+\zeta^{219}x^{66}+\zeta^{292}x^{17}+\zeta^{73}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{292}x^{64}+\zeta^{292}x^8$ $L_2=\zeta^{365}x^{64}+\zeta^{73}x^8+x$	$\zeta^{73}x^{129}+\zeta^{365}x^{66}+\zeta^{73}x^{17}+\zeta^{73}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{438}x^{64}+x$ $L_2=\zeta^{438}x^{64}+\zeta^{292}x^8$	$\zeta^{365}x^{129}+\zeta^{438}x^{66}+\zeta^{292}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{438}x^{64}+x$ $L_2=x^64+\zeta^{438}x^8$	$\zeta^{365}x^{129}+x^{66}+\zeta^{438}x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{292}x^{64}+x$ $L_2=\zeta^{292}x^{64}+x^8$	$\zeta^{73}x^{129}+\zeta^{292}x^{66}+x^{10}+x^3$	new
$i=1$, $L_1=\zeta^{292}x^{64}+\zeta^{365}x^8$ $L_2=x^{64}+x$	$\zeta^{73}x^{129}+x^{66}+\zeta^{219}x^{17}+x^3$	new
$i=2$, $L_1=\zeta^{292}x^{64}+x$ $L_2=\zeta^{438}x^{64}+\zeta^{438}x^8$	$\zeta^{146}x^{257}+\zeta^{438}x^{68}+\zeta^{438}x^{12}+x^5$	new
$i=2$, $L_1=\zeta^{292}x^{64}+\zeta^{219}x^8$ $L_2=\zeta^{365}x^8+x$	$\zeta^{146}x^{257}+\zeta^{365}x^{33}+\zeta^{365}x^{12}+x^5$	eq. to 8.1 in [5, Table 11]
$i=2$, $L_1=\zeta^{146}x^{64}+x^8$ $L_2=\zeta^{146}x^{64}+x$	$\zeta^{73}x^{257}+\zeta^{146}x^{68}+x^{33}+x^5$	new
$i=2$, $L_1=\zeta^{219}x^{64}+\zeta^{219}x^8+x$ $L_2=\zeta^{438}x^{64}+\zeta^{438}x^8$	$\zeta^{365}x^{257}+\zeta^{438}x^{68}+\zeta^{365}x^{33}+\zeta^{438}x^{12}+x^5$	new
$i=2$, $L_1=\zeta^{292}x^{64}+\zeta^{146}x^8+x$ $L_2=\zeta^{219}x^{64}+x^8$	$\zeta^{146}x^{257}+\zeta^{219}x^{68}+\zeta^{73}x^{33}+x^{12}+x^5$	new
$i=2$, $L_1=\zeta^{146}x^{64}+\zeta^{219}x^8$ $L_2=\zeta^{219}x^{64}+x$	$\zeta^{73}x^{257}+\zeta^{219}x^{68}+\zeta^{365}x^{33}+x^5$	new
$i=4$, $L_1=\zeta^{146}x^{64}+x$ $L_2=\zeta^{146}x^{64}+\zeta^{73}x^8$	$\zeta^{292}x^3+\zeta^{146}x^{80}+\zeta^{73}x^{24}+x^{17}$	new

Remark 1. It is possible to generate an APN map with a linear shift starting from a function that it is not APN. For example, consider $\mathbb{F}_{2^6}$, where the function $F(x) = x^5$ is not APN. With $L(x) = \zeta x^8$ we construct the APN map

$$F_L(x) = x^4 L(x) + xL(x)^4 = \zeta x^{12} + \zeta^4 x^{33},$$

where $F_L(x) = M(x^3)$ for the linear permutation $M(x) = \zeta x^4 + \zeta^4 x^{32}$.

3 Isotopic shifts with nonlinear functions

In this section we consider the case when the function used in the shift is not necessarily linear.

In [3], it has been proved that in even dimension an isotopic shift of the Gold function, with a linear function defined over $\mathbb{F}_2[x]$, cannot be APN. In the following, we show that for any quadratic function in even dimension we cannot obtain APN functions shifting by any polynomial with all coefficients in $\mathbb{F}_2$.

Proposition 2. *Let n be an even integer and consider a quadratic function F. An isotopic shift F_L for any $L \in \mathbb{F}_2[x]$ cannot be APN.*

Proof. Given $F(x) = \sum_{i<j} b_{ij} x^{2^i+2^j} + \sum_i b_i x^{2^i} + c$ we have

$$F_L(x) = \sum_{i<j} b_{ij}[x^{2^i} L(x)^{2^j} + x^{2^j} L(x)^{2^i}] + c$$

and $L(x^2) = L(x)^2$. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$. Defining $\Delta_\alpha(x) = F_L(x + \alpha) + F_L(x) + F_L(\alpha)$, we have

$$\begin{aligned}\Delta_\alpha(\alpha+1) = &\sum_{i<j} b_{ij}[L(\alpha+1)^{2^{j-i}}(\alpha+1) + (\alpha+1)^{2^{j-i}} L(\alpha+1) \\ &+ L(\alpha)\alpha^{2^{j-i}} + \alpha L(\alpha)^{2^{j-i}}]^{2^i} + c\end{aligned}$$

When $j - i$ odd, the term of the sum is zero since $\alpha^{2^{j-i}} = \alpha + 1$, $L(\alpha)^{2^{j-i}} = L(\alpha+1)$ and $L(\alpha+1)^{2^{j-i}} = L(\alpha)$. In the case $j - i$ even, the term of the sum is also zero due to the fact that $\alpha^{2^{j-i}} = \alpha$ and $L(\alpha)^{2^{j-i}} = L(\alpha)$. So the function cannot be APN. □

3.1 Nonlinear shift for the Gold functions

If we consider an isotopic shift of a Gold function without the restriction $L(x)$ linear function, then $L(x) = \sum c_j x^j$ and the isotopic shift will be of the form

$$\mathcal{G}_{i,L}(x) = x^{2^i} L(x) + xL(x)^{2^i}. \tag{3}$$

We have $\mathcal{G}_{i,L}(x^2)^{2^{-1}} = x^{2^i} M(x) + xM(x)^{2^i}$, where $M = \sum c_j^{2^{-1}} x^j$, and $\zeta^{-2^i-1}\mathcal{G}_{i,L}(\zeta x) = x^{2^i} N(x) + xN(x)^{2^i}$, where $N(x) = \sum c_j \zeta^{j-1} x^j$. Hence we obtain the following.

Proposition 3. *Let $q = 2^n$, $\mathbb{F}_q = \langle \zeta \rangle$ and $\mathcal{G}_i = x^{2^i+1}$ be APN over $\mathbb{F}_q$. Suppose $\mathcal{G}_{i,L}$ is constructed with $L(x) = \sum_{j=0}^{2^n-2} b_j x^j$. Then $\mathcal{G}_{i,L}$ is linear equivalent to $\mathcal{G}_{i,M}$, where $M(x) = \sum_{j=0}^{2^n-2} (b_j \zeta^{k(j-1)})^{2^t} x^j$ for any k, t integers.*

Hence it is possible to restrict the search of one possible non-zero coefficient of the function.

Theorem 2. *Over $\mathbb{F}_{2^n}$ with n an odd integer, consider $F(x)$ a known APN power function (excluding the Dobbertin function). Then there exists a monomial $L(x)$ and a Gold function $\mathcal{G}_i = x^{2^i+1}$ such that the shift $\mathcal{G}_{i,L}$ is equivalent to F.*

Proof.

1. Consider the Kasami function $x^{2^{2t}-2^t+1}$. If t is odd, then let i be an integer such that $n = 2i+t$. Then, considering $L = ax^{2^{n-i}+2^{n-i+1}\dots+2^{n-i+t-1}}$ we have
$$\begin{aligned}\mathcal{G}_{i,L} &= a^{2^i} x^{2^t} + ax^{2^{n-i}+2^{n-i+1}\dots+2^{n-i+t-1}+2^i} \\ &= a^{2^i} x^{2^t} + ax^{2^i(2^t+2^{t+1}\dots+2^{2t-1}+1)} \\ &= a^{2^i} x^{2^t} + ax^{2^i(2^{2t}-2^t+1)}.\end{aligned}$$
If t is even, let i be an integer such that $t = 2i$. Then, with $L = ax^{2^i+2^{i+1}+\dots+2^{3i-1}}$ we have $\mathcal{G}_{i,L} = a^{2^i} x^{2^{2t}-2^t+1} + ax^{2^{3i}}$.
2. For the inverse function, x^{2^n-2}, considering $L(x) = ax^{2^{2t}-2}$, where t is such that $n = 2t+1$, we have $\mathcal{G}_{1,L} = a^2 x^{2(2^n-2)} + ax^{2^{2t}}$.
3. Let $n = 2t+1$ and consider the Welch function x^{2^t+3}. If t is odd, then consider i such that $t = 2i-1$. With $L(x) = ax^{2^i+2^{i+1}}$ we obtain $\mathcal{G}_{i,L} = a^{2^i} x^{2^{2i}(2^{2i-1}+3)} + ax^{2^{i+2}}$. If t is even, then consider i such that $t = 2i$. Using $L(x) = ax^{2^{3i+1}+2^{3i+2}}$ we obtain $\mathcal{G}_{i,L} = a^{2^i} x^4 + ax^{2^{3i+1}(2^{2i}+3)}$.
4. For $n = 2t+1$, with t odd, let $t = 2i-1$. Then, with $L = ax^{2^n-2^i}$ we obtain
$$\begin{aligned}\mathcal{G}_{i,L} &= a^{2^i} x^{2^i-2^{2i}+1} + ax = a^{2^i} x^{2^{2i}(2^{-i}+2^{-2i}-1)} + ax \\ &= a^{2^i} x^{2^{2i}(2^{3i-1}+2^{2i-1}-1)} + ax = a^{2^i} x^{2^{2i}(2^{(3t+1)/2}+2^t-1)} + ax\end{aligned}$$
is equivalent to the Niho function (indeed $(3t+1)/2 = (6i-3+1)/2 = 3i-1$). If t is even, let $t = 2i$. Then with $L = ax^{2^{n-i}+2^{n-i+1}\dots+2^{n-1}}$
$$\begin{aligned}\mathcal{G}_{i,L} = &\quad a^{2^i} x^{2^i} + ax^{2^{n-i}+2^{n-i+1}\dots+2^{n-1}+2^i} \\ = &\quad a^{2^i} x^{2^i} + ax^{2^{n-i}(1+2\dots+2^{i-1}+2^{2i})} \\ = &\quad a^{2^i} x^{2^i} + ax^{2^{n-i}(2^i-1+2^{2i})}\end{aligned}$$
is equivalent to Niho function.
5. Let $n = 2i+1$ and j be an integer such that $\gcd(n,j) = 1$. Then with $L = ax^{2^{i+j}-2^i}$
$$\begin{aligned}\mathcal{G}_{i,L} = &\quad a^{2^i} x^{2^{2i+j}-2^{2i}+1} + ax^{2^{i+j}} \\ = &\quad a^{2^i} x^{2^{2i}(2^j+2^{-2i}-1)} + ax^{2^{i+j}} \\ = &\quad a^{2^i} x^{2^{2i}(2^j+1)} + ax^{2^{i+j}}\end{aligned}$$

is equivalent to Gold with parameter j.

$\square$

4 Conclusions

We presented some generalizations of the isotopic shift construction introduced in [3] for the case when the starting function is a Gold power function. In particular, using a generalized form of the isotopic shift with $\mathbb{F}_q$-polynomials, we were able to construct a general family of quadratic APN functions. This allows us to classify into an infinite family the only previously known unclassified example of APN functions for $n = 9$, and to provide 15 new APN functions on $\mathbb{F}_{2^9}$. We also investigated the case of constructing an isotopic shift with a nonlinear function. In this case, for any odd n we can obtain all known power APN functions (except the Dobbertin case) using a nonlinear monomial function.

Clearly, the introduced ideas of generalized isotopic constructions are applicable also in case when the starting function is not necessarily a Gold function, but this is currently a matter for further investigations.

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. E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptol., vol. 4, no. 1, pp. 3-72, 1991.
3. Budaghyan, L, Calderini, M., Carlet, C., Coulter, R., Villa, I.: *Constructing APN functions through isotopic shifts*, ePrint Archive: Report 2018/769, submitted.
4. Budaghyan, L, Calderini, M., Carlet, C., Coulter, R., Villa, I.: *On isotopic construction of APN functions*, Sequences and Their Applications (SETA) 2018, Oct 2018, Hong-Kong, China.
5. E. Edel and A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), 59–81.
6. L. Budaghyan, C. Carlet, and G. Leander, *Constructing New APN Functions from Known Ones*, Finite Fields and Their Applications, **15** (2009), pp. 150–159
7. 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 .