CONSTRUCTING APN FUNCTIONS THROUGH ISOTOPIC SHIFTS

LILYA BUDAGHYAN, MARCO CALDERINI, CLAUDE CARLET, ROBERT S. COULTER, AND IRENE VILLA

Abstract. Almost perfect nonlinear (APN) functions over fields of characteristic 2 play an important role in cryptography, coding theory and, more generally, information theory as well as mathematics. Building new APN families is a challenge which has not been successfully addressed for more than seven years now.
The most general known equivalence relation preserving APN property in characteristic 2 is CCZ-equivalence. Extended to general characteristic, it also preserves planarity. In the case of quadratic planar functions, it is a particular case of isotopic equivalence. We apply the idea of isotopic equivalence to transform APN functions in characteristic 2 into other functions, some of which can be APN. We deduce new quadratic APN functions and a new quadratic APN family.

1. Introduction

This paper is concerned with functions, and hence polynomials, over finite fields. Let p be a prime, $n \in \mathbb{N}$, and $q = p^n$. We use $\mathbb{F}_q$ to denote the finite field of order q, and follow the well-established convention of using $\mathbb{F}_q^\star$ to denote its multiplicative group. Throughout, ζ denotes a primitive element of $\mathbb{F}_q$, so that $\mathbb{F}_q^\star = \langle \zeta \rangle$. It is an important fact that any function defined on $\mathbb{F}_q$ can be represented uniquely by an element of the polynomial ring $\mathbb{F}_q[x]$ of degree less than q. One can easily prove this via Lagrange interpolation, for example. Generally, we shall use function and polynomial interchangeably, unless we wish to rely specifically on the form of the polynomial, in which case we will be precise.

Let $F \in \mathbb{F}_q[x]$. The value set of F over $\mathbb{F}_q$ is denoted by $\mathcal{V}(F)$, i.e.

$$\mathcal{V}(F) = \{F(c) \,:\, c \in \mathbb{F}_q\}.$$

We also denote the set of roots of $F(x)$ over $\mathbb{F}_q$ by $\ker(F)$. The polynomial F is a *permutation polynomial (PP)* over $\mathbb{F}_q$ if $\mathcal{V}(F) = \mathbb{F}_q$, and is a *complete mapping* over $\mathbb{F}_q$ if both F and $F(x) + x$ are PPs.

We define the *difference operator of* F, denoted $\Delta_F \in \mathbb{F}_q[x, y]$, by

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

When there is no ambiguity about which F we are referring to, we simply use Δ. Note that Δ_F is symmetric in x and y. We refer to $D_a F(x) = \Delta(x, a) + F(a)$ as the *derivative of F in the direction of a*.

Fix $\delta \in \mathbb{N}$. A function F is called *differentially δ-uniform* if for $a, b \in \mathbb{F}_q$, $a \neq 0$, the equation $\Delta(x, a) = b$ admits at most δ solutions $x \in \mathbb{F}_q$. Differential uniformity measures the contribution of a function, used as a substitution box (S-box)

inside a block cipher, to the resistance of the cryptosystem to differential cryptanalysis, with small values of δ corresponding to better resistance. Consequently, 1-uniform functions are optimal; for such a function, all of its non-zero derivatives are permutations. In cryptographic applications these functions were coined *perfect nonlinear (PN)* by Nyberg [20], while they were earlier introduced as *planar functions* by Dembowski and Ostrom [15] in their seminal work on projective planes allowing a collineation group acting transitively on the affine points. The existence of an involution in the additive group means such functions cannot exist in even characteristic; here, the best resistance belongs to functions that are differentially 2-uniform. Such "(n,n)-functions" having optimal differential uniformity are called *almost perfect nonlinear (APN)*, see Nyberg [21]. They play a prominent role in the design of block ciphers and their study by Nyberg has allowed the Advanced Encryption Standard (AES) to have good S-boxes. Their study is also closely related to important questions on error correcting codes, since it is shown in [10] that any (n,n)-function F such that $F(0)=0$ is APN if and only if the linear code admitting for parity check matrix $H = \begin{bmatrix} 1 & \zeta & \zeta^2 & \dots & \zeta^{2^n-2} \\ F(1) & F(\zeta) & F(\zeta^2) & \dots & F(\zeta^{2^n-2}) \end{bmatrix}$ has minimum distance 5, where ζ is a primitive element of the field $\mathbb{F}_{2^n}$, and where each symbol stands for the column of its coordinates with respect to a basis of the $\mathbb{F}_2$-vector space $\mathbb{F}_{2^n}$. And the construction in the late 50's of the 2-error correcting BCH codes by Bose, Ray-Chaudhuri and Hocquenghem relies on the APNness of the power function x^3 (even if, at that time, the notion had not been yet introduced). Moreover, the code of generator matrix H above has Hamming weights $0, 2^{n-1}-2^{\frac{n-1}{2}}, 2^{n-1}$ and $2^{n-1}+2^{\frac{n-1}{2}}$ if and only if F is almost bent (a stronger notion than APNness, see [11]).
APN functions also play a role in algebraic manipulation detection (AMD), in applied cryptography and coding, see [14].

Further special classes of polynomials that play a central role in our work are defined as follows. For $F \in \mathbb{F}_q[x]$:

- F is *linear* if $F(x) = \sum_i a_i x^{p^i}$. Also known as linearised polynomials. The set of all linear polynomials of degree less than q is in 1-to-1 correspondence with the set $\mathrm{End}(n,p)$ of all linear transformations of $\mathbb{F}_q$, when viewed as a vector space over $\mathbb{F}_p$. Consequently, when F is linear, both $\mathcal{V}(F)$ and $\ker(F)$ are subspaces of $\mathbb{F}_q$.The set of all reduced degree linear PPs under composition modulo $x^q - x$ corresponds to the general linear group $\mathrm{GL}(n,p)$, the group of all non-singular linear transformations. One can (and we do) talk of linear functions over $\mathbb{F}_q \times \mathbb{F}_q$ also.
- F is *affine* if it differs from a linear polynomial by a constant.
- F is a *Dembowski-Ostrom (DO)* polynomial if $F(x) = \sum_{i,j} a_{ij} x^{p^i+p^j}$.
- F is *quadratic* if it differs from a DO polynomial by an affine polynomial. Quadratic polynomials can be categorised as those polynomials whose derivatives are all affine, see Coulter and Matthews [13], Theorem 3.1.

Note that a quadratic function F is APN over $\mathbb{F}_q$ if and only if for all $a \in \mathbb{F}_q^\star$, $\ker(\Delta_F(x,a)) = \{0,a\}$.

There are several equivalence relations that preserve differential uniformity; we list them below. Let $F, F' \in \mathbb{F}_q[x]$. Then F and F' are:

- *affine equivalent* if there exist affine permutations $A_1, A_2 \in \mathbb{F}_q[x]$ for which $F' \equiv A_1 \circ F \circ A_2 \bmod (x^q - x)$.
- *extended affine equivalent (EA-equivalent)* if there exist affine permutations $A_1, A_2 \in \mathbb{F}_q[x]$ and an affine map $A \in \mathbb{F}_q[x]$ for which $F' \equiv (A_1 \circ F \circ A_2) + A \bmod (x^q - x)$.
- *Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent)* [10] if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_q \times \mathbb{F}_q$ that maps the graph of F onto the graph of F', $\mathcal{L}(G_F) = G_{F'}$, where the graph of F is the set $G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$.

These relations are related to each other. Indeed, affine equivalence is obviously a particular case of EA-equivalence, which is itself a particular case of CCZ-equivalence [10]. As the addition of a constant term does not alter the APN or PN property, for ease of discourse, we assume throughout the paper that any APN or PN function F has zero constant term, i.e $F(0) = 0$.

The concept of *isotopic equivalence* was originally defined by Albert [1] in the study of presemifields and semifields. A *presemifield* is a ring with no zero divisor, and whose operations satisfy left and right distributivity. A *semifield* is a presemifield containing a multiplicative identity. Presemifields need not be commutative nor associative, though in the finite case associativity implies commutativity by Wedderburn's Theorem [22]. In [18], Section 2.4, Knuth gives a simple proof that the additive group of a finite presemifield is necessarily elementary Abelian. Consequently, any finite presemifield must have order a prime power q, and can be represented by $\mathbb{S} = (\mathbb{F}_q, +, \star)$ with field addition and the multiplication $\star$ given by $x \star y = \phi(x, y)$, where $\phi \in \mathbb{F}_q[x, y]$ is linear in each variable.

Given two presemifields $\mathbb{S}_1 = (\mathbb{F}_q, +, \star)$ and $\mathbb{S}_2 = (\mathbb{F}_q, +, *)$, they are called *isotopic* if there exist three linear permutations $T, M, N \in \mathbb{F}_q[x]$ such that

$$T(x * y) = M(x) \star N(y),$$

for any $x, y \in \mathbb{F}_q$. If $M = N$, then $\mathbb{S}_1$ and $\mathbb{S}_2$ are called *strongly isotopic*. It was shown by Coulter and Henderson [12] that there is a 1-to-1 correspondence between commutative presemifields of odd order and planar DO polynomials. Indeed, given a quadratic planar function $F \in \mathbb{F}_q[x]$, a commutative presemifield $\mathbb{S}_F = (\mathbb{F}_q, +, \star)$ is defined by the multiplication $x \star y = \Delta_F(x, y)$. Conversely, given a commutative presemifield $\mathbb{S}_F = (\mathbb{F}_q, +, \star)$ of odd order, the function $F(x) = \frac{1}{2}(x \star x)$ necessarily defines a planar DO polynomial. It is natural, then, to extend the notion (at least in odd characteristic) of isotopic equivalence to quadratic PN functions, where two quadratic PN functions are isotopic if and only if their corresponding presemifields are isotopic. Furthermore, it is known that CCZ-equivalence is a particular case of isotopic equivalence. Indeed, Budaghyan and Helleseth [8] showed that two planar DO polynomials F and F' are CCZ-equivalent if and only if the corresponding commutative semifields $\mathbb{S}_F$ and $\mathbb{S}_{F'}$ are strongly isotopic.

In this paper we move to study isotopic equivalence with respect to APN functions in characteristic 2. In particular, we shall introduce a new construction method for APN functions based on isotopic equivalence. We make the following formal definition, which is the central concept considered in this article (and which will appear natural after we state Theorem 2.1).

Definition 1.1. Let $F, L \in \mathbb{F}_q[x]$. The *isotopic shift of F by L*, denoted by F_L, is the polynomial given by

$$F_L(x) = \Delta_F(x, L(x)) = F(x + L(x)) - F(x) - F(L(x)). \tag{1}$$

The paper is organized as follows. In Section 2 we show how isotopic shifts arise naturally in the study of planar functions. This result acts as motivation for studying isotopic shifts in the parallel area of APN functions. Before narrowing our scope to APN functions, we make some general observations in Section 3 concerning isotopic shifts. We then restrict ourselves to considering isotopic shifts of APN functions. Firstly, in Section 4, we consider how we may obtain the same function by isotopically shifting a given APN function F in characteristic 2 by different L. Then, in Section 5, we begin our main study, that of isotopic shifts of quadratic APN functions by linear maps (in particular in characteristic 2). We show that only bijective or 2-to-1 linear maps can possibly produce an APN function from the isotopic shift of a quadratic APN. As an aside, we show how to construct all q-to-1 maps on $\mathbb{F}_{q^n}$. We then proceed in Section 6 to concentrate specifically on isotopic shifts of Gold functions in characteristic 2. Highlights of our results are as follows:

- A new family of APN functions defined over $\mathbb{F}_{2^{km}}$ is determined, see Theorem 6.3, and for $k = m = 3$, this family produces an APN function that is not equivalent to any APN function belonging to an already known class, see Section 7.2. This is the first time since seven years that such family is found (since [24]).
- We show that an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original function, even if we shift only Gold functions by linear monomials, see Lemma 6.5.
- We show that every quadratic APN function over $\mathbb{F}_{2^6}$ is EA-equivalent to an isotopic shift of x^3, see Table 2; and also EA-equivalent to an isotopic shift of $x^3 + \zeta^{-1}\operatorname{Tr}(\zeta^3 x^9)$, see Table 3.

We also provide much computational data in the last section of the paper.

2. Isotopic equivalence for planar quadratic functions revisited

Our first result shows that the concept of isotopic shifts is, in fact, a very natural concept. Recall that istopic shifts F_L are defined in (1).

Theorem 2.1. *Let $F, F' \in \mathbb{F}_q[x]$ be quadratic planar functions (null at 0). Then F and F' are isotopic equivalent if and only if F' is EA equivalent to some isotopic shift F_L of F by a linear permutation polynomial $L \in \mathbb{F}_q[x]$.*

Proof. By definition, quadratic planar functions are isotopic equivalent if the presemifields defined by them are isotopic. That is, the presemifields defined by multiplications $\star$ and $*$, with

$$x \star y = \Delta_{F'}(x, y) \text{ and } x * y = \Delta_F(x, y),$$

respectively, are isotopic. Note that the linear parts of F and F' do not play a role in these operations. In the calculations below, we replace then the quadratic functions by their DO parts (that is, we erase their linear parts, without loss of generality up to EA equivalence).

According to Fermat's little theorem, we have $2^p \equiv 2 \pmod p$ and therefore $2^{p^j+p^k} \equiv$

4 [mod p] for every non-negative integers j, k, and thanks to the fact that we erased the linear parts of F and F', we have $x \star x = 2F'(x)$ and $x * x = 2F(x)$. For some linear permutations $T, M, N \in \mathbb{F}_q[x]$, we have

$$T(x \star y) = M(x) * N(y), \tag{2}$$

for all $x, y \in \mathbb{F}_q$. Hence,

$$T(x \star x) = T(2F'(x)) = 2T(F'(x))$$

and

$$T(x \star x) = M(x) * N(x) = \Delta_F(M(x), N(x)),$$

which leads to

$$2T(F'(M^{-1}(x))) = \Delta_F(x, N(M^{-1}(x))).$$

As this holds for all $x \in \mathbb{F}_q$, we see that this is, in fact, a polynomial identity, and F' is EA equivalent to F_L with $L = N \circ M^{-1}$, a linear permutation. □

Theorem 2.1 shows that, for isotopic equivalent quadratic planar functions, what takes us beyond CCZ-equivalence is the isotopic shift by a linear permutation L. For linear shifts of APN functions, we do not restrict L to be a permutation. As with planar quadratic functions, we will see that an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original function.

3. Generic results on isotopic shifts

With regards to isotopic shifts, an easy first observation is that for any $F \in \mathbb{F}_q[x]$ and any permutation $L \in \mathbb{F}_q[x]$, we have

$$F_L(L^{[-1]}(x)) \equiv F_{L^{[-1]}}(x) \bmod (x^q - x), \tag{3}$$

where $L^{[-1]}$ is the compositional inverse of L. In particular, thanks to EA-equivalence, if L is a linear permutation polynomial, then F_L and $F_{L^{[-1]}}$ have the same differential uniformity. Along similar lines, we have the following theorem.

Theorem 3.1. *Let $F, F' \in \mathbb{F}_q[x]$ be arbitrary polynomials. If F and F' are affine equivalent, say $F(x) \equiv A_1(F'(A_2(x))) \bmod (x^q - x)$, where $A_1, A_2 \in \mathbb{F}_q[x]$ are linear permutations, then for $L \in \mathbb{F}_q[x]$, F_L is affine equivalent to F'_M where $M = A_2 \circ L \circ A_2^{[-1]}$.*

Proof. Since $F = A_1 \circ F' \circ A_2$ with A_1, A_2 linear permutation polynomials, we have

$$\begin{aligned}
F_L(x) &= \Delta_F(x, L(x)) \\
&= F(x + L(x)) - F(x) - F(L(x)) \\
&= A_1\left(F'(A_2(x) + A_2(L(x))) - F'(A_2(x)) - F'(A_2(L(x)))\right) \\
&= A_1\left(F'(A_2(x) + M(A_2(x))) - F'(A_2(x)) - F'(M(A_2(x)))\right) \\
&= A_1(\Delta_{F'}(A_2(x), M(A_2(x)))) \\
&= A_1(F'_M(A_2(x))),
\end{aligned}$$

and this completes the proof. □

Let $\mathrm{GL} = \mathrm{GL}(n, p)$ and $\mathcal{S}$ be the set of all polynomials in $\mathbb{F}_q[x]$ of degree less than q. Then GL has a natural conjugation action on $\mathcal{S}$ given by $F \cdot L = L(F(L^{[-1]}(x))) \bmod (x^q - x)$ for $F \in \mathcal{S}$ and $L \in \mathrm{GL}$ (here $F \cdot L$ means F is being

acted on by L by the conjugation action). In the most general sense, we are interested in isotopic shifts of arbitrary polynomial $F \in \mathcal{S}$ by arbitrary polynomial $L \in \mathcal{S}$. Set $\mathrm{N_{GL}}(L)$ to be the stabiliser of L under the action. Then Theorem 3.1 shows that isotopic shifts of F by elements of $\mathcal{S}$ splits naturally into affine equivalent "conjugacy classes" of the action of GL as F_L and F'_L will be affine equivalent whenever $F' = M \circ F \circ M^{[-1]}$ and $M \in \mathrm{N_{GL}}(L)$. More generally, we will be interested in isotopic shifts of elements of $\mathcal{S}$ by elements of $\mathrm{End} = \mathrm{End}(\mathbb{F}_p^n)$ (the larger set of endomorphisms, *i.e.* linear transformations). Note that the action of GL on $\mathcal{S}$ may be restricted to an action on End.

We will be mainly concerned with the case where F is a quadratic APN function and L is linear. We note that, for F a quadratic,

$$F_L + F_M = F_{L+M} \tag{4}$$

for arbitrary choices of polynomials L, M.

4. Isotopic shifts of APN functions

Throughout this section, $q = 2^n$ for some $n \in \mathbb{N}$. We first consider how an isotopic shift of an APN function may generate the zero polynomial. (We remind the reader that throughout the paper, we assume any APN function has zero constant term.)

Theorem 4.1. *Let $F \in \mathbb{F}_q[x]$ be an APN function and $L \in \mathbb{F}_q[x]$. Then F_L is the zero function if and only if $L(a) \in \{0, a\}$ for all $a \in \mathbb{F}_q^\star$. Furthermore, if L is linear, then F_L is the zero function if and only if L is either the zero polynomial or the polynomial x.*

Proof. Suppose $F_L(x) = 0$. As F is APN, we know that for all $a \in \mathbb{F}_q^\star$, $\Delta_F(x, a) = 0$ if and only if $x \in \{0, a\}$. Now $F_L(x) = \Delta_F(x, L(x))$, so that for all $a \in \mathbb{F}_q^\star$, $L(a) \in \{0, a\}$ is forced.
Conversely, if $L(a) \in \{0, a\}$ for all $a \in \mathbb{F}_q^\star$, then clearly $F_L(a) = \Delta_F(a, L(a)) = 0$, while $F_L(0) = \Delta_F(0, L(0)) = 0$. Hence $F_L(x) = 0$.
Now suppose L is linear. Since $L(a) \in \{0, a\}$ for all $a \in \mathbb{F}_q$, we have $\mathbb{F}_q = \mathcal{V}(L) \oplus \ker(L)$. Suppose $0 < \dim(\ker(L)) < n$. Then there exist $v \in \mathcal{V}(L)$ (which implies $v = L(v)$) and $z \in \ker(L)$ with $vz \neq 0$ and $v + z \neq 0$. Thus

$$v = v + 0 = L(v) + L(z) = L(v + z) \in \{0, v + z\},$$

a contradiction. Hence $\ker(L) = \mathbb{F}_q$ or $\ker(L) = \{0\}$. In the former case, $L(x) = 0$, while in the latter case $L(x) = x$. □

Our motivation for establishing this result is not directly related to being concerned with generating the zero polynomial, but with the more practical problem of understanding how distinct L can yield the same isotopic shift of a given DO APN function.

Corollary 4.2. *Let $F \in \mathbb{F}_q[x]$ be a DO APN function and $L, M \in \mathbb{F}_q[x]$. The following statements hold.*

(i) *$F_L = F_M$ if and only if $L(a) + M(a) \in \{0, a\}$ for all $a \in \mathbb{F}_q^\star$.*
(ii) *Suppose L, M are linear. Then $F_L = F_M$ if and only if $L = M$ or $L(x) = M(x) + x$ as polynomials.*

Proof. We have from (4) that $F_L = F_M$ if and only if $F_N(x) = 0$, where $N = L+M$. Both results now follow from Theorem 4.1. □

A consequence of Corollary 4.2 is that there is a sort of duality that occurs among isotopic shifts, between $L(x)$ and $L(x) + x$. That is, any conditions derived on L for the isotopic shift F_L to be APN apply equally to both $L(x)$ and $L(x) + x$.

5. Isotopic shifts of quadratic APN functions

In this section, we restrict ourselves to isotopic shifts of quadratic APN functions by linear polynomials. In the planar case, for the isotopic shift to be planar we require the linear polynomial involved to be a permutation polynomial. The corresponding result for the APN case is as follows. Here we assume $q = 2^n$ for some $n \in \mathbb{N}$.

Theorem 5.1. *Let $F \in \mathbb{F}_q[x]$ be a quadratic APN function and $L \in \mathbb{F}_q[x]$ be linear. Set $M(x) = L(x) + x$. If F_L is APN, then the following statements hold.*

(i) *L is either a permutation or 2-to-1, and L is injective on $\mathcal{V}(L)$.*
(ii) *M is either a permutation or 2-to-1, and M is injective on $\mathcal{V}(M)$.*

Proof. We need only establish (i), as the duality spelled out in Corollary 4.2(ii) will then imply (ii). As F is a quadratic polynomial, $\Delta_F(x, a)$ is a linear operator for all $a \in \mathbb{F}_q^\star$. Consequently, $\Delta_{F_L}(x, a)$ is also linear, and F_L being APN is equivalent to $\ker(\Delta_{F_L}(x, a)) = \{0, a\}$ for all $a \in \mathbb{F}_q^\star$. Applying the linear operator identity to the difference operators involved one can show that, for any $a \in \mathbb{F}_q^\star$,

$$\Delta_{F_L}(x, a) = \Delta_F(x, L(a)) + \Delta_F(a, L(x)). \tag{5}$$

Suppose L is not a permutation polynomial, so that there exists some $z \in \ker(L)$ with $z \neq 0$. Then $\Delta_{F_L}(x, z) = \Delta_F(z, L(x))$. Clearly, any $x \in \ker(L)$ satisfies $\Delta_{F_L}(x, z) = 0$, so that

$$\{0, z\} \subseteq \ker(L) \subseteq \ker(\Delta_{F_L}(x, z)) = \{0, z\}.$$

Thus $\ker(L) = \{0, z\}$ is forced and L is 2-to-1. Furthermore, since $\Delta_{F_L}(x, z) = \Delta_F(z, L(x))$ and $\Delta_F(z, z) = 0$, we must have $z \notin \mathcal{V}(L)$. Thus, viewed as a vector space over $\mathbb{F}_2$, we have $\mathbb{F}_q = \mathcal{V}(L) \oplus \langle z \rangle$. Since $L(x + z) = L(x)$ for all $x \in \mathbb{F}_q$, we must have $L(\mathcal{V}(L)) = \mathcal{V}(L)$. □

We have the following corollary, which eliminates some possibilities for L when the field has square order.

Corollary 5.2. *Set q to be an even power of 2. Let $F \in \mathbb{F}_q[x]$ be a quadratic APN function and $L \in \mathbb{F}_2[x]$ be linear. If F_L is APN over $\mathbb{F}_q$, then L is 2-to-1.*

Proof. Set $M(x) = L(x) + x$. Suppose, by way of contradiction, that F_L is APN over $\mathbb{F}_q$ and L is a permutation polynomial. Then $L(1) = 1$ is forced. Thus $M(1) = M(0) = 0$. Now $\mathbb{F}_4 = \{0, 1, \gamma, \gamma+1\}$ is a subfield of $\mathbb{F}_q$, and since $L \in \mathbb{F}_2[x]$ is a permutation polynomial, we must have either $L(\gamma) = \gamma$ or $L(\gamma) = \gamma + 1$.

If $L(\gamma) = \gamma$, then $M(\gamma) = 0$, so that M has more than two roots, and this contradicts Theorem 5.1 (ii). If $L(\gamma) = \gamma + 1$, then $M(\gamma) = 1$, and so $1 \in \mathcal{V}(M)$. But then $0, 1 \in \mathcal{V}(M)$ and $M(0) = M(1)$, so that M is not injective on $\mathcal{V}(M)$, again contradicting Theorem 5.1 (ii). Thus, L cannot be a permutation polynomial. □

In light of Theorem 5.1, understanding how to construct 2-to-1 mappings would be of some utility. We therefore take a brief interlude from considering the role of isotopic shifts in the theory of APN functions to develop some theory on 2-to-1, or more generally q-to-1, functions.

5.1. **On q-to-1 $\mathbb{F}_q$-linear maps.** For this subsection, q is an arbitrary prime power. We begin with a proposition.

Proposition 5.3. *The number of $\mathbb{F}_q$-linear q-to-1 maps over $\mathbb{F}_{q^n}$ is given by*

$$\frac{q^n-1}{q-1}\prod_{i=0}^{n-2}(q^n-q^i).$$

Proof. Any linear map over $\mathbb{F}_{q^n}$ can be viewed as a linear transformation, and so to count the number of q-to-1 maps, it suffices to determine the number of $\mathbb{F}_q$-linear maps over $\mathbb{F}_{q^n}$ for which the image space has dimension $n-1$. We proceed in much the same way as one counts the number of non-singular linear transformations, but with a small twist.

Choose a basis $\beta_1,\ldots,\beta_n$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. To construct a q-to-1 $\mathbb{F}_q$-linear map L we proceed as follows: For β_1, there are two choices: either $L(\beta_1)\in \mathrm{span}(0)$ or $L(\beta_1)\notin \mathrm{span}(0)$. In the former case, $\mathrm{span}(L(\beta_2),\ldots,L(\beta_n))$ must then have dimension $n-1$, and we can do this in N ways where

$$N=\prod_{i=0}^{n-2}(q^n-q^i). \tag{6}$$

Otherwise, we have q^n-1 choices for β_1. Now for β_2, we have $L(\beta_2)\in\mathrm{span}(L(\beta_1))$ or $L(\beta_2)\notin\mathrm{span}(L(\beta_1))$. In the former case, there are q choices for $L(\beta_2)$ and as $\mathrm{span}(L(\beta_1),L(\beta_3),L(\beta_4),\ldots,L(\beta_n))$ must have dimension $n-1$, we have qN ways of constructing L in this case. Otherwise, there are q^n-q choices for $L(\beta_2)$, and we proceed to $L(\beta_3)$. The argument is now clear, and we find the number of q-to-1 $\mathbb{F}_q$-linear maps over $\mathbb{F}_{q^n}$ is given by $N+qN+q^2N+\ldots+q^{n-1}N$, as claimed. □

Theorem 5.4. *A $\mathbb{F}_q$-linear map $L\in\mathbb{F}_{q^n}[x]$ is q-to-1 if and only if $L(bx)\equiv M(x^q-x) \bmod (x^{q^n}-x)$ for some $\mathbb{F}_q$-linear permutation $M\in\mathbb{F}_{q^n}[x]$ and some $b\in\mathbb{F}_{q^n}^\star$.*

Proof. Firstly, suppose $L(bx)\equiv M(x^q-x) \bmod (x^{q^n}-x)$ for some linear permutation M and some b. It is clear L is a $\mathbb{F}_q$-linear map. To prove $L(bx)$ is q-to-1, it suffices to show $\ker(M(x^q-x))=\mathbb{F}_q$. The only zero in $\mathbb{F}_{q^n}$ of M is 0, as M is assumed to be a linear permutation. Thus the only elements of $\ker(M(x^q-x))$ are the roots of x^q-x, and this is precisely $\mathbb{F}_q$.
Now suppose L is a q-to-1 $\mathbb{F}_q$-linear map over $\mathbb{F}_{q^n}$. Then $\ker(L)=\langle b\rangle$ for some $b\in\mathbb{F}_{q^n}^\star$. Set $L_1(x)=L(bx)$, so that $\ker(L_1)=\mathbb{F}_q$. Then x^q-x divides $L_1(x)$, and consequently, $L_1(x)=M(x^q-x)$ for some $\mathbb{F}_q$-linear map over $\mathbb{F}_{q^n}$, see for example Lidl and Niederreiter [19], Exercise 3.68. If M is a permutation, then there is nothing further to prove. So suppose M is not a permutation. Since $\ker(x^q-x)=\mathbb{F}_q$ and x^q-x is a $\mathbb{F}_q$-linear map, the image set $\mathcal{V}(x^q-x)$ is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of dimension $n-1$. Furthermore, $\ker(M)\cap\mathcal{V}(x^q-x)=\{0\}$, as otherwise L_1 would not be q-to-1. Since $\ker(M)\oplus\mathcal{V}(x^q-x)$ is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, it follows that $\ker(M)=\langle z\rangle$ for some $z\in\mathbb{F}_{q^n}^\star$ and $\mathbb{F}_{q^n}=\mathcal{V}(x^q-x)\oplus\langle z\rangle$. Now $M(x)=M(y)$ if and only if $y-x\in\langle z\rangle$. Consequently, M is injective on $\mathcal{V}(x^q-x)$. Set $S=\mathcal{V}(M(x^q-x))=M(\mathcal{V}(x^q-x))$. Then S is a subspace of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of

dimension $n-1$. Set $\mathbb{F}_{q^n} = S \oplus \langle w \rangle$ for some $w \in \mathbb{F}_{q^n}^\star \setminus S$. We define a new $\mathbb{F}_q$-linear map M_1 over $\mathbb{F}_{q^n}$ as follows:

$$M_1(y) = \begin{cases} M(y) & \text{if } y \in \mathcal{V}(x^q - x), \\ cw & \text{if } y = cz \text{ for some } c \in \mathbb{F}_q. \end{cases}$$

It now follows that M_1 is a $\mathbb{F}_q$-linear permutation on $\mathbb{F}_{q^n}$ and $M(x^q - x) = M_1(x^q - x)$ for all $x \in \mathbb{F}_{q^n}$. Thus $L(bx) \equiv M_1(x^q - x) \bmod (x^{q^n} - x)$ for some $\mathbb{F}_q$-linear permutation M_1, as required. □

We have the following corollary, showing it is also not particularly difficult to construct 2-to-1 linear maps satisfying Theorem 5.1(i).

Corollary 5.5. *Let n be a positive integer, L be a linear permutation over $\mathbb{F}_{2^n}$ and $z \in \mathbb{F}_{2^n}^\star$. Set $M(zx) = L(x^2 + x)$. The following statements hold.*

(i) *M is 2-to-1 with $\ker(M) = \{0, z\}$.*
(ii) *For $y \in \mathbb{F}_{2^n}$ we have $L(y) \notin \mathcal{V}(M)$ if and only if $x^2 + x + y$ is irreducible over $\mathbb{F}_{2^n}$. In particular, $z \notin \mathcal{V}(M)$ if and only if $x^2 + x + y$ is irreducible over $\mathbb{F}_{2^n}$, where $y \in \mathbb{F}_{2^n}^\star$ is the unique pre-image of z under L.*

Proof. Part (i) is immediate from Theorem 5.4. For (ii), $L(y) \in \mathcal{V}(M)$ if and only if there exists $u \in \mathbb{F}_{2^n}$ satisfying $L(u^2 + u) = L(y)$, but this is equivalent to u being a root of $x^2 + x + y$. □

6. Isotopic shifts of Gold functions

For the remainder of this paper we fix $q = 2^n$. The DO monomials in characteristic 2 which are APN are, up to composition by Frobenius automorphism, the so-called Gold functions $\mathcal{G}_i(x) = x^{2^i+1}$ over $\mathbb{F}_{2^n}$ with $\gcd(i, n) = 1$. First studied by Gold [17] in context of sequence design and rediscovered in 1993 by Nyberg in [21], Gold functions have played an important role in the study of APN functions, and, in particular, in understanding CCZ-equivalence [7]. For $\mathcal{G}_i$ and any $L \in \mathbb{F}_q[x]$, we use $\mathcal{G}_{i,L}$ to denote the isotopic shift of $\mathcal{G}_i$ by L; that is

$$\mathcal{G}_{i,L}(x) = x^{2^i} L(x) + x L^{2^i}(x). \tag{7}$$

It is an easy observation that $\mathcal{G}_i$ and $\mathcal{G}_{n-i}$ are linearly equivalent. In fact, this is a necessary and sufficient condition for Gold functions to be linear equivalent, and if they are not linear equivalent, then they are not CCZ-equivalent [23]. This linear equivalence extends to isotopic shifts as

$$\mathcal{G}_{i,L}(x)^{2^{n-i}} \equiv \mathcal{G}_{n-i,L}(x) \bmod (x^q - x).$$

6.1. **General restrictions on L.** We expand on (7) further. Let the linear polynomial L be represented as $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$. Then expanding in (7) we have

$$\mathcal{G}_{i,L}(x) = \sum_{j=0}^{n-1} \left(b_j x^{2^i + 2^j} + b_j^{2^i} x^{2^{i+j}+1} \right).$$

We first note

$$\begin{aligned}\mathcal{G}_{i,L}(x^{2^{n-1}})^2 &= \sum_{j=0}^{n-1}\left(b_j^2 x^{2^i+2^j} + b_j^{2^{i+1}} x^{2^{i+j}+1}\right)\\ &= x^{2^i} M(x) + x M^{2^i}(x)\\ &= \mathcal{G}_{i,M}(x),\end{aligned}$$

where $M(x) = \sum_{j=0}^{n-1} b_j^2 x^{2^j}$. We also have, with ζ a primitive element,

$$\begin{aligned}\zeta^{-(2^i+1)}\mathcal{G}_{i,L}(\zeta x) &= \zeta^{-(2^i+1)} \sum_{j=0}^{n-1}\left(b_j \zeta^{2^i+2^j} x^{2^i+2^j} + b_j^{2^i} \zeta^{2^{i+j}+1} x^{2^{i+1}+1}\right)\\ &= \sum_{j=0}^{n-1}\left(b_j \zeta^{2^j-1} x^{2^i+2^j} + b_j^{2^i} \zeta^{2^i(2^j-1)} x^{2^{i+1}+1}\right)\\ &= \sum_{j=0}^{n-1}\left(b_j \zeta^{2^j-1} x^{2^i+2^j} + (b_j \zeta^{2^j-1})^{2^i} x^{2^{i+1}+1}\right)\\ &= x^{2^i} N(x) + x N^{2^i}(x)\\ &= \mathcal{G}_{i,N}(x),\end{aligned}$$

where $N(x) = \sum_{j=0}^{n-1} b_j \zeta^{2^j-1} x^{2^j}$.

From the above two equivalences we can perform a restriction over one non-zero coefficient of the linear function $L(x)$. Fixing an integer j such that $0 < j \leq n-1$, then we can restrict the search of all possible linear functions $L(x)$ with $b_j \neq 0$ to those with $b_j = \zeta^k$ with $0 \leq k < 2^j - 1$ and k either 0 or odd. We summarise with the following statement.

Proposition 6.1. *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 $\mathcal{G}_{i,L}$ as (7) is constructed with $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$. Then $\mathcal{G}_{i,L}$ is linear equivalent to $\mathcal{G}_{i,M}$, where $M(x) = \sum_{j=0}^{n-1} (b_j \zeta^{k(2^j-1)})^{2^t} x^{2^j}$ for any k, t integers.*

Our next result is related to Theorem 5.1 and shows that in certain situations we may obtain, for Gold functions, slightly stronger restrictions on L than those outlined in Theorem 5.1. We say L is a q-polynomial over $\mathbb{F}_{q^n}$ if $L(x) = \sum b_i x^{q^i}$. Any q-polynomial over $\mathbb{F}_{q^n}$ is a linear transformation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Theorem 6.2. *Let $q = 2^m$, with $m > 1$, and suppose $\mathcal{G}_i = x^{2^i+1}$ is APN over $\mathbb{F}_{q^n}$. If $\mathcal{G}_{i,L}$ as in (7) is APN over $\mathbb{F}_{q^n}$ with L a q-polynomial, then L is a complete mapping over $\mathbb{F}_{q^n}$.*

Proof. Set $\Delta_a(x) = \Delta_{\mathcal{G}_{i,L}}(x, a)$, with $a \in \mathbb{F}_{q^n}^\star$. Since $\mathcal{G}_{i,L}(x)$ is a quadratic APN function, we have $\ker(\Delta_a(ax)) = \{0, 1\}$. For $x \in \mathbb{F}_q^\star$, we have $L(ax) = xL(a)$. So,

if $x \in \mathbb{F}_q^\star \setminus \{0,1\}$, then we have

$$\begin{aligned}
0 &\neq \Delta_a(ax) \\
&= ax\,L(a)^{2^i} + aL(ax)^{2^i} + (ax)^{2^i}L(a) + a^{2^i}L(ax) \\
&= ax\,L(a)^{2^i} + ax^{2^i}L(a)^{2^i} + (ax)^{2^i}L(a) + a^{2^i}xL(a) \\
&= ax\,L(a)\big(L(a)^{2^i-1} + x^{2^i-1}L(a)^{2^i-1} + a^{2^i-1}x^{2^i-1} + a^{2^i-1}\big) \\
&= ax\,L(a)\big(L(a)^{2^i-1} + a^{2^i-1}\big)\,(x^{2^i-1}+1).
\end{aligned}$$

As $\mathcal{G}_i$ is APN over $\mathbb{F}_{q^n}$, we know $\gcd(2^i-1, q^n-1) = 1$, so that $z \mapsto z^{2^i-1}$ is a bijection. Consequently, $x^{2^i-1} = 1$ if and only if $x = 1$, which we have excluded. Hence, for all $a \in \mathbb{F}_{q^n}^\star$, we must have $L(a) \neq 0$ and $L(a)^{2^i-1} \neq a^{2^i-1}$. This latter condition is equivalent to $L(a) \neq a$ for all $a \in \mathbb{F}_{q^n}^\star$, again because $z \mapsto z^{2^i-1}$ is a bijection. Since L is a linear transformation, we conclude L is a complete mapping over $\mathbb{F}_{q^n}$. □

We now prove a theorem that leads to new examples of APN functions.

Theorem 6.3. *Let $n = km$ and $d = \gcd(q-1, \frac{q^k-1}{q-1})$, where $q = 2^m$. Let d' be the positive integer having the same prime factors as d, each being raised at the same power as in $\frac{q^k-1}{q-1}$, hence such that $\gcd(q-1, \frac{q^k-1}{(q-1)d'}) = 1$. Let $U = \langle \zeta^{d'(q-1)} \rangle$ be the multiplicative subgroup of $\mathbb{F}_{q^k}^\star$ of order $\left(\frac{q^k-1}{(q-1)d'}\right)$ and consider the set $W = \{y\zeta^j;\ j = 0, \ldots, d'-1,\ y \in U\}$. Let $L \in \mathbb{F}_{q^k}[x]$ be a q-polynomial and let $\mathcal{G}_i = x^{2^i+1}$ be an APN Gold function over $\mathbb{F}_{q^k}$ (i.e. such that $\gcd(i,n) = 1$). Then $\mathcal{G}_{i,L}$ as in (7) is APN over $\mathbb{F}_{q^k}$ if and only if the following conditions are satisfied:*

(i) *for any $u \in W$, $L(u) \notin \{0, u\}$;*
(ii) *if n is even then $|\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}| \leq 1$;*
(iii) *for distinct $u, v \in W$ satisfying $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$, we have*

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin \mathbb{F}_q^\star.$$

Proof. Any element $x \in \mathbb{F}_{q^k}^\star$ can be expressed in the form $x = ut$ with $u \in W$ and $t \in \mathbb{F}_q^\star$. Indeed, since $\mathbb{F}_{q^k}^\star = \langle \zeta \rangle$, we have $x = \zeta^{d'z+j}$, for some integers z and j where $0 \leq j \leq d'-1$. For ease of notation, set $l = \frac{q^k-1}{(q-1)d'}$. Since $\gcd(q-1, l) = 1$, for any such z, there exist integers r and s such that $z = r(q-1) + sl$. Hence we have

$$x = \zeta^{d'z+j} = \zeta^{d'r(q-1)}\zeta^j\zeta^{d'sl} = ut, \tag{8}$$

where, denoting $y = \zeta^{d'r(q-1)} \in U$, we have $u = y\zeta^j \in W$ and $t = \zeta^{d'sl} = \zeta^{s(\frac{q^k-1}{q-1})} \in \mathbb{F}_q^\star$. Since $|W \times \mathbb{F}_q^\star| = |W| \cdot |\mathbb{F}_q^\star| = (d'|U|) \cdot (q-1) = d' \cdot \frac{q^k-1}{d'(q-1)} \cdot (q-1) = q^k - 1 = |\mathbb{F}_{q^k}^\star|$, two distinct elements in $\mathbb{F}_{q^k}^\star$ cannot have the same representation, u and t are unique. Using the representation (8) for x, we have $L(x) = tL(u)$.

Let $a \in \mathbb{F}_{q^k}$ and $\Delta_a(x) = \Delta_{\mathcal{G}_{i,L}}(x, a)$ so that

$$\Delta_a(x) = x^{2^i}L(a) + L(x)a^{2^i} + xL(a)^{2^i} + L(x)^{2^i}a.$$

Then $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$ if and only if $\ker(\Delta_a) = \{0, a\}$ for all $a \in \mathbb{F}_{q^k}^\star$. Now apply the representation (8) for both $x = ut$ and $a = vs$ with $u, v \in W$ and $t, s \in \mathbb{F}_q$. Then

$$\begin{aligned}\Delta_a(x) &= u^{2^i} t^{2^i} sL(v) + v^{2^i} s^{2^i} tL(u) + uts^{2^i} L(v)^{2^i} + vst^{2^i} L(u)^{2^i} \\ &= ts\left(t^{2^i-1}\left(u^{2^i} L(v) + vL(u)^{2^i}\right) + s^{2^i-1}\left(v^{2^i} L(u) + uL(v)^{2^i}\right)\right).\end{aligned}$$

So in this representation, $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$ if and only if the only solutions to $\Delta_{vs}(ut) = 0$ are $t = 0$, or $u = v$ and $t = s$.

Assume $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$. Then L is a complete mapping on $\mathbb{F}_{q^k}$ by Theorem 6.2; hence Condition (i) is satisfied. For showing Condition (ii), suppose that n is even and $|\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}| > 1$. Since L is a complete linear mapping, the elements of $\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}|$ cannot be in $\mathbb{F}_2^\star$ and since $|\{\frac{L(u)}{u} : u \in W\} \cap \mathbb{F}_{2^2}| > 1$ these elements are then α and α^2, where α is a primitive element of $\mathbb{F}_{2^2}^\star$. There exist then two (distinct) elements $u, v \in W$ such that $L(u) = \alpha u$ and $L(v) = \alpha^2 v$. In this case we have $u^{2^i} L(v) + vL(u)^{2^i} = u^{2^i} \alpha^2 v + v\alpha^2 u^{2^i} = 0$, because i being odd (n being even), we have $\alpha^{2^i} = \alpha^2$, and similarly $v^{2^i} L(u) + uL(v)^{2^i} = 0$. Hence $\Delta_{vs}(ut) = 0$ for any $s, t \in \mathbb{F}_q$. Therefore Condition (ii) must hold. To establish Condition (iii), assume $u^{2^i} L(v) + vL(u)^{2^i} \neq 0$. As $\ker(\Delta_{vs}) = \{0, vs\}$, we know that for all $t \in \mathbb{F}_q^\star$, we must have

$$t^{2^i-1} + s^{2^i-1}\left(\frac{v^{2^i} L(u) + uL(v)^{2^i}}{u^{2^i} L(v) + vL(u)^{2^i}}\right) \neq 0.$$

As $\mathcal{G}_i$ is APN over $\mathbb{F}_{q^k}$ by hypothesis, we know $\gcd(2^i - 1, q - 1) = 1$, and so t^{2^i-1} ranges over all of $\mathbb{F}_q^\star$ as t does. Consequently, we must have

$$\frac{v^{2^i} L(u) + uL(v)^{2^i}}{u^{2^i} L(v) + vL(u)^{2^i}} \notin \mathbb{F}_q^\star,$$

which is Condition (iii).

Conversely, assume that Conditions (i), (ii) and (iii) hold. Since $L(ut) = tL(u)$, we have that L is a complete mapping by (i). Assume that $\Delta_{vs}(ut) = 0$. We must show $t = 0$, or $u = v$ and $t = s$. Assume that $t \neq 0$, we have:

$$t^{2^i-1}\left(u^{2^i} L(v) + vL(u)^{2^i}\right) + s^{2^i-1}\left(v^{2^i} L(u) + uL(v)^{2^i}\right) = 0. \tag{9}$$

Firstly, suppose $u = v$. Then (9) becomes

$$\left(t^{2^i-1} + s^{2^i-1}\right)\left(u^{2^i} L(u) + uL(u)^{2^i}\right) = 0.$$

Thus $t^{2^i-1} = s^{2^i-1}$ or $u^{2^i} L(u) = uL(u)^{2^i}$. By (i), $L(u) \neq 0$, so the latter reduces further to $L(u)^{2^i-1} = u^{2^i-1}$. But this is equivalent to $L(u) = u$, which cannot hold by (i). Thus $t^{2^i-1} = s^{2^i-1}$, from which we deduce $t = s$, as required.

It remains to show that $\Delta_{vs}(ut) = 0$ has no solutions when $t \neq 0$ and $u \neq v$. Suppose $x = ut$ is a solution such that $u^{2^i} L(v) + vL(u)^{2^i} = 0$. Then (9) forces $v^{2^i} L(u) + uL(v)^{2^i} = 0$ also. So we have

$$\frac{L(v)}{v} + \frac{L(u)^{2^i}}{u^{2^i}} = 0 \text{ and } \frac{L(u)}{u} + \frac{L(v)^{2^i}}{v^{2^i}} = 0.$$

Combining, we find

$$\frac{L(u)}{u} = \frac{L(u)^{2^{2i}}}{u^{2^{2i}}},$$

so $\frac{L(u)}{u} \in \mathbb{F}_{2^{2i}}$. If n is odd we have $\mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_2$, which implies that $\frac{L(u)}{u}$ is equal to 0 or 1. This is not possible due to Condition (i). On the other hand, if n is even then $\mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^n} = \mathbb{F}_{2^2}$. Hence $\frac{L(u)}{u} = \alpha$, primitive element in $\mathbb{F}_{2^2}^\star$, and $\frac{L(v)}{v} = \left(\frac{L(u)}{u}\right)^{2^i} = \alpha^{2^i} = \alpha^2$. This leads to a contradiction for Condition (ii). Hence, if $x = ut$ is a solution, then $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. Now dividing by $u^{2^i}L(v) + vL(u)^{2^i}$ in (9) yields

$$t^{2^i-1} + s^{2^i-1}\left(\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}}\right) = 0.$$

However, there are no solutions to this equation by (iii). This proves $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{q^k}$. □

The case where $n = 3m$ with $m \geq 3$ will be of particular interest. As we shall discuss later in the computational results section, applying Theorem 6.3 in this case leads to a new APN function CCZ-inequivalent to known APN families.

We conclude this section with the following result for linear function L having coefficient in $\mathbb{F}_2$.

Proposition 6.4. *Set $q = 2^n$ with n an even integer. Suppose $\mathcal{G}_i = x^{2^i+1}$ is APN over $\mathbb{F}_q$. Then for any $L \in \mathbb{F}_2[x]$ linear $\mathcal{G}_{i,L}$ defined as in (7) is not APN.*

Proof. Let $L(x) = \sum_{j\in J} x^{2^j}$, for some $J \subseteq \{0, ..., n-1\}$. Then

$$\mathcal{G}_{i,L}(x) = \sum_{j\in J}[x^{2^{j+i}+1} + x^{2^j+2^i}].$$

Let $\Delta_1(x) = \Delta_{\mathcal{G}_{i,L}}(x, 1)$ so that

$$\Delta_1(x) = \sum_{j\in J}[(x^{2^{j+i}} + x) + (x^{2^j} + x^{2^i})].$$

It is easy to check that $\mathbb{F}_4 \subset \ker(\Delta_1)$. Indeed, let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, we have that $0, 1 \in \ker(\Delta_1)$. Since $\mathcal{G}_i$ is APN then i is odd, $\alpha^{2^i} = \alpha + 1$ and

$$(\alpha^{2^{j+i}} + \alpha) + (\alpha^{2^j} + \alpha^{2^i}) = ((\alpha + 1)^{2^j} + \alpha) + (\alpha^{2^j} + \alpha + 1) = 0.$$

Thus, $\Delta_1(\alpha) = 0$, which implies $\mathbb{F}_4 \subset \ker(\Delta_1)$. □

6.2. **Restricting L to having 1 term.** First we consider the case when the linear map is just a monomial, $L(x) = ux^{2^j}$. It follows from (3) that we need only consider j where $j \leq n/2$.

Lemma 6.5. *Let $\mathcal{G}_i = x^{2^i+1}$ be APN over $\mathbb{F}_q$, $q = 2^n$, $L(x) = ux^{2^j} \in \mathbb{F}_q[x]$ and $\mathcal{G}_{i,L}$ as in (7). The following statements hold.*

(i) *If $j = 0$ and $u \in \mathbb{F}_{2^n} \setminus \mathbb{F}_2$, then $\mathcal{G}_{i,L}$ is linearly equivalent to $\mathcal{G}_i$.*
(ii) *If n is odd, $j = i$, and $u \in \mathbb{F}_{2^n}^\star$, then $\mathcal{G}_{i,L}$ is linearly equivalent to $\mathcal{G}_{2i}$ and (provided $n > 3$) CCZ-inequivalent to $\mathcal{G}_i$.*

(iii) *If $n = 2j$, then $\mathcal{G}_{i,L}$ is linearly equivalent to $\mathcal{G}_{|j-i|}$ whenever $ux^{2^i} + u^{2^i}x^{2^{j+i}}$ is a permutation. In such cases, $\mathcal{G}_{i,L}$ is CCZ-equivalent to $\mathcal{G}_i$ if and only if $j = 2i$ or $2i - j = n$.*
(iv) *If $\gcd(j, n) = 1$, then $\mathcal{G}_{i,L}$ is not APN over $\mathbb{F}_q$. Except for the case when n odd and $j = i$.*
(v) *If $\gcd(j + i, |j - i|, n) > 1$, then $\mathcal{G}_{i,L}$ is not APN over $\mathbb{F}_q$. In particular, if n is even and j is odd $\mathcal{G}_{i,L}$ is not APN.*

Proof. Firstly, set $L(x) = ux$ with $u \notin \mathbb{F}_2$. Then $\mathcal{G}_{i,L} = (u+u^{2^i})\mathcal{G}_i$, which is clearly linearly equivalent to $\mathcal{G}_i$. Now let $L(x) = ux^{2^j}$, $u \in \mathbb{F}_{2^n}^\star$. Then

$$\mathcal{G}_{i,L}(x) = ux^{2^i+2^j} + u^{2^i}x^{2^{i+j}+1}. \tag{10}$$

If $i = j$, then (10) becomes $\mathcal{G}_{i,L}(x) = ux^{2^{i+1}} + u^{2^i}\mathcal{G}_{2i}(x)$, which is APN and equivalent to $\mathcal{G}_{2i}$ provided $\gcd(2i, n) = 1$; i.e. provided n is odd. It was shown by Budaghyan, Carlet and Leander [4] that these two functions are CCZ-inequivalent provided $n > 3$. This proves (ii). For (iii), it is easily checked that

$$\mathcal{G}_{i,L}(x) \equiv (ux^{2^i} + u^{2^i}x^{2^{j+i}}) \circ \mathcal{G}_{|j-i|}(x) \bmod (x^q - x).$$

The statement in (iii) on equivalence is clear.

Now, let $\gcd(j, n) = 1$. Then $\mathcal{G}_{i,L}(x) = ux^{2^j+2^i} + u^{2^i}x^{2^{j+i}+1}$. For $a \in \mathbb{F}_q^\star$, set $\Delta_a(x) = \Delta_{\mathcal{G}_{i,L}}(x, a)$. Then

$$\Delta_a(ax) = ua^{2^j+2^i}(x^{2^{j-i}} + x)^{2^i} + u^{2^i}a^{2^{j+i}+1}(x^{2^{j+i}} + x).$$

Now, $\mathcal{G}_{i,L}$ is APN if and only if $\ker(\Delta_a(ax)) = \{0, 1\}$ for all $a \in \mathbb{F}_q^\star$. Let $L_1(x) = x^{2^{j-i}} + x$ and $L_2(x) = x^{2^{j+i}} + x$, so that

$$\Delta_a(ax) = ua^{2^j+2^i}L_1(x)^{2^i} + u^{2^i}a^{2^{j+i}+1}L_2(x).$$

If n is even, j and i are odd numbers and the obtained function cannot be APN since $\mathbb{F}_4 \subseteq \ker(L_1) \cap \ker(L_2)$, and for all $x \in \ker(L_1) \cap \ker(L_2)$ we have that x is a solution of $\Delta_a(ax) = 0$. If n is odd, from (ii) we have that for $j = i$, $\mathcal{G}_{i,L}$ is APN. Then, let us consider $j \neq i$. In this case, $\ker(L_1) \subsetneq \mathbb{F}_q$ and $\ker(L_2) \subsetneq \mathbb{F}_q$ since $0 < |j - i| < n$ and $0 < j + i < n$, so there exists some element $\bar{x} \in \mathbb{F}_q^\star \setminus \{1\}$ (note that $\mathbb{F}_2 \subseteq \ker(L_1) \cap \ker(L_2)$) such that $L_1(\bar{x})\, L_2(\bar{x}) \neq 0$. Now $\Delta_a(ax) = 0$ is equivalent to

$$L_1(x)^{2^i} + u^{2^i-1}a^{(2^j-1)(2^i-1)}L_2(x) = 0.$$

Since $a \mapsto a^{(2^j-1)(2^i-1)}$ is a permutation of $\mathbb{F}_q$ (both i and j are coprime with n), there exists a such that $a^{(2^j-1)(2^i-1)} = \frac{L_1(\bar{x})^{2^i}}{u^{2^i-1}L_2(\bar{x})}$, implying $\bar{x} \in \ker(\Delta_a(ax))$. So $\mathcal{G}_{i,L}$ is not APN. Then, statement (iv) is proved.

Let us consider statement (v). From the proof of (iv), we have that for all $x \in \ker(L_1) \cap \ker(L_2)$, x is a solution of $\Delta_a(ax) = 0$. Then, since $\gcd(j+i, |j-i|, n) = d > 1$, for some integer d, we have $\mathbb{F}_{2^d} \subseteq \ker(L_1) \cap \ker(L_2)$ and so $\mathcal{G}_{i,L}$ cannot be APN. □

6.3. **Restricting L to having 2 terms.** We now move to considering L being a linear binomial.

Lemma 6.6. *Let m be a positive integer, $q = 2^n$ with $n = 2m$, and*

$$L(x) = ux^{2^m} + vx, \tag{11}$$

with $u, v \in \mathbb{F}_q^\star$ and $v \neq 1$. Set $z = v + v^{2^i}$. If $\mathcal{G}_{i,L}$ is APN, then $\mathcal{G}_{i,M}$ is an APN function EA-equivalent to $\mathcal{G}_{i,L}$ for the following choices of linear $M \in \mathbb{F}_q[x]$:

(i) $M(x) = u\zeta^{2^m-1}x^{2^m} + vx$.
(ii) $M(x) = ux^{2^m} + wx$, *where* $w + w^{2^i} = z^{2^m}$;
(iii) $M(x) = u^2x^{2^m} + wx$ *where* $w + w^{2^i} = z^2$.

Proof. Given linear L as in (11), equation (7) is of the form

$$\mathcal{G}_{i,L}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + zx^{2^i+1}. \tag{12}$$

We want to prove that in each case the obtained function is EA-equivalent to the original map.

Case (i). If instead of u we consider $u\zeta^{2^m-1}$ in (12), then we obtain

$$\mathcal{G}_{i,M}(x) = u^{2^i}\zeta^{2^i(2^m-1)}x^{2^{m+i}+1} + u\zeta^{2^m-1}x^{2^m+2^i} + zx^{2^i+1},$$

which is linear equivalent to $\mathcal{G}_{i,L}$ as $\mathcal{G}_{i,M}(\zeta^{-1}x) = \zeta^{-2^i-1}\mathcal{G}_{i,L}(x)$.

Case (ii). For M as specified, we have

$$\mathcal{G}_{i,M}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + z^{2^m}x^{2^i+1},$$

and

$$\mathcal{G}_{i,M}(u^{-2^m}x^{2^m})^{2^m} = u^{-2^i-1}\mathcal{G}_{i,L}(x).$$

Hence $\mathcal{G}_{i,M}$ is linear equivalent to $\mathcal{G}_{i,L}$.

Case (iii). In this last case we obtain the function

$$\mathcal{G}_{i,M}(x) = u^{2^{i+1}}x^{2^{m+i}+1} + u^2x^{2^m+1} + w^2x^{2^i+1},$$

and $\mathcal{G}_{i,M}(x^2)^{2^{2m-1}} = \mathcal{G}_{i,L}(x)$.

□

Lemma 6.7. *Let m be an even positive integer and $q = 2^n$ with $n = 2m$. Suppose $\mathcal{G}_i$ is APN over $\mathbb{F}_q$. Set $L(x) = ux^{2^m} + vx$ with $v \in \mathbb{F}_q$ satisfying $v + v^{2^i} = 1$ and $u = w^{2^m-1}$ for $w \in \mathbb{F}_q^\star$. Then $\mathcal{G}_{i,L}$ is an APN function over $\mathbb{F}_q$ EA-equivalent to $\mathcal{G}_{m-i}$.*

Proof. In this case the isotopic shift of $\mathcal{G}_i$ by L is given by

$$\begin{aligned}\mathcal{G}_{i,L}(x) &= u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + x^{2^i+1}\\ &= w^{2^{m+i}-2^i}x^{2^{m+i}+1} + w^{2^m-1}x^{2^m+2^i} + x^{2^i+1}.\end{aligned}$$

Now note $w^{-2^i-1}\mathcal{G}_{i,L}(xw^{-1}) = x^{2^{m+i}+1} + x^{2^m+2^i} + x^{2^i+1}$, and this latter function was shown to be EA-equivalent to $x^{2^{m-i}+1}$ by Budaghyan, Helleseth, Li and Sun [9]. □

We end this subsection by deriving a necessary condition for $\mathcal{G}_{i,L}$ in certain restricted settings.

Lemma 6.8. *Let m be a positive integer, $n = 2m$, and $q = 2^n$. Let $u, v \in \mathbb{F}_q^\star$. If $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_q$ with $L(x) = ux^{2^m} + vx$, then*

$$u^{2^i}x^{2^i} + ux + v^{2^i} + v = 0$$

has no solution x such that $x^{2^m+1} = 1$.

Proof. From the given L we obtain in (7) that

$$\mathcal{G}_{i,L}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + (v^{2^i} + v)x^{2^i+1}.$$

If $\mathcal{G}_{i,L}$ is APN, then

$$a^{-(2^i+1)}\Delta_a(ax) = (ua^{2^m-1})^{2^i}(x^{2^{m+i}}+x)+(ua^{2^m-1})(x^{2^m}+x^{2^i})+(v^{2^i}+v)(x^{2^i}+x) \neq 0$$

for any $a \neq 0$ and $x \neq 0, 1$. Assume $x \in \mathbb{F}_{2^m}$. Then we have

$$a^{-(2^i+1)}\Delta_a(ax) = \left(u^{2^i}a^{(2^m-1)2^i} + ua^{2^m-1} + v^{2^i} + v\right)(x^{2^i} + x) \neq 0$$

Let $y = a^{2^m-1}$. Then,

$$u^{2^i}y^{2^i} + uy + v^{2^i} + v \neq 0$$

for all $y \in \mathbb{F}_q$ such that $y^{2^m+1} = 1$. □

In particular when we consider the Gold function $\mathcal{G}_1 = x^3$ we obtain the following.

Lemma 6.9. *Let m be an even positive integer, $n = 2m$, and $q = 2^n$. Set $u = \zeta^i$, with $0 \leq i < 2^m - 1$. If $v \in \mathbb{F}_q$ is such that $v(v + 1) = \zeta^{j(2^m+1)}$ for some $0 \leq j < 2^m - 1$ and $\mathcal{G}_{1,L}$ is APN over $\mathbb{F}_q$ with $L(x) = ux^{2^m} + vx$, then*

$$\zeta^{(2^m+1)(2j-i)} + \zeta^{i(2^m+1)} \neq 1.$$

Moreover, if there exists a positive integer l such that $\zeta^{i+l(2^m-1)}+\zeta^{2^m i+l(1-2^m)} = 1$, then $i \neq j$.

Proof. From the given L we obtain in (7) that

$$\mathcal{G}_{1,L}(x) = \zeta^{2i}x^{2^{m+1}+1} + \zeta^i x^{2^m+2} + \zeta^{j(2^m+1)}x^3.$$

If $\mathcal{G}_{1,L}$ is APN, then

$$a^{-3}\Delta_a(ax) = (\zeta^i a^{2^m-1})^2(x^{2^{m+1}} + x) + (\zeta^i a^{2^m-1})(x^{2^m} + x^2) + \zeta^{j(2^m+1)}(x^2 + x) \neq 0$$

for any $a \neq 0$ and $x \neq 0, 1$. Assume $x \in \mathbb{F}_{2^m}$. Then we have

$$a^{-3}\Delta_a(ax) = ((\zeta^i a^{2^m-1})^2 + \zeta^i a^{2^m-1} + \zeta^{j(2^m+1)})(x^2 + x) \neq 0.$$

Let $a = \zeta^l$ for a positive integer l. Then

$$a^{-3}\Delta_a(ax) = (\zeta^{2(i+l(2^m-1))} + \zeta^{i+l(2^m-1)} + \zeta^{j(2^m-1)})(x^2 + x) \neq 0. \tag{13}$$

Suppose that $\zeta^{(2^m+1)(2j-i)}+\zeta^{i(2^m+1)}+1 = 0$. Multiplying this equality by $\zeta^{i(2^m+1)}$ and then taking its 2^{n-1}th power we get

$$\zeta^{i(2^m+1)} + \zeta^{2^{n-1}i(2^m+1)} + \zeta^{j(2^m+1)} = 0.$$

For $l = 2^{n-1}i$, we have $i + l(2^m - 1) = i2^{n-1}(2^m + 1)$, and so we have a choice of a for which $a^{-2}\Delta_a(ax) = 0$, contradicting the hypothesis.

Assume now that there exists an integer l such that $\zeta^{i+l(2^m-1)}+\zeta^{2^m i+l(1-2^m)}=1$. Then using (13) we find

$$\begin{aligned}0 \neq &\zeta^{2(i+l(2^m-1))}+\zeta^{(i+l(2^m-1))}+\zeta^{j(2^m-1)}= \\ &\zeta^{i+l(2^m-1)}(\zeta^{i+l(2^m-1)}+1)+\zeta^{j(2^m+1)}= \\ &\zeta^{i+l(2^m-1)}\zeta^{2^m i+l(1-2^m)}+\zeta^{j(2^m+1)}= \\ &\zeta^{i(2^m+1)}+\zeta^{j(2^m+1)},\end{aligned}$$

implying $i \neq j$. □

6.4. **Restricting L to having 3 terms.** From the computational analysis performed for the Gold function $\mathcal{G}_1(x)=x^3$, see Section 7 below, we observed that, when L has 3 terms and $n=3m$, the linear polynomial

$$L(x)=ax^{2^{2m}}+bx^{2^m}+cx \tag{14}$$

is a good generator of APN functions via shifts of $\mathcal{G}_1$. In this case, we have

$$\mathcal{G}_{1,L}(x)=a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3. \tag{15}$$

As proved in Proposition 6.1, the polynomial $L(x)$ generates an isotopic shift of $\mathcal{G}_i$ equivalent to the one generated by

$$M(x)=(a\zeta^{(2^{2m}-1)j})^{2^k}x^{2^{2m}}+(b\zeta^{(2^2-1)j})^{2^k}x^{2^m}+c^{2^k}x. \tag{16}$$

Consideration of this case led to Theorem 6.3. The case with $q=2^m$, $n=3m$ with m odd, in Theorem 6.3 is exactly the situation that we observed in our computational results that led to Theorem 6.3. As we shall note in Section 7, this specific case leads to the construction of a new APN function $n=9$ which is CCZ-inequivalent to any known APN function.

7. Computational results

Using the software algebra package MAGMA [2] we studied the possible linear functions $L(x)$ for which $\mathcal{G}_{i,L}$, as in (7), is an APN function over $\mathbb{F}_{2^n}$. The obtained APN functions have been compared, using CCZ-equivalence, to those presented in tables of [16]. There, the authors listed all known APN functions for $n\in\{6,7,8,9\}$. For purposes of comparison, we will refer to the numbering given in those lists.

Due to the classification of the linear functions L based on the number of terms, we do not consider in the computational analysis linear function with x as term. Indeed, if a function $L(x)=\sum_{j=1}^{n-1}b_jx^{2^j}+x$ has d terms then it will construct the same isotopic shift constructed by the function $L(x)+x$ that has one term less.

7.1. **Data for $\mathcal{G}_{i,L}$ where L has 1 or 2 terms.** When L has just one term, all possible cases with $3\leq n\leq 12$ considering all APN Gold functions $\mathcal{G}_i=x^{2^i+1}$, with $\gcd(i,n)=1$, have been analysed and the only APN functions arising are those presented in Lemma 6.5.

When L has exactly two terms, we determined those isotopic shifts of $\mathcal{G}_i$ by L that are APN over $\mathbb{F}_{2^n}$ for $6\leq n\leq 11$. Apart from the $n=6$ case, we obtained APN functions only for $n=2m$ and $L(x)=ux^{2^m}+vx$. For $n\in\{12,14,16\}$ we only considered L of the form $ux^{2^m}+vx$. In particular, we found that if $n\in\{8,12,16\}$, then $\mathcal{G}_{i,L}$ from (7) is either equivalent to $\mathcal{G}_i$ or to $\mathcal{G}_{m-i}$. In the

other cases, $n \in \{10, 14\}$, the obtained APN maps are all equivalent to the original Gold function $\mathcal{G}_i$.

When $n = 6$, with $\mathbb{F}_{2^6}^\star = \langle\zeta\rangle$, considering isotopic shifts of the Gold function $\mathcal{G}_1 = x^3$ more cases occur:

- For $L(x) = ux^8 + vx = ux^{2^m} + vx$ it is possible to construct APN functions equivalent to $\mathcal{G}_1$ or to function number 2.1 in [16, Table 5] $(x^3 + x^{10} + \zeta x^{24})$.
- For $L(x) = ux^{16} + vx$, where u is not a cube and $v + v^2 = 1$, the constructed function is APN and equivalent to number 1.2 in [16, Table 5] $(x^3 + \zeta^{11}x^6 + \zeta x^9)$.
- For $L(x) = ux^{16} + vx^4$, where u is not a cube and $v = u^{26}$, the constructed function is APN and again equivalent to number 1.2 in [16, Table 5].

7.2. **Data for $\mathcal{G}_{i,L}$ where L has 3 terms and new APN functions.** When the function L has 3 terms, none of them equal to x, we analysed $\mathcal{G}_{i,L}$ for the cases $n \in \{6, 7, 8, 9\}$ and obtained the following results.

$n = 6$: for $\mathcal{G}_{1,L}$ the only valid trinomial is of the form $ax^{2^4} + bx^{2^2} + cx$ and can construct APN functions equivalent to $\mathcal{G}_1$ and to number 1.2 in [16, Table 5]$(x^3 + \zeta^{11}x^6 + \zeta x^9)$.

$n = 7$: no valid trinomial was found.

$n = 8$: for $\mathcal{G}_{1,L}$ the only valid trinomial is of the form $ax^{2^6} + bx^{2^4} + cx^{2^2}$ and can construct APN functions equivalent to number 1.2 in [16, Table 9]$(x^3 + \mathrm{Tr}(x^9))$;
for $\mathcal{G}_{3,L}$ the only valid trinomial is of the form $ax^{2^6} + bx^{2^4} + cx^{2^2}$ and can construct APN functions equivalent to number 1.11 in [16, Table 9]$(x^9 + \mathrm{Tr}(x^3))$.

$n = 9$: for $\mathcal{G}_{1,L}$ the only valid trinomial is of the form $ax^{2^6} + bx^{2^3} + cx$ and can construct APN functions not equivalent to any function from the known APN families; for $\mathcal{G}_{2,L}$ and $\mathcal{G}_{4,L}$ no valid trinomials were found.

The cases obtained for $n = 8$ are instances of Theorem 6.3 where k=4 and m=2. In particular with $L = \zeta^{106}x^{2^6} + \zeta^{175}x^{2^4} + \zeta x^{2^2}$, $\mathcal{G}_{1,L}$ is equivalent to $x^3 + \mathrm{Tr}(x^9)$, function discovered by Dillon et al. in 2006 [3], and with the same L $\mathcal{G}_{3,L}$ is equivalent to $x^9 + \mathrm{Tr}(x^3)$.
For $n = 9$, $\mathcal{G}_{1,L}$ leads us to an inequivalence result. For this reason we focused on functions of this particular form and noticed that, for $m = \frac{9}{3}$,

$$L(x) = ax^{2^6} + bx^{2^3} + cx = ax^{2^{2m}} + bx^{2^m} + cx.$$

Hence, for $n = 3m$, we analysed the possible APN functions $\mathcal{G}_{1,L}$ as in (7) constructed using the linear function $L(x)$ of the form $ax^{2^{2m}} + bx^{2^m} + cx$. Due to Proposition 6.1, we restricted the search to those linear polynomials for which $b = \zeta^t$ with $0 \le t < 2^m - 1$ and t either zero or odd. Setting to $d = c^2 + c$, we obtained the following results:

$n = 6$: If

$$[a, b, d] \in \left\{ \begin{matrix} [\zeta^3, 1, \zeta^{35}], [\zeta^9, 1, \zeta^9], [\zeta^{11}, 1, \zeta^{28}], [\zeta, \zeta, \zeta^{39}], \\ [\zeta^{10}, \zeta, \zeta^{56}], [\zeta^{12}, \zeta, \zeta^{18}], [\zeta^{18}, \zeta, \zeta^{30}], [\zeta^{27}, \zeta, \zeta^{28}] \end{matrix} \right\},$$

then $\mathcal{G}_{1,L}$ is equivalent to $\mathcal{G}_i$. Otherwise, if $[a, b, d] = [\zeta^5, \zeta, 1]$, then $\mathcal{G}_{1,L}$ is equivalent to $x^3 + \zeta^{-1}\,\mathrm{Tr}(\zeta^3 x^9)$.

$n = 9$: Just one function was found, with $[a, b, d] = [\zeta^{424}, \zeta, \zeta^{34}]$. As mentioned above, $\mathcal{G}_{1,L}$ is not equivalent to any APN function from the known APN families.

$n = 12$: If

$$[a, b, d] \in \left\{[\zeta^{1962}, \zeta^3, \zeta^{1365}], [\zeta^{290}, \zeta, \zeta^{2184}], [\zeta^{904}, \zeta^5, \zeta^{546}]\right\},$$

then $\mathcal{G}_{1,L}$ is equivalent to $\mathcal{G}_1$. Indeed, let us denote by F_1, F_2 and F_3 the functions relative to $[\zeta^{1962}, \zeta^3, \zeta^{1365}]$, $[\zeta^{290}, \zeta, \zeta^{2184}]$ and $[\zeta^{904}, \zeta^5, \zeta^{546}]$, respectively. We have that

$$F_1(x) = \zeta^{3924}x^{513} + \zeta^{1962}x^{258} + \zeta^6 x^{33} + \zeta^3 x^{18} + \zeta^{1365}x^3,$$

and $L_1(x)^3 = L_2(F_1(x)/\zeta^{1365})$, with

$$L_1(x) = \zeta^{1416}x^{2^{2m}} + \zeta^{1914}x^{2^m} + x, \quad L_2(x) = \zeta^{153}x^{2^{2m}} + \zeta^{1647}x^{2^m} + x.$$

$$F_2(x) = \zeta^{580}x^{513} + \zeta^{290}x^{258} + \zeta^2 x^{33} + \zeta^a x^{18} + \zeta^{2184}x^3,$$

and $L_1(x)^3 = L_2(F_2(x)/\zeta^{2184})$, with

$$L_1(x) = \zeta^{3566}x^{2^{2m}} + \zeta^{3277}x^{2^m} + x, \quad L_2(x) = \zeta^{2508}x^{2^{2m}} + \zeta^{1641}x^{2^m} + x.$$

$$F_3(x) = \zeta^{1808}x^{513} + \zeta^{904}x^{258} + \zeta^{10}x^{33} + \zeta^5 x^{18} + \zeta^{546}x^3,$$

and $L_1(x)^3 = L_2(F_3(x)/\zeta^{546})$, with

$$L_1(x) = \zeta^{1723}x^{2^{2m}} + \zeta^{824}x^{2^m} + x, \quad L_2(x) = \zeta^{1074}x^{2^{2m}} + \zeta^{2472}x^{2^m} + x.$$

Therefore, combining the computational result obtained for $n = 9$ with the $n = 3m$ instance of Theorem 6.3, we are able to present a new family of APN functions defined over $\mathbb{F}_{2^{3m}}$ for an integer m. Indeed the function

$$\mathcal{G}_{1,L}(x) = a^2x^{2^{2m+1}+1} + b^2x^{2^{m+1}+1} + ax^{2^{2m}+2} + bx^{2^m+2} + dx^3,$$

with the restrictions as set out in Theorem 6.3, is APN and when $m = 3$ this function is not equivalent to any APN function belonging to an already known family.

In Table 1 there are listed, up to CCZ-equivalence, the APN maps defined over $\mathbb{F}_{2^9}$ belonging to known families. To this list we added the new function found with Theorem 6.3.

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

Functions	Families	no. Table 11 in [16]
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
$Tr_1^9(x^9) + x^3$	[5]	1.2
$Tr_3^9(x^{18} + x^9) + x^3$	[6]	1.3
$Tr_3^9(x^{36} + x^{18}) + x^3$	[6]	1.4
$x^3 + x^{10} + \zeta^{438}x^{136}$	–	8.1
$\zeta^{337}x^{129} + \zeta^{424}x^{66} + \zeta^2 x^{17} + \zeta x^{10} + \zeta^{34}x^3$	the function from Theorem 6.3	–

Consequentially we extended the computations performed to the case of shifts of the general Gold function $\mathcal{G}_i = x^{2^i+1}$. For $6 \leq n \leq 8$ and $\mathcal{G}_i$ not equivalent to $\mathcal{G}_1$ no linear trinomials L were found that can construct APN functions.

7.3. **The cases $3 \leq n \leq 5$.** Exhaustive searching was carried out for small dimensions. Shifts of $\mathcal{G}_1$ (and $\mathcal{G}_2$ in $n = 5$) that produced APN functions in all cases produced APN functions equivalent to the Gold functions $\mathcal{G}_1$ (and $\mathcal{G}_2$ in $n = 5$). We give some additional details below for completeness.

n = 3: All obtained APN functions are equivalent to $\mathcal{G}_1$. Valid linear functions were:
- monomials as described in Lemma 6.5 (i) and (ii), and their compositional inverses. In this case, this amounts to all possible linear monomials ux^{2^j} with $j \in \{0, 1, 2\}$ and $u \in \mathbb{F}_8 \setminus \mathbb{F}_2$.
- binomials resulting from the monomial examples above via Corollary 4.2 (ii).
- trinomials, there were 126 distinct linear trinomials L for which $\mathcal{G}_{1,L}$ was APN.

There are a total of 462 linear functions that are either permutation polynomials or 2-to-1 maps over $\mathbb{F}_8$. Of these, a total of 162 yields APN functions. Of course, as n increases the ratio of successful shifts drops sharply.

n = 4: All obtained APN functions are equivalent to $\mathcal{G}_1$. Valid linear functions were:
- monomials as described in Lemma 6.5 (i) and (iii).
- binomials as described in Lemma 6.6, along with those resulting from the monomials above via Corollary 4.2 (ii).
- trinomials, there were a total of 600 distinct linear trinomials L for which $\mathcal{G}_{1,L}$ was APN.
- quadrinomials, there were 2880 distinct linear quadrinomials L for which $\mathcal{G}_{1,L}$ was APN.

n = 5: For shifts of $\mathcal{G}_1$ all obtained APN functions are equivalent to $\mathcal{G}_1$ or $\mathcal{G}_2$. Valid linear functions were:
- monomials as described in Lemma 6.5 (i) (for $\mathcal{G}_1$) and (ii) (for $\mathcal{G}_2$).
- binomials.
  For $\mathcal{G}_1$, of the form $\zeta^i x^{16} + \zeta^{17i} x^8$.
  For $\mathcal{G}_2$, of the form $ux^4 + vx^2, ux^8 + vx^2$ (31 examples in each case), along with those resulting from the monomials above via Corollary 4.2 (ii).
- trinomials.
  For $\mathcal{G}_1$, of the form $\zeta^i x^{16} + \zeta^{17i} x^8 + \zeta^{29i} x^2$, along with those resulting from the binomials above via Corollary 4.2 (ii).
  For $\mathcal{G}_2$, of the form $ux^8 + vx^4 + wx^2, ux^{16} + vx^4 + wx^2$ (31 examples in each case), along with those resulting from the binomials above via Corollary 4.2 (ii).
- quadrinomials, there were a total of 2201 distinct linear quadrinomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_1$, and 3317 distinct linear quadrinomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_2$.
- pentanomials, there were a total of 15190 distinct linear pentanomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_1$, and 11625 distinct linear pentanomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_2$.

For shifts of $\mathcal{G}_2$ all obtained APN functions are equivalent to $\mathcal{G}_1$ or $\mathcal{G}_2$. Valid linear functions were:

- monomials as described in Lemma 6.5 (ii) (for $\mathcal{G}_1$) and (i) (for $\mathcal{G}_2$).
- binomials.
  For $\mathcal{G}_1$, of the form $\zeta^i x^4 + \zeta^{21i} x^2$, $\zeta^i x^8 + \zeta^{9i} x^2$.
  For $\mathcal{G}_2$, of the form $\zeta^i x^{16} + \zeta^{17i} x^8$,
  along with those resulting from the monomials above via Corollary 4.2 (ii).
- trinomials.
  For $\mathcal{G}_1$, of the form $\zeta^i x^8 + \zeta^{27i} x^4 + \zeta^{9i} x^2$, of the form $ux^{16} + vx^4 + wx^2$ (186 examples), along with those resulting from the binomials above via Corollary 4.2 (ii).
  For $\mathcal{G}_2$, of the form $\zeta^i x^{16} + \zeta^{17i} x^8 + \zeta^{29i} x^2$, of the form $ux^{16} + vx^4 + wx$ (155 examples), along with those resulting from the binomials above via Corollary 4.2 (ii).
- quadrinomials, there were a total of 3100 distinct linear quadrinomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_1$, and 2635 distinct linear quadrinomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_2$, along with those resulting from the trinomials above via Corollary 4.2 (ii).
- pentanomials, there were a total of 13330 distinct linear pentanomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_1$, and 13950 distinct linear pentanomials L for which $\mathcal{G}_{1,L}$ was APN and equivalent to $\mathcal{G}_2$, along with those resulting from the quadrinomials above via Corollary 4.2 (ii).

7.4. **The case $n = 6$.** For $n = 6$ we checked $\mathcal{G}_{1,L}$ over general linear functions $L(x)$ satisfying the restriction outlined in Theorem 5.1. The results obtained, up to CCZ-equivalence, are summarized in Table 2. With such a construction we were able to obtain, for every quadratic APN function listed in [16, Table 5], a CCZ-equivalent APN function $\mathcal{G}_{1,L}$. Moreover, each function in the mentioned list is CCZ-equivalent to

- $\mathcal{G}_{1,L}$ where L is a linear permutation; and
- $\mathcal{G}_{1,L}$ where L is 2-to-1.

We also found that similar results can be obtained when we consider isotopic shifts of the APN function $x^3 + \zeta^{-1} \operatorname{Tr}(\zeta^3 x^9)$; these results are summarized in Table 3.

7.5. **Additional data for isotopic shifts of $x^3 + \operatorname{Tr}(x^9)$.** We have also carried out some additional analysis for the quadratic APN function

$$F(x) = x^3 + \operatorname{Tr}(x^9). \tag{17}$$

In this case, the isotopic shift of F by a linear function L is of the form

$$f_L(x) = xL(x)(x + L(x)) + \operatorname{Tr}(xL(x)(x^7 + L^7(x))). \tag{18}$$

We may immediately observe some trivial constructions.

TABLE 2. Linear functions $L(x)$ for which $\mathcal{G}_{1,L}$ as in (7) is APN over $\mathbb{F}_{2^6} = \langle\zeta\rangle$, up to CCZ-equivalence, and their comparison with Table 5 in [16]. We also specify if $L(x)$ is 1-to-1 or 2-to-1

#-to-1	$L(x)$	no. in Table 5 [16]
1-to-1	ζx (or $x^{16} + \zeta^3 x^4 + \zeta^{17} x$)	1.1
2-to-1	$x^{32} + x^{16} + x^8 + x^4 + x^2 + \zeta^{21} x$	1.1
1-to-1	$\zeta x^{16} + \zeta^{21} x$	1.2
2-to-1	$x^{32} + \zeta x^{16} + \zeta^{27} x^8 + \zeta^{46} x^4 + \zeta^{18} x^2 + \zeta^{33} x$	1.2
1-to-1	$x^{32} + \zeta^{13} x^{16} + x^8 + \zeta^{30} x^4 + \zeta x^2 + \zeta^{20} x$	2.5
2-to-1	$x^{32} + \zeta^9 x^{16} + \zeta^{31} x^8 + \zeta^{16} x^4 + \zeta^{57} x^2 + \zeta^{29} x$	2.5
1-to-1	$x^{16} + \zeta^5 x^8 + \zeta^8 x^4 + \zeta^{34} x^2 + \zeta^{57} x$	2.12
2-to-1	$x^{16} + \zeta^5 x^8 + \zeta^8 x^4 + \zeta^{34} x^2 + \zeta^{20} x$	2.12
1-to-1	$x^8 + \zeta^5 x$	2.1
2-to-1	$x^{32} + \zeta x^{16} + \zeta^9 x^8 + \zeta^{39} x^4 + \zeta^7 x^2 + \zeta^{31} x$	2.1
1-to-1	$x^{32} + \zeta x^{16} + \zeta^{25} x^8 + \zeta^8 x^4 + \zeta^{42} x^2 + \zeta^{31} x$	2.2
2-to-1	$x^{32} + \zeta x^{16} + \zeta^{41} x^8 + \zeta^{49} x^4 + \zeta^5 x^2 + \zeta^5 x$	2.2
1-to-1	$\zeta x^{16} + x^8 + \zeta^{50} x^4 + x^2 + \zeta^{47} x$	2.6
2-to-1	$x^{32} + \zeta x^{16} + \zeta^{16} x^8 + \zeta^{26} x^4 + \zeta^{14} x^2 + \zeta^{14} x$	2.6
1-to-1	$x^{32} + \zeta x^{16} + \zeta^{23} x^8 + \zeta^{53} x^4 + \zeta^{52} x^2 + \zeta x$	2.7
2-to-1	$x^{32} + \zeta x^{16} + \zeta^{23} x^8 + \zeta^{53} x^4 + \zeta^{52} x^2 + \zeta^{56} x$	2.7
1-to-1	$x^{32} + \zeta^{23} x^8 + \zeta^{31} x^4 + \zeta^{46} x^2 + \zeta^{50} x$	2.3
2-to-1	$x^{32} + x^{16} + \zeta^{15} x^8 + \zeta^{42} x^4 + \zeta^{15} x^2 + \zeta^{16} x$	2.3
1-to-1	$x^{32} + \zeta x^{16} + \zeta^{26} x^8 + \zeta^{50} x^4 + \zeta^{57} x^2 + \zeta^{34} x$	2.8
2-to-1	$x^{32} + \zeta^{13} x^8 + \zeta^{57} x^4 + \zeta^{36} x^2 + \zeta^{31} x$	2.8
1-to-1	$x^{16} + \zeta^9 x^8 + \zeta^9 x^4 + \zeta^{47} x^2 + \zeta^{50} x$	2.9
2-to-1	$x^{32} + x^{16} + \zeta^5 x^8 + \zeta^{50} x^4 + \zeta^8 x^2 + \zeta^{60} x$	2.9
1-to-1	$x^{32} + \zeta x^{16} + \zeta^{42} x^8 + \zeta^3 x^4 + \zeta^{14} x^2 + \zeta^{22} x$	2.4
2-to-1	$x^{32} + \zeta x^{16} + \zeta^7 x^8 + \zeta^{51} x^4 + \zeta^{33} x^2 + \zeta^{14} x$	2.4
1-to-1	$x^{32} + \zeta x^{16} + \zeta^{20} x^8 + \zeta^{28} x^4 + \zeta^{23} x^2 + \zeta^{36} x$	2.10
2-to-1	$x^{32} + \zeta x^{16} + \zeta^6 x^8 + \zeta^8 x^4 + \zeta^{26} x^2 + \zeta^{21} x$	2.10

- For n even, set $L(x) = ux$ with u a primitive cubed root of unity in $\mathbb{F}_q$, so that $u^2 + u + 1 = 0$. Then we have

$$\begin{aligned} f_L(x) &= u(u+1)x^3 + \mathrm{Tr}(u(u^7+1)x^9) \\ &= (u^2+u)x^3 + \mathrm{Tr}((u^8+u)x^9) \\ &= x^3 + \mathrm{Tr}((u^2+u)x^9) \\ &= x^3 + \mathrm{Tr}(x^9). \end{aligned}$$

TABLE 3. Linear functions $L(x)$ for which the isotopic shift of $x^3 + \zeta^{-1}\operatorname{Tr}(\zeta^3 x^9)$ is APN over $\mathbb{F}_{2^6} = \langle\zeta\rangle$, up to CCZ-equivalence, and their comparison with Table 5 in [16]. We also specify if $L(x)$ is 1-to-1 or 2-to-1

#-to-1	$L(x)$	no.
1-to-1	$\zeta^9 x$	1.1
2-to-1	$x^{32} + \zeta^{12}x^{16} + \zeta^{24}x^8 + \zeta^{24}x^4 + \zeta^{30}x^2 + \zeta^{47}x$	1.1
1-to-1	$\zeta^{21} x$	1.2
2-to-1	$\zeta^{31}x^{16} + \zeta^{60}x^4 + \zeta^{11}x^2 + \zeta^{30}x$	1.2
1-to-1	$\zeta^{10}x^{16} + \zeta^{11}x^8 + \zeta^{35}x^4 + \zeta^{27}x^2 + \zeta^{26}x$	2.5
2-to-1	$\zeta^{10}x^{16} + \zeta^{11}x^8 + \zeta^{35}x^4 + \zeta^{27}x^2 + \zeta^{6}x$	2.5
1-to-1	$\zeta^{19}x^{16} + \zeta^{3}x^8 + \zeta^{29}x^4 + \zeta^{39}x^2 + \zeta^{24}x$	2.12
2-to-1	$\zeta^{28}x^{16} + \zeta x^8 + \zeta^{31}x^4 + \zeta^{51}x^2 + \zeta^{4}x$	2.12
1-to-1	$x^8 + \zeta^9 x$	2.1
2-to-1	$\zeta^{11}x^8 + \zeta^{61}x^4 + \zeta^{51}x^2 + \zeta^{33}x$	2.1
1-to-1	$\zeta^{15}x^{16} + \zeta^{6}x^8 + \zeta^{47}x^4 + \zeta^{21}x^2 + \zeta^{48}x$	2.2
2-to-1	$x^{16} + \zeta^{14}x^8 + \zeta^{49}x^4 + \zeta^{13}x^2 + \zeta^{4}x$	2.2
1-to-1	$x^{32} + \zeta^{19}x^{16} + \zeta^{23}x^8 + \zeta^{38}x^4 + \zeta^{16}x^2 + \zeta^{58}x$	2.6
2-to-1	$x^{32} + \zeta^{19}x^{16} + \zeta^{23}x^8 + \zeta^{38}x^4 + \zeta^{16}x^2 + \zeta^{25}x$	2.6
1-to-1	$x^{16} + \zeta^{7}x^8 + \zeta^{52}x^4 + \zeta^{7}x^2 + \zeta^{25}x$	2.7
2-to-1	$\zeta^{2}x^{16} + \zeta^{8}x^8 + \zeta^{40}x^4 + \zeta^{38}x^2 + \zeta^{5}x$	2.7
1-to-1	$\zeta^{3}x^8 + \zeta^{43}x^4 + \zeta^{23}x^2 + \zeta^{9}x$	2.3
2-to-1	$\zeta x^{16} + \zeta x^8 + \zeta^{4}x^4 + \zeta^{46}x$	2.3
1-to-1	$x^{16} + \zeta^{8}x^8 + \zeta^{7}x^4 + \zeta^{49}x^2 + \zeta^{46}x$	2.8
2-to-1	$x^{16} + \zeta^{8}x^8 + \zeta^{7}x^4 + \zeta^{49}x^2 + \zeta^{22}x$	2.8
1-to-1	$\zeta x^8 + \zeta^{14}x^4 + \zeta^{13}x^2 + \zeta^{43}x$	2.9
2-to-1	$\zeta x^8 + \zeta^{14}x^4 + \zeta^{13}x^2 + \zeta^{37}x$	2.9
1-to-1	$\zeta^{11}x^8 + \zeta^{22}x^4 + \zeta^{22}x^2 + \zeta^{50}x$	2.4
2-to-1	$\zeta^{3}x^{16} + \zeta^{15}x^8 + \zeta^{15}x^4 + \zeta^{40}x^2 + \zeta^{11}x$	2.4
1-to-1	$\zeta^{6}x^{16} + \zeta^{16}x^8 + \zeta^{52}x^4 + \zeta^{20}x^2 + \zeta^{52}x$	2.10
2-to-1	$\zeta x^{16} + \zeta^{16}x^8 + \zeta^{36}x^4 + \zeta^{61}x^2 + \zeta^{36}x$	2.10

- For n a multiple of 3, set $L(x) = ux$ with u a primitive 7th root of unity. Then we have

$$\begin{aligned} f_L(x) &= u(u+1)x^3 + \operatorname{Tr}(u(u^7+1)x^9) \\ &= u(u+1)x^3. \end{aligned}$$

Observation 7.1. For n a multiple of 3, the APN function x^3 can be obtained as an isotopic shift of $x^3 + \operatorname{Tr}(x^9)$.

Computational results for this case can be summarized as follows.

- When the function L has 1 term.

$n = 7$: Only two linear functions were found: $L(x) = x^8$ and $L(x) = x^{16}$. Both functions obtained are CCZ-equivalent to number 2.2 in [16, Table 7] ($x^3 + x^{17} + x^{33} + x^{34}$).

$n = 8$: Two types of linear functions yielded APN shifts:
- $L(x) = \zeta^{85}x$ and $L(x) = \zeta^{170}x$. This is the cube root of unity case observed above.
- $L(x) = \zeta^i x^{16}$, $i = 9 \cdot 2^r, 85 \cdot 2^r, 111 \cdot 2^r$. The functions obtained are CCZ-equivalent to $x^9 + \mathrm{Tr}(x^3)$.

$n = 9$: $L(x) = \zeta^i x$, $i = 73 \times j$. This is the 7th root of unity case observed above.

$n = 10$: $L(x) = \zeta^i x$, $i = 341, 682$. This is the cube root of unity case observed above.

$n = 11$: No valid monomial was found.

$n = 12$: Two types of linear functions yielded APN shifts:
- $L(x) = \zeta^i x$, $i = 1365, 2730$. This is the cube root of unity case observed above.
- $L(x) = \zeta^i x^{64}$, $i = 585 \times j$. This is the 7th root of unity case observed above.

- When the function L has 2 terms, different from x.

$n = 7$: No valid binomial was found.

$n = 8$: $L(x) = \zeta^i x^{16} + \zeta^j x$, ($j = 17$ and $i = 35, 50, 140, 200$), or ($j = 34$ and $i = 25, 70$), or ($i = 0$, $j = 85, 170$). The functions obtained are CCZ-equivalent to number 1.2 in [16, Table 9] ($x^9 + \mathrm{Tr}(x^3)$).

7.6. **Restricting the coefficients of L to $\mathbb{F}_2$.** Proposition 6.4 shows that a linear function L with coefficients in $\mathbb{F}_2$ cannot generate an APN function from isotopic shift of Gold functions over extension fields of even degree. This was investigated further computationally, over extension fields of odd degree. We looked at $\mathcal{G}_{i,L}$ for valid $\mathcal{G}_i$ and $L \in \mathbb{F}_2[x]$ to see when APN functions are obtained. The results are presented in Table 4.

It can be seen from the table that linear 2-to-1 functions occur when $n = 5$ but otherwise we only obtained APN functions from $\mathcal{G}_{i,L}$ for L a permutation polynomial.

We also looked at isotopic shifts of $x^3 + \mathrm{Tr}(x^9)$ by linear $L \in \mathbb{F}_2[x]$. For $7 \leq n \leq 12$, the only linear functions for which APN functions were obtained were for $n = 7$, with $L(x) = x^8$ or $L(x) = x^{16}$. In both cases, the obtained APN function was equivalent to $x^3 + x^{17} + x^{33} + x^{34}$, number 2.2 in [16, Table 7].

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] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[3] K. A. Browning, J. F. Dillon, R. E. Kibler, M. T. McQuistan. APN Polynomials and Related Codes. *Journal of Combinatorics, Information and System Science*, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday, vol. 34, no. 1-4, pp. 135-159, 2009.

TABLE 4. Linear functions $L(x) \in \mathbb{F}_2[x]$ for which $\mathcal{G}_{i,L}$ is APN over $\mathbb{F}_{2^n}$. The functions are divided based on the equivalence class of $\mathcal{G}_{i,L}$.

$n=3$	$\mathcal{G}_{i,L}$ equiv	$L(x)$
$\mathcal{G}_1$	$\mathcal{G}_1$	x^2, x^4
$n=5$	$\mathcal{G}_{i,L}$ equiv	$L(x)$
$\mathcal{G}_1$	$\mathcal{G}_1$	$x^{16}+x^8, x^{16}+x^8+x^2,$
$\mathcal{G}_1$	$\mathcal{G}_2$	x^2, x^4+x^2, x^8+x^2 $x^8+x^4+x^2, x^{16}, x^{16}+x^4+x^2$
$\mathcal{G}_2$	$\mathcal{G}_2$	$x^{16}+x^8, x^{16}+x^8+x^2$
$\mathcal{G}_2$	$\mathcal{G}_1$	$x^4, x^4+x^2, x^8, x^8+x^2,$ $x^8+x^4+x^2, x^{16}+x^4+x^2$
$n=7$	$\mathcal{G}_{i,L}$ equiv	$L(x)$
$\mathcal{G}_1$	$\mathcal{G}_2$	x^2, x^{64}
$\mathcal{G}_2$	$\mathcal{G}_3$	x^4, x^{32}
$\mathcal{G}_3$	$\mathcal{G}_1$	x^8, x^{16}
$n=9$	$\mathcal{G}_{i,L}$ equiv	$L(x)$
$\mathcal{G}_1$	$\mathcal{G}_2$	x^2, x^{256}
$\mathcal{G}_2$	$\mathcal{G}_4$	x^4, x^{128}
$\mathcal{G}_3$	$\mathcal{G}_1$	x^{16}, x^{32}
$n=11$	$\mathcal{G}_{i,L}$ equiv	$L(x)$
$\mathcal{G}_1$	$\mathcal{G}_2$	x^2, x^{1024}
$\mathcal{G}_2$	$\mathcal{G}_4$	x^4, x^{512}
$\mathcal{G}_3$	$\mathcal{G}_5$	x^8, x^{256}
$\mathcal{G}_4$	$\mathcal{G}_3$	x^{16}, x^{128}
$\mathcal{G}_4$	$\mathcal{G}_1$	x^{32}, x^{64}

[4] L. Budaghyan, C. Carlet, and G. Leander, *On inequivalence between known power APN functions*, BFCA 2008, Proceedings of the International Workshop on Boolean Functions: Cryptography and Applications (Copenhagen, Denmark), 2008.

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

[6] 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.

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

[8] L. Budaghyan and T. Helleseth, *New commutative semifields defined by PN multinomials*, Cryptogr. Commun. **3** (2011), 1–16.

[9] L. Budaghyan, T. Helleseth, N. Li, and B. Sun, *Some results on the known classes of quadratic APN* , Codes, Cryptology and Information Security (Said El Hajji, Abderrahmane Nitaj, and El Mamoun Souidi, eds.), Springer, Cham, 2017, pp. 3–16.

[10] C. Carlet, P. Charpin, and V. Zinoviev, *Bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15** (1998), 125–156.

[11] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.

[12] R.S. Coulter and M. Henderson, *Commutative presemifields and semifields*, Adv. Math. **217** (2008), 282–304.

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

[14] R. Cramer, Y. Dodis, S. Fehr, C. Padro, and D. Wichs. Detection of algebraic manipulation with application to robust secret sharing and fuzzy extractors. *EUROCRYPT 2008, Lecture Notes in Computer Science* 4965, pp. 471-488, 2008.
[15] P. Dembowski and T.G. Ostrom, *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.
[16] E. Edel and A. Pott, *A new almost perfect nonlinear function which is not quadratic*, Adv. Math. Commun. **3** (2009), 59–81.
[17] R. Gold, *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, IEEE Trans. Inform. Theory, **14** 1968, pp. 154–156.
[18] D.E. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.
[19] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).
[20] K. Nyberg, *Perfect nonlinear S-boxes*, Advances in Cryptology – Eurocrypt '91 (D.W. Davies, ed.), Lecture Notes in Computer Science, vol. 547, 1991, pp. 378–386.
[21] K. Nyberg, *Differentially uniform mappings in cryptography*, Advances in Cryptology – Eurocrypt '93 (T. Helleseth, ed.), Lecture Notes in Computer Science, vol. 765, 1993, pp. 55–64.
[22] J.H.M. Wedderburn, *A theorem on finite algebras*, Trans. Amer. Math. Soc. **6** (1905), 349–352.
[23] S. Yoshiara, *Equivalences of power APN functions with power or quadratic APN functions*, J. Algebr. Comb. textbf44, 2016, pp. 561–585.
[24] Y. Zhou and A. Pott. *A New Family of Semifields with 2 Parameters*. Advances in Mathematics, 234:43-60, 2013.

(L. Budaghyan, M. Calderini & I. Villa) Department of Informatics, University of Bergen, Bergen, Norway

(C. Carlet) LAGA, University of Paris 8, Paris, France and University of Bergen, Norway

(R.S. Coulter) Department of Mathematical Sciences, University of Delaware, Newark, Delaware, United States of America.