# 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, mathematics and information theory. In this paper we deduce a new method for constructing APN functions by studying the isotopic equivalence, concept defined for quadratic planar functions in fields of odd characteristic.**

**In particular, we construct a family of quadratic APN functions which provides a new example of an APN mapping over $\mathbb{F}_{2^9}$ and includes an example of another APN function $x^9+\mathrm{Tr}(x^3)$ over $\mathbb{F}_{2^8}$, known since 2006 and not classified up to now. We conjecture that the conditions for this family are satisfied by infinitely many APN functions.**

## I. Introduction

This paper is concerned with functions, 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 the paper, $\zeta$ 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 from $\mathbb{F}_q$ to itself can be represented uniquely by an element of the polynomial ring $\mathbb{F}_q[x]$ of degree less than $q$. For this reason, in order to avoid abuse of notation, we consider polynomials modulo $(x^q - x)$.

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 $\Delta$. Note that $\Delta_F$ is symmetric in $x$ and $y$. For $a \in \mathbb{F}_q^\star$, we refer to $D_aF(x) = \Delta(x,a) + F(a)$ as the *derivative of $F$ in the direction of $a$*.

Fix $\delta \in \mathbb{N}$. A function $F$ is called *differentially $\delta$-uniform* if for $a, b \in \mathbb{F}_q$, $a \neq 0$, the equation $\Delta(x,a) = b$ admits at most $\delta$ 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 $\delta$ 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 [19], while they were earlier introduced as *planar functions* by Dembowski and Ostrom [14] 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 [20]. 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, as APN functions define optimal codes in certain sense (see for instance [11]). APN functions also play a role in algebraic manipulation detection (AMD), in applied cryptography and coding, see [13].

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 $F(x) = \sum_i a_i x^{p^i}$. In this case both $\mathcal{V}(F)$ and $\ker(F)$ are subspaces of $\mathbb{F}_q$.
- $F$ is *affine* if it differs from a linear polynomial by a constant.
- $F$ is a *Dembowski-Ostrom (DO)* polynomial if $F(x) = \sum_{0\le i\le j<n} a_{ij} x^{p^i+p^j}$, whit $i<j$ if $p=2$.
- $F$ is *quadratic* if it differs from a DO polynomial by an affine polynomial.

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 (linear) equivalent* if there exist affine (respectively, linear) permutations $A_1, A_2 \in \mathbb{F}_q[x]$ for which $F' = A_1 \circ F \circ A_2$.
- *extended affine equivalent (EA-equivalent)* if $F' = (A_1 \circ F \circ A_2) + A$ for $A_1, A_2 \in \mathbb{F}_q[x]$ affine permutations and $A \in \mathbb{F}_q[x]$ affine map.
- *Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent)* [11] if there exists an affine permutation $\mathcal{L}$ of $\mathbb{F}_q \times \mathbb{F}_q$ that maps the graph of $F$, the set $G_F = \{(x, F(x)) : x \in \mathbb{F}_{p^n}\}$, onto the graph of $F'$, $\mathcal{L}(G_F) = G_{F'}$.

These equivalences 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 [11]. As the addition of a constant term does not alter the APN or

This paper was presented in part at SETA 2018.

L. Budaghyan, M. Calderini & I. Villa are with the Department of Informatics, University of Bergen, Bergen, Norway, {L.Budaghyan,M.Calderini,I.Villa}@uib.no.

C. Carlet is with LAGA, University of Paris 8, Paris, France and University of Bergen, Norway, claude.carlet@gmail.com.

R.S. Coulter is with the Department of Mathematical Sciences, University of Delaware, Newark, Delaware, United States of America, coulter@udel.edu.

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. Any finite presemifield has order a prime power $q$ and can be represented by $\mathbb{S} = (\mathbb{F}_q, +, \star)$, with field addition $+$ and multiplication $\star$ given by $x \star y = \phi(x, y)$, where $\phi \in \mathbb{F}_q[x, y]$ is a bilinear map.

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, for any $x, y \in \mathbb{F}_q$, $T(x * y) = M(x) \star N(y)$. 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, 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, [9].

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 II.1).

**Definition I.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 II 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 maps, in Section III we make some general observations on isotopic shifts. We then restrict ourselves to considering isotopic shifts of APN functions. Firstly, in Section IV, we consider how we may obtain the same function by isotopically shifting a given APN map $F$ in characteristic 2 by different $L$. Then, in Section V, 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 VI to concentrate specifically on isotopic shifts of Gold functions in characteristic 2. Highlights of our results are as follows:

- A family of quadratic APN functions is constructed over $\mathbb{F}_{2^{km}}$ using isotopic shift method (see Theorem VI.3). For $k = m = 3$, this family provides an APN function which is not CCZ-equivalent to any APN function belonging to an already known class, see Section VII-B. For $k = 4$, $m = 2$, we obtain APN maps equivalent to $x^9 + \mathrm{Tr}(x^3)$, a function known since 2006 [3] and which has not been part of any known family of APN functions up to now.
- We show that an isotopic shift of an APN function can lead to APN functions CCZ-inequivalent to the original one, even if we shift only Gold functions by linear monomials, see Lemma VI.6.
- We show that every quadratic APN function over $\mathbb{F}_{2^6}$ is EA-equivalent to an isotopic shift of $x^3$ and also EA-equivalent to an isotopic shift of $x^3 + \zeta^{-1}\,\mathrm{Tr}(\zeta^3 x^9)$.

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

## II. 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 II.1.** *Let $F, F' \in \mathbb{F}_q[x]$ be quadratic planar functions (null at 0). If $F$ and $F'$ are isotopic equivalent then $F'$ 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 $x \star y = \Delta_{F'}(x, y)$ 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). Then 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 get

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

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 II.1 shows that, for isotopic equivalent quadratic planar functions, what takes us beyond CCZ-equivalence is the isotopic shift by a linear permutation $L$. In the past years classes of APN mappings were used for constructing planar functions. For this reason we investigated whether the

isotopic shift, which can construct PN functions in fields of odd characteristic, can also construct APN maps in fields of even characteristic. 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 map can lead to APN functions CCZ-inequivalent to the original map.

## III. 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

$$F_L(L^{-1}(x)) = F_{L^{-1}}(x), \tag{3}$$

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 III.1.** *Let $F, F' \in \mathbb{F}_q[x]$ be arbitrary polynomials. If $F$ and $F'$ are EA-equivalent, say $F(x) = A_1 \circ F' \circ A_2(x) + A(x)$, in addition with the restriction $A_2(0) = 0$, 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 $F = A_1 \circ F' \circ A_2 + A$ with $A_2$ linear permutation polynomials, we have

$$\begin{aligned} F_L(x) =& \Delta_F(x, L(x)) = F(x + L(x)) - F(x) - F(L(x)) \\ =& A_1\big(F'(A_2(x) + A_2(L(x))) - F'(A_2(x)) \\ & - F'(A_2(L(x)))\big) + A(0) \\ =& A_1\big(F'(A_2(x) + M(A_2(x))) - F'(A_2(x)) \\ & - F'(M(A_2(x)))\big) + A(0), \end{aligned}$$

and with $A_3(x) = A_1(x) + A(0)$ we have $F_L = A_3 \circ F'_M \circ A_2$. □

**Corollary III.2.** *If $F, F' \in \mathbb{F}_q[x]$ are EA-equivalent and quadratic, then for $L \in \mathbb{F}_q[x]$, $F_L$ is EA-equivalent to $F'_M$ where $M = \bar{A}_2 \circ L \circ \bar{A}_2{}^{-1}$, $\bar{A}_2(x) = A_2(x) + A_2(0)$.*

*Proof.* If $F'$ is quadratic then $F' \circ A_2(x) = F'(\bar{A}_2(x)) + N(x)$, $N$ affine. Hence we have $F_L(x) = A_1 \circ F'_M \circ \bar{A}_2(x) + A_3(x)$, $A_3$ affine. □

Let $\mathrm{GL} = \mathrm{GL}(n, p)$ be the general linear group of degree $n$ over $\mathbb{F}_p$ 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 $\mathrm{N}_{\mathrm{GL}}(L)$ to be the stabiliser of $L$ under the conjugation action of GL. Then Theorem III.1 shows that isotopic shifts of $F$ by elements of $\mathcal{S}$ split 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 $M \in \mathrm{N}_{\mathrm{GL}}(L)$. 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 $F$ quadratic and $L, M$ arbitrary polynomials,

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

## IV. 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 that throughout the paper, we assume any APN function has zero constant term.)

**Theorem IV.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 IV.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 IV.1. □

A consequence of Corollary IV.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 $L(x) + x$.

## V. 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 again assume $q = 2^n$.

**Theorem V.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 IV.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 V.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 V.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 V.1 (ii). Thus, $L$ cannot be a permutation polynomial. □

In light of Theorem V.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.

### A. On $q$-to-1 $\mathbb{F}_q$-linear maps

For this subsection, $q$ is an arbitrary prime power. The number of $\mathbb{F}_q$-linear $q$-to-1 maps over $\mathbb{F}_{q^n}$ (or equivalently the number of matrices with entries in $\mathbb{F}_q$ of rank $n - 1$) is given by the following Proposition (see for instance [17]).

**Proposition V.3.** *The number of $\mathbb{F}_q$-linear $q$-to-1 maps over $\mathbb{F}_{q^n}$ is given by*

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

**Theorem V.4.** *A $\mathbb{F}_q$-linear map $L \in \mathbb{F}_{q^n}[x]$ is $q$-to-1 if and only if $L(bx) = M(x^q - x)$ for some $\mathbb{F}_q$-linear permutation $M \in \mathbb{F}_{q^n}[x]$ and some $b \in \mathbb{F}_{q^n}^\star$.*

*Proof.* It is clear that $L(bx) = M(x^q - x)$ is a (linear) $q$-to-1 map whenever $M$ is a permutation. 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 [18, Exercise 3.68]). Suppose that $M$ is not a permutation. Then, since $L_1$ is $q$-to-1 we have $\ker(M) = \langle z \rangle$ for some $z \notin \mathcal{V}(x^q - x)$ and $\mathbb{F}_{q^n} = \mathcal{V}(x^q - x) \oplus \langle z \rangle$. Consequently, $M$ is injective on $\mathcal{V}(x^q - x)$. Set $S = \mathcal{V}(M(x^q - x)) = M(\mathcal{V}(x^q - x))$ and let $w \in \mathbb{F}_{q^n}^\star \setminus S$. Now, consider $M_1$ defined by $M_1(y + cz) = M(y) + cw$ for all $y \in \mathcal{V}(x^q - x)$ and $c \in \mathbb{F}_q$. It is easy to check that $M_1$ is a linear permutation over $\mathbb{F}_{q^n}$, and $M(x^q - x) = M_1(x^q - x)$ for all $x \in \mathbb{F}_{q^n}$. □

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

**Corollary V.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 V.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 $x^2 + x + y$. □

## VI. 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 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 [16] in context of sequence design and rediscovered in 1993 by Nyberg in [20], Gold functions have played an important role in the study of APN functions, and, in particular, in understanding CCZ-equivalence [8]. 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

$$\mathcal{G}_{i,L}(x) = x^{2^i} L(x) + x L^{2^i}(x). \tag{6}$$

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 [21]. This linear equivalence extends to isotopic shifts as $\mathcal{G}_{i,L}(x)^{2^{n-i}} = \mathcal{G}_{n-i,L}(x)$.

### A. General restrictions on $L$

We expand on (6) further. Let the linear polynomial $L$ be represented as $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$. Then expanding in (6) we have

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

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

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

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 VI.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* (6) *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.*

When $L$ is a linear function, the linear operator of $\mathcal{G}_{i,L}$ has the following form:

$$\Delta_a(x) = \Delta_{\mathcal{G}_{i,L}}(x,a) = xL(a)^{2^i} + aL(x)^{2^i} + x^{2^i} L(a) + a^{2^i} L(x). \quad (7)$$

Our next result is related to Theorem V.1 and shows that in certain situations we may obtain, for Gold functions, slightly stronger restrictions on $L$ than those outlined in Theorem V.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 VI.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* (6) *is APN over $\mathbb{F}_{q^n}$ with $L$ a $q$-polynomial, then $L$ is a complete mapping over $\mathbb{F}_{q^n}$.*

*Proof.* Since $\mathcal{G}_{i,L}(x)$ is a quadratic APN function, we have $\ker(\Delta_a(ax)) = \{0,1\}$, for $a \in \mathbb{F}_{q^n}^\star$. For $x \in \mathbb{F}_q^\star$, we have $L(ax) = xL(a)$. So, if $x \in \mathbb{F}_q^\star \setminus \{0,1\}$, from (7) we have

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

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 which provides a construction of quadratic APN functions containing new examples of such functions.

**Theorem VI.3.** *Let $n = km$, $\mathbb{F}_{2^n}^\star = \langle \zeta \rangle$ 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* (6) *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

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

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 $a \in \mathbb{F}_{q^k}^\star$ and $\Delta_a(x)$ from (7). 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

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

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 VI.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 $\alpha$ and $\alpha^2$, where $\alpha$ 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 VI.3 in this case leads to a new APN function CCZ-inequivalent to known APN families.

Following the same steps of Theorem VI.3 we can extend the previous result as follows.

**Corollary VI.4.** *Let $n = km$ and $d = \gcd(q-1, \frac{q^k-1}{q-1})$, where $q = 2^m$. Let $d'$, $U$ and $W$ be defined as in Theorem VI.3. Let $L \in \mathbb{F}_{q^k}[x]$ be a $q$-polynomial and let $\mathcal{G}_i = x^{2^i+1}$ be a Gold function over $\mathbb{F}_{q^k}$ (even not APN). Then $\mathcal{G}_{i,L}$ as in* (6) *is differentially $2^j$-uniform over $\mathbb{F}_{q^k}$, where $j = \gcd(i, m)$, if and only if the following conditions are satisfied:*

(i) *for any $u \in W$, $L(u)^{2^i-1} \notin \{0, u^{2^i-1}\}$;*

(ii) *for distinct $u, v \in W$ satisfying $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$, we have*

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin U',$$

*where $U' = \langle\bar{\zeta}^{\frac{q-1}{\bar{d}}}\rangle$, $\bar{\zeta} = \zeta^{\frac{q^k-1}{q-1}}$ and $\bar{d} = \gcd(2^i-1, q-1)$.*

*Proof.* Let $a \in \mathbb{F}_{q^k}^\star$ and $\Delta_a(x)$ as (7). If we consider $x \in \mathbb{F}_q$, then we have

$$\Delta_a(ax) = ax\,L(a)\big(L(a)^{2^i-1} + a^{2^i-1}\big)\,(x^{2^i-1} + 1),$$

implying that $a\mathbb{F}_{2^j} \subseteq \ker(\Delta_a)$. Then $\mathcal{G}_{i,L}$ is differentially $2^j$-uniform over $\mathbb{F}_{q^k}$ if and only if $\ker(\Delta_a) = a\mathbb{F}_{2^j}$ for all $a \in \mathbb{F}_{q^k}^\star$. Moreover, if $\mathcal{G}_{i,L}$ is differentially $2^j$-uniform then we have that Condition (i) holds.

Now, consider any $x \in \mathbb{F}_{q^k}$, and apply the representation (8) for both $x = ut$ and $a = vs$ with $u, v \in W$ and $t, s \in \mathbb{F}_q$. Then

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

So, $\mathcal{G}_{i,L}$ is differentially $2^j$-uniform if and only if the only solutions to $\Delta_{vs}(ut) = 0$ are $t = 0$, or $u = v$ and $t \in s\mathbb{F}_{2^j}^\star$. For

establishing Condition (ii), assume $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. As $\ker(\Delta_{vs}) = vs\mathbb{F}_{2^j}$, we know that for all $t \in \mathbb{F}_q^\star$, we must have

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

Since $U' = \{t^{2^i-1} : t \in \mathbb{F}_q^\star\}$, we must have

$$\frac{v^{2^i}L(u) + uL(v)^{2^i}}{u^{2^i}L(v) + vL(u)^{2^i}} \notin U',$$

which is Condition (ii).

Conversely, assume that Conditions (i), (ii) hold. Assume that $\Delta_{vs}(ut) = 0$. We must show $t = 0$, or $u = v$ and $t \in s\mathbb{F}_{2^j}^\star$. Assume that $t \neq 0$, we have:

$$t^{2^i-1}\left(u^{2^i}L(v)+vL(u)^{2^i}\right)+s^{2^i-1}\left(v^{2^i}L(u)+uL(v)^{2^i}\right)=0. \quad (10)$$

Supposing $u = v$, (10) 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), $u^{2^i}L(u) \neq uL(u)^{2^i}$, so $t^{2^i-1} = s^{2^i-1}$, from which we deduce $t \in s\mathbb{F}_{2^j}^\star$, as required.

Now, we need 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 (10) implyes $v^{2^i}L(u) + uL(v)^{2^i} = 0$ also. So, as in Theorem VI.3 we obtain $\frac{L(u)}{u} \in \mathbb{F}_{2^{2i}}$ which contradicts Condition (i). Thus, if $x = ut$ is a solution, $u^{2^i}L(v) + vL(u)^{2^i} \neq 0$. Dividing by $u^{2^i}L(v) + vL(u)^{2^i}$ in (10) we obtain

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

However, there are no solutions to this equation by (ii). □

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

**Proposition VI.5.** *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 function, $\mathcal{G}_{i,L}$ defined as in* (6) *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 $\Delta_1(x)$ from (7), 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 $\mathbb{F}_4 \subset \ker(\Delta_1)$. □

### *B. 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 VI.6.** *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* (6)*. 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

$$\mathcal{G}_{i,L}(x) = ux^{2^i+2^j} + u^{2^i}x^{2^{i+j}+1}. \quad (11)$$

If $i = j$, then (11) 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 [5] that these two functions are CCZ-inequivalent provided $n > 3$. This proves (ii). For (iii), it is easily checked that

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

The statement in (iii) on equivalence is clear.

Now, let $\gcd(j, n) = 1$. For $a \in \mathbb{F}_q^\star$, set $\Delta_a(x)$ as in (7). 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. □

### C. Restricting $L$ to having 2 terms

Consider now $L$ as a linear binomial.

**Lemma VI.7.** *Let $m$ be a positive integer, $q = 2^n$ with $n = 2m$, and*

$$L(x) = ux^{2^m} + vx, \tag{12}$$

*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 (12), equation (6) is of the form

$$\mathcal{G}_{i,L}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + zx^{2^i+1}. \tag{13}$$

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 (13), 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 $\mathcal{G}_{i,M}$ is linear equivalent to $\mathcal{G}_{i,L}$ since
$\mathcal{G}_{i,M}(x) = u^{2^i}x^{2^{m+i}+1} + ux^{2^m+2^i} + z^{2^m}x^{2^i+1}$,
$\mathcal{G}_{i,M}(u^{-2^m}x^{2^m})^{2^m} = u^{-2^i-1}\mathcal{G}_{i,L}(x)$.

Case (iii). In this last case we obtain $\mathcal{G}_{i,M}(x^2)^{2^{2m-1}} = \mathcal{G}_{i,L}(x)$ since
$\mathcal{G}_{i,M}(x) = u^{2^{i+1}}x^{2^{m+i}+1} + u^2x^{2^m+2^i} + z^2x^{2^i+1}$.

□

**Lemma VI.8.** *Let $m$ be an even positive integer and $q = 2^{2m}$. 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 $x^{2^{m-i}+1}$ in [10]. □

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

**Lemma VI.9.** *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 (6) 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

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

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

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

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 function $\mathcal{G}_1 = x^3$ we obtain the following.

**Lemma VI.10.** *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 (6) 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

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

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

$$\begin{aligned}&a^{-3}\Delta_a(ax) =\\ &(\zeta^{2(i+l(2^m-1))} + \zeta^{i+l(2^m-1)} + \zeta^{j(2^m+1)})(x^2 + x) \neq 0.\end{aligned} \tag{14}$$

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 (14) 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 $i \neq j$. □

### D. Restricting $L$ to having 3 terms

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

$$L(x) = ax^{2^{2m}} + bx^{2^m} + cx \tag{15}$$

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

$$\begin{aligned} \mathcal{G}_{1,L}(x) =& a^2 x^{2^{2m+1}+1} + b^2 x^{2^{m+1}+1} \\ &+ ax^{2^{2m}+2} + bx^{2^m+2} + (c^2+c)x^3. \end{aligned} \tag{16}$$

As proved in Proposition VI.1, the polynomial $L(x)$ generates an isotopic shift of $\mathcal{G}_i$ equivalent to the one generated by

$$M(x) = (a\zeta^{(2^{2m}-1)j})^{2^k} x^{2^{2m}} + (b\zeta^{(2^m-1)j})^{2^k} x^{2^m} + c^{2^k} x. \tag{17}$$

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

## VII. Computational results

We studied the possible linear functions $L(x)$ for which $\mathcal{G}_{i,L}$, as in (6), 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 [15], where all known (at that time) APN functions for $n \in \{6, 7, 8, 9\}$ are listed. For purposes of comparison, we will refer to the numbering given in those lists. Later, in [22], many more quadratic APN functions were constructed for the cases $n = 7, 8$. However, in our computational results, we did not obtain any of the functions of [22] (which are not already in the lists of [15]).

Note that, since for any linear $L$ isotopic shifts by $L(x)$ and $L(x) + x$ give the same function $F_L$, whenever we have $L(x) = \sum_{j=0}^{n-1} b_j x^{2^j}$ with $b_0 = 1$ we can consider $L'(x) = \sum_{j=1}^{n-1} b_j x^{2^j}$ instead.

### A. 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 VI.6.

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 (6) 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 $\mathcal{G}_{L,1}$ more APN cases occur:

- $L(x) = ux^8 + vx = ux^{2^m} + vx$ can give functions equivalent to $\mathcal{G}_1$ or to function number 2.1 in [15, Table 5] ($x^3 + x^{10} + \zeta x^{24}$).
- $L(x) = ux^{16} + vx$, where $u$ is not a cube and $v + v^2 = 1$, gives a function equivalent to number 1.2 in [15, Table 5] ($x^3 + \zeta^{11}x^6 + \zeta x^9$).
- $L(x) = ux^{16} + vx^4$, where $u$ is not a cube and $v = u^{26}$, gives a function equivalent to number 1.2 in [15, Table 5].

### B. 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 $n \in \{6, 7, 8, 9\}$. For $n = 7$ no valid trinomial was found. For the cases $n = 6, 8, 9$, all the trinomials found are $\mathbb{F}_{2^m}$-polynomials and thus instances of Theorem VI.3. In particular we obtain:

- $n = 6$ ($k = 3$, $m = 2$): from $\mathcal{G}_1$ we can construct APN functions CCZ-equivalent to $\mathcal{G}_1$ and to number 1.2 in [15, Table 5]($x^3 + \zeta^{-1}\operatorname{Tr}(\zeta^3 x^9)$).
- $n = 8$ ($k = 4$, $m = 2$): from $\mathcal{G}_1$ we can construct APN functions CCZ-equivalent to number 1.2 in [15, Table 9]($x^3 + \operatorname{Tr}(x^9)$); from $\mathcal{G}_3$ we can construct APN functions CCZ-equivalent to number 1.11 in [15, Table 9] ($x^9 + \operatorname{Tr}(x^3)$), map not in any known family of APN functions until now.
- $n = 9$ ($k = 3$, $m = 3$): from $\mathcal{G}_1$ we can construct APN functions not CCZ-equivalent to any function from the known APN families (all CCZ-equivalent to N. 8 in Table I).

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 trinomial $L$ was found that can construct APN function.

For $n = 9$, $\mathcal{G}_{1,L}$ leads us to an inequivalence result. Hence, for $n = 3m$, we analysed the possible APN functions $\mathcal{G}_{i,L}$ as in (6) constructed using the linear function $L(x)$ of the form $ax^{2^{2m}} + bx^{2^m} + cx$. Considering Proposition VI.1 and setting to $d = c^{2^i} + c$, we obtained, up to EA-equivalence, the following results:

- $m = 2$: The obtained $\mathcal{G}_{1,L}$'s APN cases are equivalent to $\mathcal{G}_1$ or to $x^3 + \zeta^{-1}\operatorname{Tr}(\zeta^3 x^9)$.
- $m = 3$: We obtain for $\mathcal{G}_{1,L}$ the values $\{[\zeta^{424}, \zeta, \zeta^{34}]$, $[\zeta^{263}, \zeta, \zeta^{272}]$, $[\zeta^{508}, \zeta, \zeta^{132}]\}$. Using iteratively Proposition VI.1 it is possible to prove that the three cases are CCZ-equivalent to each other and, as mentioned above, $\mathcal{G}_{1,L}$ is not equivalent to any APN function from the known APN families. For $\mathcal{G}_{i,L}$ with $i \neq 1$ no APN map can be constructed.

- $m = 4$: $\mathcal{G}_{1,L}$ is APN for $[a, b, d] \in \{[\zeta^{1962}, \zeta^3, \zeta^{1365}], [\zeta^{290}, \zeta, \zeta^{2184}], [\zeta^{904}, \zeta^5, \zeta^{546}]\}$. For these cases, it is possible to prove that they are equivalent to $\mathcal{G}_1$. In particular, for any of the shift $\mathcal{G}_{1,L}$ it is possible to find $L_1$ and $L_2$ $\mathbb{F}_{2^4}$-polynomials such that $L_1(\mathcal{G}_{1,L}(x)) = \mathcal{G}_1(L_2(x))$. Using the same $L$'s, identical results are obtained for $\mathcal{G}_{i,L}$ with $i = 5$.

With the restriction on the subfield $\mathbb{F}_{2^m}$ no choice was found for $m = 5$ but for $m = 6$ we obtain that $\mathcal{G}_{1,L}$ is APN for $[a, b, d] \in \{[\zeta^{37449}, 1, \zeta^{112347}], [\zeta^{149796}, 1, \zeta^{187245}], [\zeta^{74898}, 1, \zeta^{224694}]\}$. The same results, using the identical $L$'s, can be obtained also for $\mathcal{G}_{i,L}$ for $i = 5, 7$.

**Remark VII.1.** As shown above, the conditions of Theorem VI.3 are satisfied for many functions in dimensions $n = 6, 8, 9, 12, 18$. In particular with $k = m = 3$ we obtain a map $\mathcal{G}_{1,L}$ not CCZ-equivalent to any known map so far. In addition for $k = 4$ and $m = 2$ we obtain a map $\mathcal{G}_{3,L}$ equivalent to $x^9 + Tr(x^3)$, an APN map known since 2006 [3] which has not been part of any known family of APN functions up to now. Both functions have classical Walsh spectrum (see [15] for the definition). Computations for larger $n$ are complicated and we leave this as an open problem indicated in a conjecture below.

**Conjecture VII.2.** The conditions of Theorem VI.3 are satisfied by infinitely many APN functions. That is, the family of APN functions of Theorem VI.3 is infinite.

In Table I we list, up to CCZ-equivalence, all known quadratic APN maps defined over $\mathbb{F}_{2^9}$ (with references to families to which they belong). Note that we also have families of non-quadratic power APN functions defined over $\mathbb{F}_{2^9}$ but, as proven in [21], if a quadratic APN function is CCZ-equivalent to a power function then it is EA-equivalent to a Gold functions, and, therefore, we do not need to compare the constructed functions with these power functions. In the Table we also list $\Gamma$-ranks of the functions ($\Gamma$-rank is a CCZ-invariant paramenter, see [15] for more details). To this list we added the new function found with Theorem VI.3.

Table I
CCZ-INEQUIVALENT QUADRATIC APN POLYNOMIALS OVER $\mathbb{F}_{2^9}$

| N. | Functions | $\Gamma$-rank | Families | in [15, Table 11] |
|---|---|---|---|---|
| 1 | $x^3$ | 38470 | Gold | 1.1 |
| 2 | $x^5$ | 41494 | Gold | 2.1 |
| 3 | $x^{17}$ | 38470 | Gold | 3.1 |
| 4 | $Tr_1^9(x^9) + x^3$ | 47890 | [6] | 1.2 |
| 5 | $Tr_3^9(x^{18} + x^9) + x^3$ | 48428 | [7] | 1.3 |
| 6 | $Tr_3^9(x^{36} + x^{18}) + x^3$ | 48460 | [7] | 1.4 |
| 7 | $x^3 + x^{10} + \zeta^{438}x^{136}$ | 48608 | – | 8.1 |
| 8 | $\zeta^{337}x^{129} + \zeta^{424}x^{66} + \zeta^2x^{17} + \zeta x^{10} + \zeta^{34}x^3$ | 48596 | Theorem VI.3 | – |

### C. The cases $3 \leq n \leq 5$

For these cases, all APN functions are classified [2] and they are all CCZ-equivalent to the Gold functions and to the inverse function. So, from Lemma VI.6 we have that all quadratic APN functions can be obtained from the isotopic shifts of $\mathcal{G}_1$.

### D. The case $n = 6$

For $n = 6$ we checked $\mathcal{G}_{1,L}$ with linear $L$ satisfying Theorem V.1 and obtained, for every existing quadratic APN function a CCZ-equivalent APN function $\mathcal{G}_{1,L}$. Moreover, all these quadratic APNs can be derived both by $L$ permutation and a 2-to-1 map. Similar results are obtained when we consider isotopic shifts of the APN function $x^3 + \zeta^{-1}\,\mathrm{Tr}(\zeta^3 x^9)$ (see [4, Tables 2,3]).

Note that, in general, the number of all the DO-polynomials over $\mathbb{F}_{2^n}$ is $q^{\binom{n}{2}}$, where $q = 2^n$, and the number of all the possible shifts of a fixed function $F$ are $q^n$. So, also for small values of $n$ the number of the linear shifts that we can obtain from one fixed function is much smaller than the number of the DO-polynomials. Moreover, for isotopic shifts we are restricted to only shifts by linear permutation or 2-to-1 maps which further constrains the search area. Hence, obtaining all possible quadratic APN functions for $n = 6$ as an isotopic shift of a single function, indicates that the isotopic shift is a powerful method for constructing APN functions.

### E. Additional data for isotopic shifts of $x^3 + \mathrm{Tr}(x^9)$

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

$$F_L(x) = xL(x)(x + L(x)) + \mathrm{Tr}(xL(x)(x^7 + L^7(x))). \quad (18)$$

We may immediately observe some trivial constructions.

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 $F_L(x) = x^3 + \mathrm{Tr}(x^9)$.

**Observation VII.3.** For $n$ a multiple of 3, the APN function $x^3$ can be obtained as an isotopic shift of $x^3 + \mathrm{Tr}(x^9)$ (set $L(x) = ux$ with $u$ primitive 7-th root of unity, $F_L(x) = u(u + 1)x^3$).

Computational results, which are different from the two cases above, can be summarized as follows. When the function $L$ has 1 term:

> $[n = 7]$ the obtained $F_L(x)$'s are CCZ-equivalent to number 2.2 in [15, Table 7] ($x^3 + x^{17} + x^{33} + x^{34}$);
> $[n = 8]$ the obtained $F_L(x)$'s are CCZ-equivalent to $F(x)$ or to $x^9 + \mathrm{Tr}(x^3)$;
> $[n = 11]$ no valid monomial was found.

When the function $L$ has 2 terms, different from $x$:

> $[n = 8]$ the obtained $F_L(x)$'s are CCZ-equivalent to $x^9 + \mathrm{Tr}(x^3)$.

### F. Restricting the coefficients of $L$ to $\mathbb{F}_2$

Proposition VI.5 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

$L \in \mathbb{F}_2[x]$. Except the case $n = 5$, for $3 \leq n \leq 11$ we obtained APN shifts only for $L(x) = x^{2^i}$ which is the case (ii) in Lemma VI.6. For $n = 5$ there are several polynomials which take $\mathcal{G}_i$ to $\mathcal{G}_j$ for $1 \leq i, j \leq 2$.

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 functions were CCZ-equivalent to $x^3+x^{17}+x^{33}+x^{34}$, number 2.2 in [15, Table 7].

## ACKNOWLEDGEMENTS

This research was supported by Trond Mohn Stiftelse (TMS) foundation.

## 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] M. Brinkmann and G. Leander, *On the classification of APN functions up to dimension five*. Designs, Codes and Cryptography 49.1-3 (2008), 273-288.

[3] K. A. Browning, J. F. Dillon, et al., APN Polynomials and Related Codes, Banff 2006, *Journal of Combinatorics, Information and System Science*, 34.1-4, 135-159, 2009.

[4] L. Budaghyan, M. Calderini, C. Carlet, R. Coulter, I. Villa, *Constructing APN functions through isotopic shifts*. Cryptology ePrint Archive, Report 2018/769.

[5] L. Budaghyan, C. Carlet, and G. Leander, *On inequivalence between known power APN functions*, Preceedings of BFCA 2008, Copenhagen, Denmark, May 2008.

[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.

[8] 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.

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

[10] L. Budaghyan, T. Helleseth, N. Li, and B. Sun, *Some results on the known classes of quadratic APN* , Codes, Cryptology and Information Security, Springer, Cham, 2017, pp. 3–16.

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

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

[13] 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.

[14] P. Dembowski and T.G. Ostrom, *Planes of order $n$ with collineation groups of order $n^2$*, Math. Z. **103** (1968), 239–258.

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

[16] R. Gold, *Maximal recursive sequences with 3-valued recursive crosscorrelation functions*, IEEE Trans. Inform. Theory, **14** 1968, pp. 154–156.

[17] D. Laksov, A. Thorup, "Counting Matrices with Coordinates in Finite Fields and of Fixed Rank," Math. Scand. 74, 1994, pp.19-33.

[18] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

[19] 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.

[20] 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.

[21] S. Yoshiara, *Equivalences of power APN functions with power or quadratic APN functions*, J. Algebr. Comb. **44**, 2016, pp. 561–585.

[22] Y. Yu, M. Wang, and Y. Li, *A matrix approach for constructing quadratic APN functions*, Designs, codes and cryptography 73.2 (2014): 587-600.

**Lilya Budaghyan** is a professor and a leader of the Selmer Center in Secure Communication at the University of Bergen (Norway). Her main research interest is in the field of cryptographic Boolean functions and their applications. She obtained her PhD degree from the University of Magdeburg (Germany, 2005) and habilitation degree from the University of Paris VIII (France, 2013). She has been with the University of Bergen since 2007. She also conducted her research at the Yerevan State University (Armenia, 1998-2003), University of Magdeburg (Germany, 2003-2005), University of Trento (Italy, 2005-2007), Telecom ParisTech (2011), Universities of Paris VIII and Paris XIII (2012-2013).
Prof. Budaghyan has been awarded Trond Mohn Foundation award (2016), Young Research Talent Grant from Norwegian Research Council (2014), postdoctoral fellowship award from Foundation of Mathematical Sciences of Paris (2012) and Emil Artin Junior Prize in Mathematics (2011). Since 2018 she is a member of the Norwegian Academy of Technological Sciences (NTVA).

**Marco Calderini** received the Ph.D. degrees in Mathematics from the University of Trento (Italy). From June 2015 to August 2017, he also held a postdoctoral position at the University of Trento. Since September 2017 he is a postdoctoral fellow at the Selmer Center in Secure Communication, University of Bergen (Norway). His research interests are principally Cryptography and Coding Theory.

**Claude Carlet** received the Ph.D. degree from the University of Paris 6, Paris, France, in 1990 and the Habilitation to Direct theses from the University of Amiens, France, in 1994. He was Associate Professor with the Department of Computer Science at the University of Amiens, France, from 1990 to 1994, Professor with the Department of Computer Science at the University of Caen, France, from 1994 to 2000 and with the Department of mathematics, University of Paris 8, Saint-Denis, France since then, where he is now Professor Emeritus. He is also related to the University of Bergen, Norway. His research interests include Boolean functions, cryptology and coding theory. Prof. Carlet was Associate Editor for Coding Theory of IEEE Transactions on Information Theory from March 2002 until February 2005. He is the Editor in Chief of the journal "Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences" (CCDS) published by Springer. He is in the editorial boards of the journals "Designs, Codes and Cryptography" (Springer), "Advances in Mathematics of Communications" (AIMS),"International Journal of Computer Mathematics" (Taylor & Francis), Journal of Algebraic Combinatorics (JACO, Springer) and "International Journal of Information and Coding Theory" (Inderscience publishers).

**Robert S. Coulter** obtained his Ph.D. in 1998 from the School of Computer Science and Electrical Engineering at the University of Queensland. He held postdoctoral positions with the Information Security Research Centre at the Queensland University of Technology (1998-2000) and at the Centre for Discrete Mathematics and Computing at the University of Queensland (2000-2002). He also held a Lecturer position with Deakin University (2002-2003). He has been a professor in the Department of Mathematical Sciences at the University of Delaware since 2003. His research interests include functions over finite fields and cryptology.

**Irene Villa** received the B.S. degree in mathematics from the University of Milano-Bicocca, Italy, in 2013 and the M.S. degree in mathematics from the University of Trento, Italy, in 2015. She is currently a Ph.D. student at the Department of Informatics at the University of Bergen, Norway. Her research interests include functions over finite fields and cryptology.