Triplicate functions

Lilya Budaghyan, Ivana Ivkovic, and Nikolay Kaleyski

Department of Informatics, University of Bergen

{lilya.budaghyan, ivana.ivkovic, nikolay.kaleyski}@uib.no

Abstract

We define the class of triplicate functions as a generalization of 3-to-1 functions over $\mathbb{F}_{2^n}$ for even values of n. We investigate the properties and behavior of triplicate functions, and of 3-to-1 among triplicate functions, with particular attention to the conditions under which such functions can be APN. We compute the exact number of distinct differential sets of power APN functions and quadratic 3-to-1 functions; we show that, in this sense, quadratic 3-to-1 functions are a generalization of quadratic power APN functions for even dimensions, while quadratic APN permutations are generalizations of quadratic power APN functions for odd dimensions. We show that quadratic 3-to-1 APN functions cannot be CCZ-equivalent to permutations in the case of doubly-even dimensions. We survey all known infinite families of APN functions with respect to the presence of 3-to-1 functions among them, and conclude that for even n almost all of the known infinite families contain functions that are quadratic 3-to-1 or EA-equivalent to quadratic 3-to-1 functions. We also give a simpler univariate representation of the family recently introduced by Göloglu singly-even dimensions n than the ones currently available in the literature.

I. Introduction

An (n, m)-function, or vectorial Boolean function when the dimensions n and m are clear from the context, is any function from the vector space $\mathbb{F}_2^n$ over the finite field $\mathbb{F}_2$ to the vector space $\mathbb{F}_2^m$. Intuitively, an (n, m)-function maps an input of n bits (zeros and ones) to an output of m bits; since any data can be encoded in binary, practically any operation on any kind of data can be modeled as a vectorial Boolean function. For this reason, (n, m)-functions naturally occur in many different areas of mathematics, computer science, and engineering. In particular, they play an important role in symmetric cryptography: virtually all modern block ciphers incorporate cryptographically strong (n, m)-functions as essential parts of their design; typically, the non-linear part of the cipher is modeled as a vectorial Boolean function, and so the cryptographic security of the encryption directly depends on the properties of this vectorial Boolean function. A prime example is the well-known and near ubiquitously used cipher Rijndael [32], [33], which was selected as the Advanced Encryption Standard (AES) by the US National Institute of Standards and Technology (NIST), and is considered to be one of the most reliable block ciphers to date. A crucial part of its design is an (8,8)-function carefully selected for its cryptographic properties.

One of the most efficient known cryptanalytic attacks that can be used against block ciphers is differential cryptanalysis [4]. The differential uniformity δ_F of a vectorial Boolean function F measures how well it resists differential attacks; more precisely, the lower the value of δ_F, the more resilient it is to this type of cryptanalysis. In the case when $n = m$ (so that the number of input bits is the same as the number of output bits, which is one of the most important cases in practice), we have $\delta_F \geq 2$ for any (n, n)-function F. The functions that attain this lower bound with equality are called almost perfect nonlinear (APN), and therefore provide the best possible resistance to differential cryptanalysis. The interest in studying these functions, however, is not restricted to the practical needs of cryptography: APN functions have a natural combinatorial definition, and they correspond to optimal objects in many other areas of research, including algebra, sequence design, coding theory, combinatorial design theory, projective geometry, and others. Constructing new instances of such functions, and studying their properties therefore has a far-reaching significance that has the potential to advance many other disciplines.

Unfortunately, APN functions tend to be very difficult to construct and analyze. This is partly due to the fact that they are cryptographically optimal objects, and as such do not have much structure or clear patterns. On the other hand, the number $(2^n)^{2^n}$ of (n, n)-functions becomes prohibitively large even for relatively small values of n, and means that finding APN functions by exhaustive search is completely out of the question; computational searches can only be performed on very specific subclasses of functions (where the number of functions is small enough to be processed on a computer within a reasonable amount of time), and even then, mathematical constructions and non-trivial techniques frequently have to be used in order to make the entire procedure feasible.

The vector space $\mathbb{F}_2^n$ can be identified with the finite field $\mathbb{F}_{2^n}$; and APN (n, n)-functions are typically represented as univariate polynomials over $\mathbb{F}_{2^n}$. To date, six infinite families of APN monomials, and 15 infinite families of APN polynomials have been constructed. Upon inspecting their polynomial representations in the case of even n, we can see that most of them are of a very special form: namely, all of their exponents are divisible by 3, which has the consequence that they are 3-to-1 functions (meaning that every element $y \neq 0$ in the image set $\mathrm{Im}(F)$ of one of these functions F has precisely three preimages). Upon closer inspection, we can see that even many of the known APN functions whose exponents are not all divisible by 3 are still 3-to-1 functions. This suggests that there is some connection between a function being 3-to-1 and being APN.

Functions that are 3-to-1 with all exponents divisible by 3 (which in this paper we call "canonical") have previously been studied in [26]; that paper contains some interesting results on the behavior and properties of such functions. In particular, it

helps to explain why some of the known families of APN functions have a Gold-like Walsh spectrum. Recently, 3-to-1 APN functions have been studied in more detail in [44], where some of the results from [26] are extended to the general case of 3-to-1 functions (in other words, 3-to-1 functions whose exponents are not necessarily divisible by 3). This interest in the behavior and properties of 3-to-1 APN functions is, in our opinion, well deserved, and warrants further investigation.

In this paper, we take several different approaches to investigate the properties of these functions and to facilitate their study. To begin with, we define a more general class of functions called triplicate functions that have the property that the sizes of all of their preimages are divisible by 3; in this way, a triplicate function will always map triples of inputs $\{x_1, x_2, x_3\}$ to the same output (so that $F(x_1) = F(x_2) = F(x_3)$) but, unlike a 3-to-1 function, distinct triples may still map to the same output; in this way, every 3-to-1 function is a triplicate function, but not every triplicate function is 3-to-1. We characterize triplicate functions by the values of their Walsh transform, and show that quadratic 3-to-1 functions can be considered as extremal objects (from several different points of view) among triplicate functions in a way very similar to how quadratic APN functions can be considered as extremal objects among all plateaued functions.

One of the aspects in which we see that 3-to-1 functions are extremal objects is with respect to their number of distinct differential sets (the differential sets of a function being the image sets of its derivatives). Besides deriving some results on the number of distinct differential sets of canonical quadratic triplicate functions, we compute the exact number of distinct differential sets of any power APN function (regardless of whether it is a triplicate or not). We show that if F is a power function on $\mathbb{F}_{2^n}$ and $a, b \in \mathbb{F}_{2^n}$, then $F(a) = F(b)$ if and only if $H_aF = H_bF$ (with H_aF being the differential set of F in direction a). In this way, 3-to-1 functions behave in the same way as power APN functions in the case of even n.

The paper is organized as follows. In Section II, we recall most of the preliminaries and background knowledge needed for the rest of the text. In Section III, we define the classes of triplicate functions and canonical triplicate functions (as well as the zero-sum property and triple summation property, which all known 3-to-1 APN functions have), and mathematically investigate their structural properties and behavior. In particular, we characterize triplicate functions and 3-to-1 among triplicate functions by their Walsh transform, and show that 3-to-1 among triplicate functions are extremal objects in some sense. We also characterize, in the case of power APN functions and of quadratic canonical 3-to-1 functions, when two differential sets coincide, and compute the exact number of distinct differential sets of these two classes of functions. In Section VI, we survey the known infinite APN families, and conclude that the majority of them contain functions that are canonical 3-to-1 functions. Finally, in Section VII, we summarize our results, and indicate some directions for future work.

II. Preliminaries

Throughout the paper, we denote the cardinality of a set S by $\#S$, while $|s|$ denotes the absolute value of $s \in \mathbb{Z}$. The **sumset** of a set S is the set $2S = \{s_1 + s_2 : s_1, s_2 \in S, s_1 \neq s_2\}$. A **multiset** is an unordered collection of elements, much like a set; unlike a set (which either contains or does not contain a certain element), a multiset can contain an element more than once. The number of times that an element occurs in a multiset is called the **multiplicity** of that element[1]. We write multisets using square brackets to distinguish them from ordinary sets; for instance, $[a, b, a, a, c]$ is a multiset that contains the elements a, b, and c, with multiplicities 3, 1, and 1, respectively. As shorthand, we will also write the number of occurrences of an element appearing more than once in the multiset as a superscript; for instance, we would write $[a, b, a, a, c]$ as $[a^3, b, c]$, indicating that the element a occurs three times, while b and c occur only once. On rare occasions, we will indicate the multiplicities in under-braces and write them underneath the respective elements instead.

A. Vectorial Boolean functions and their representations

Let n be a natural number. We denote by $\mathbb{F}_2$ the finite field of two elements, by $\mathbb{F}_2^n$ the vector space of dimension n over $\mathbb{F}_2$, and by $\mathbb{F}_{2^n}$ the extension field of degree n over $\mathbb{F}_2$. The multiplicative group of $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}^*$. We note that the elements of $\mathbb{F}_2^n$ can be identified with those of $\mathbb{F}_{2^n}$, and we will use both representations interchangeably throughout the paper. For any two natural numbers m, n such that $m \mid n$, we denote by $\mathrm{Tr}_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ the **trace function** from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_{2^m}$ defined as

$$\mathrm{Tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{2^{mi}}.$$

When $m = 1$, Tr_1^n is called the **absolute trace**; in this case, we will denote it more succinctly by Tr_n, or simply by Tr if the value of n is clear from the context.

Let n and m be natural numbers. Any mapping f from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called an n-dimensional **Boolean function**. Any mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called an (n, m)**-function**; in particular, Boolean functions are $(n, 1)$-functions. When the dimensions are not important, or are understood from the context, we refer to (n, m)-functions as **vectorial Boolean functions**. The intuition behind the name is that any (n, m)-function F can be represented as a vector $F = (f_1, f_2, \ldots, f_m)$ of m Boolean functions

[1]Formally, a multiset would be defined as a pair (S, m), where S is some set of elements, and $m : S \to \mathbb{N}$ is a mapping specifying the multiplicity of each element in the multiset. We consider that the idea behind multisets is intuitively clear by itself, and omit this formal definition in the text.

$f_1, f_2, \ldots, f_m : \mathbb{F}_2^n \to \mathbb{F}_2$ of dimension n. The value $f_i(x)$ for some $x \in \mathbb{F}_2^n$ gives the i-th coordinate y_i of the output $y = F(x) = (y_1, y_2, \ldots, y_m)$. For this reason, the Boolean functions $f_1, f_2, \ldots, f_n$ are called the **coordinate functions** of F. The non-zero linear combinations of the coordinate functions are called the **component functions** of F; thus, every coordinate function of F is also a component function of F, but not vice-versa. Some important properties of (n, m)-functions, including cryptographically significant parameters such as the nonlinearity, can be defined and analyzed in terms of their component functions.

The **image set** of an (n, m)-function F is the set $\mathrm{Im}(F) = \{F(x) : x \in \mathbb{F}_2^n\}$. For $y \in \mathrm{Im}(F)$, we will call the set $F^{-1}(y) = \{x \in \mathbb{F}_2^n : F(x) = y\}$ the **preimage set** of y under F. If $F(0) = 0$ and $\#F^{-1}(y) = 3$ for every $0 \neq y \in \mathrm{Im}(F)$, we will say that F is a **3-to-1 function**. If $n = m$ and $\#\mathrm{Im}(F) = 2^n$, we will say that F is a **permutation** of $\mathbb{F}_2^n$.

Vectorial Boolean functions can be represented in many different ways. The simplest representation involves writing down (or storing in memory, in the case of a computer implementation) the values $F(x)$ of the (n, m)-function F for all possible inputs $x \in \mathbb{F}_2^n$. This representation is referred to as the **truth table (TT)** or the **look-up table (LUT)** of F[2]. This representation can be quite efficient and convenient for computer implementations, since finding the value $F(x)$ of the function F at some input $x \in \mathbb{F}_2^n$ reduces to simply indexing an array stored in memory; this makes the implementation of (n, m)-functions as truth tables both very simple and very fast in practice. The disadvantage is, of course, that the memory needed to store the truth table increases rapidly with the dimensions n and m. Another drawback of the TT representation is that it is very hard to observe any structure or properties of the function from it; as we shall see, the algebraic degree (among various other properties) of a function can be extracted almost immediately from any of its polynomial representations, while in the case of the TT, this is not straightforward to do.

Any (n, m)-function can be represented as a polynomial in n variables over $\mathbb{F}_2^m$. More precisely, we can write

$$F(x_1, x_2, \ldots, x_n) = \sum_{I \subseteq \mathcal{P}(\{1,2,\ldots,n\})} a_I \prod_{i \in I} x_i,$$

where $\mathcal{P}(\{1, 2, \ldots, n\})$ is the power set of $\{1, 2, \ldots, n\}$, and $a_I \in \mathbb{F}_2^m$ for all $I \subseteq \mathcal{P}(\{1, 2, \ldots, n\})$. This representation is called the **algebraic normal form (ANF)** of F; it always exists, and is uniquely defined. When the number of terms with non-zero coefficients in the ANF is small, the ANF can provide a much more compact representation than the TT. A disadvantage is that finding the value $F(x)$ of F for some $x \in \mathbb{F}_2^n$ is no longer instantaneous, and involves performing some arithmetic operations; however, the smaller size of the representation typically far outweighs this loss in performance. Another benefit of the ANF over the TT is that it allows i.a. the algebraic degree of F to be easily extracted. For some $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ given in ANF, its **algebraic degree** is simply the degree of the ANF (as a multivariate polynomial), and is denoted by $\deg(F)$. The algebraic degree has some cryptographic significance, as a higher algebraic degree indicates good resistance to higher-order differential attacks [34], [43]. The algebraic degree also allows us to define some important classes of vectorial Boolean functions: for instance, we call an (n, m)-function F **affine** if $\deg(F) \leq 1$; then, much as the name would suggest, we have

$$F(x) + F(y) + F(z) = F(x + y + z)$$

for any $x, y, z \in \mathbb{F}_2^n$. If F is affine and $F(0) = 0$, so that $F(x) + F(y) = F(x + y)$ for any $x, y \in \mathbb{F}_2^n$, we say that F is **linear**. If $\deg(F) = 2$ or $\deg(F) = 3$, we say that F is **quadratic** or **cubic**, respectively. The class of quadratic functions, in particular, plays a central role in our investigations.

Perhaps the most frequently used representation of vectorial Boolean functions in the study of i.a. APN and AB functions is the **univariate representation**, in which a function is represented by a univariate polynomial. For this purpose, the domain $\mathbb{F}_2^n$ and co-domain $\mathbb{F}_2^m$ of an (n, m)-function are identified with the finite fields $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$; we further assume that m divides n, so that $\mathbb{F}_{2^m}$ is contained as a subfield in $\mathbb{F}_{2^n}$. Then F can be seen as a function over $\mathbb{F}_{2^n}$ which can be represented by a polynomial

$$F(x) = \sum_{i=0}^{2^n - 1} c_i x^i,$$

where $c_i \in \mathbb{F}_{2^n}$ for $i = 1, 2, \ldots, 2^n - 1$. Such a polynomial always exists (and can be obtained by e.g. Lagrange interpolation from the TT representation of F). In general, such a representation is not unique, and some additional restrictions need to be introduced in order to ensure uniqueness. However, when $n = m$ (so that the domain of F is the same as its co-domain), this representation is always unique. Since our study mostly concerns (n, n)-functions (as opposed to (n, m)-functions with $n \neq m$), we do not go into further details.

The univariate representation is quite important to our work, and to the study of APN and AB functions in general. Almost all of the known infinite constructions of APN functions are given in univariate form; and the class of canonical triplicate functions that we investigate in Section III is defined in terms of the univariate representation. Since the algebraic degree also

[2]Some authors reserve the term "truth table" for Boolean functions, whose output values 0 and 1 can be interpreted as "false" and "true", respectively, and call the more general manifestation of the same principle for (n, m)-functions with $m > 1$ (where the output can be any element of $\mathbb{F}_2^m$) a look-up table. We will refer to this representation as a truth table in both cases.

plays a prominent role in our investigation, we note that it can be recovered quite easily from the univariate representation of an (n,n)-function as well: indeed, the algebraic degree of F is the largest binary weight of any exponent i with $c_i \neq 0$ in the univariate representation (the binary weight, or 2-weight, of an integer i is the weight or, equivalently, number of non-zero bits, in its binary expansion).

Other representations of vectorial Boolean functions exist, and some of them can be quite useful. For instance, if F is a $(2n,m)$-function, it can be represented as a bivariate polynomial $F(x,y)$ with $x,y \in \mathbb{F}_2^n$. Some infinite constructions of APN functions are given in this bivariate representation (in fact, the univariate and bivariate representations are the only ones that have allowed for such infinite constructions at the time of writing). Representations of functions using tables, matrices, and algebraic structures have been considered in the literature, and some of them have been utilized computationally to find many new instances of APN and AB functions, e.g. [51], [53], [54], [48].

B. Derivatives of vectorial Boolean functions

The **derivative** of an (n,m)-function F in direction $a \in \mathbb{F}_{2^n}$ is the function $D_aF(x) = F(a+x) - F(a)$. Intuitively, $D_aF(x)$ expresses the difference between a pair of values of the function F when the difference between their corresponding inputs is equal to a. Since addition and subtraction represent the same operation over fields of even characteristic, we typically write $D_aF(x) = F(a+x)+F(x)$. An associated function is $(\Delta_aF)^*(x) = F(x)+F(a+x)+F(a)+F(0)$; in the case when F is quadratic, this is sometimes referred to as a symplectic form. The functions D_aF and $(\Delta_aF)^*$ typically behave similarly with respect to the study of i.a. cryptographic properties of functions; the advantage of $(\Delta_aF)^*$ is that it may sometimes be more convenient to work with due to it being symmetric in a and x, and since it has no constant term, i.e. $(\Delta_aF)^*(0) = 0$.

As remarked above, the value of $D_aF(x)$ intuitively represents the difference between two outputs of F for which their corresponding inputs are at distance a. From a cryptographic point of view, it is desirable that there should be no strong correlation between the input difference and the output difference. In other words, the possible output differences for some fixed $0 \neq a \in \mathbb{F}_2^n$ should be distributed as closely to uniform as possible (throughout all choices of $x \in \mathbb{F}_2^n$). In particular, the number of inputs $x \in \mathbb{F}_2^n$ for which $D_aF(x) = b$ should be as low as possible for all choices of $b \in \mathbb{F}_2^m$. In order to quantify this, we denote the number of solutions $x \in \mathbb{F}_2^n$ to the equation $D_aF(x) = b$ for some $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m$ by $\delta_F(a,b)$; that is,

$$\delta_F(a,b) = \#\{x \in \mathbb{F}_2^n : D_aF(x) = b\}.$$

Since we would like this number of solutions to be as low as possible throughout all choices of a,b, we define the **differential uniformity** of F as

$$\delta_F = \max\{\delta_F(a,b) : 0 \neq a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m\}.$$

The multiset $[\delta_F(a,b) : a,b \in \mathbb{F}_{2^n}]$ of all values of $\delta_F(a,b)$ is called the **differential spectrum** of F.

An (n,m)-function F is vulnerable to differential cryptanalysis [4] if δ_F is large. We can easily see that the numbers $\delta_F(a,b)$ are always even, since if x is a solution to $D_aF(x) = b$ for some choice of a and b, then so is $a+x$. Consequently, the optimal value of the differential uniformity is precisely 2. We say that an (n,n)-function F is **almost perfect nonlinear (APN)** if $\delta_F = 2$. Thus, the class of APN functions provides the best possible resistance to differential cryptanalysis.

While the notion of the derivative D_aF as described above is fundamental to the definition and study of APN functions, we can introduce some related auxiliary notions for the sake of convenience. The **differential set** H_aF of an (n,m)-function F in direction $a \in \mathbb{F}_2^n$ is simply the image set of the derivative D_aF, that is

$$H_aF = \mathrm{Im}(D_aF) = \{D_aF(x) : x \in \mathbb{F}_2^n\}.$$

Since $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if all of its derivatives D_aF for $0 \neq a$ are 2-to-1 functions, we can see that F is APN if and only if all of its differential sets H_aF for $0 \neq a$ have cardinality 2^{n-1}.

An (n,m)-function closely related to the derivative D_aF is

$$D_a^s(F) = F(x) + F(a+x) + F(a+s) = D_aF(x) + F(a+s),$$

where $s \in \mathbb{F}_2^n$. In [11], the function D_a^sF is called a **shifted derivative** with shift s. If $s = 0$, and $F(0) = 0$, this coincides with the notion of the symplectic form $(\Delta_aF)^*(x) = F(x)+F(a+x)+F(a)+F(0)$. Clearly, D_aF is 2-to-1 if and only if D_a^sF is 2-to-1 for any $0 \neq a \in \mathbb{F}_2^n, s \in \mathbb{F}_2^n$; and so APN-ness (and, more generally, differential uniformity) can be equivalently characterized in terms of D_a^sF.

Analogically to the differential sets H_aF, we can define

$$H_a^sF = \mathrm{Im}(D_a^sF) = \{D_a^sF(x) : x \in \mathbb{F}_2^n\}$$

for any (n,m)-function F and any $a,s \in \mathbb{F}_2^n$. We will refer to these sets as differential sets as well (in fact, we will see that for any (n,n)-triplicate function T, we have $H_aT = H_a^0T$ for any $a \in \mathbb{F}_{2^n}$, and so this should never cause any confusion).

The study of APN functions is an important area in the mathematical foundations of cryptography, and has been a topic of intense research at least since the 90's when the notion of an APN function was first introduced [47]. Since then, a huge

number of APN instances have been found, and several infinite constructions of APN functions have been deduced; a survey of these results is given in Section II-E below. As we shall see there, the vast majority of the known APN functions are quadratic (or CCZ-equivalent to quadratic functions). In fact, there is only a single known example of an APN function that is CCZ-equivalent to neither a monomial nor a quadratic function [8], [38], and finding more such instances is considered an important open problem.

One intuitive explanation for this abundance of quadratic functions among the known APN constructions and instances, is that checking and characterizing the APN-ness of quadratic functions is significantly easier than in the general case. The reason for this, in turn, is that the derivatives of any quadratic function are affine functions; and since the differential uniformity of a function (and the notion of being APN) is defined in terms of its derivatives, this means that in the quadratic case, characterizing APN functions involves studying the behavior of a set of affine functions. While by no means trivial, this is significantly more tractable than in the general case, where the derivatives may be of higher algebraic degree.

When the derivatives of F are affine, the differential sets H_aF and H_a^sF are affine subspaces of $\mathbb{F}_2^m$. As observed above, we always have $D_a^0F(0) = 0$, and so D_a^0F is, in fact, a linear function for any $a \in \mathbb{F}_{2^n}^*$ when F is quadratic. Consequently, the image set H_a^0F is a linear subspace for any $a \in \mathbb{F}_{2^n}^*$.

Recall that a **linear hyperplane** of $\mathbb{F}_2^n$ is any $(n-1)$-dimensional linear subspace of $\mathbb{F}_2^n$; and that an **affine hyperplane** is any affine $(n-1)$-dimensional subspace of $\mathbb{F}_2^n$ (in other words, a linear hyperplane plus a constant). Any linear hyperplane of $\mathbb{F}_2^n$ is a set of the form

$$\mathcal{H}(a) = \{x \in \mathbb{F}_2^n : \mathrm{Tr}(ax) = 0\}$$

for $0 \neq a \in \mathbb{F}_2^n$.

By the above discussion, we can see that if F is a quadratic (n, n)-function, then it is APN if and only if all the differential sets H_aF are affine hyperplanes (or, equivalently, if all the sets H_a^0F are linear hyperplanes) for $a \in \mathbb{F}_{2^n}^*$. More generally, we say that an (n, n)-function F is **generalized crooked** if all of its differential sets H_aF for $a \in \mathbb{F}_{2^n}^*$ are affine hyperplanes [45]; in the particular case when all the differential sets H_aF are complements of linear hyperplanes, we say that F is **crooked**. Clearly, any generalized crooked function is APN, and any quadratic APN function is generalized crooked; the existence of generalized crooked functions that are not quadratic is an open problem at the time of writing.

For any set $S \subseteq \mathbb{F}_{2^n}$ and any (n, n)-function F, we will denote by $[S] = \{a \in \mathbb{F}_{2^n} : H_aF = S\}$ the set of all derivative directions a for which the differential set H_aF is equal to S. In particular, we have $a \in [H_aF]$ for all $a \in \mathbb{F}_{2^n}$.

The ortho-derivative π_F [19] is an (n, n)-function that can be associated with any generalized crooked (n, n)-function F. For any $a \in \mathbb{F}_{2^n}^*$, the differential set H_a^0F of any 3-to-1 function is a linear hyperplane, and so can be written as $H_a^0F = \mathcal{H}(c_a)$ for some $c_a \in \mathbb{F}_{2^n}^*$. We define the **ortho-derivative** π_F by setting $\pi_F(a) = c_a$ for every $a \in \mathbb{F}_{2^n}^*$, and $\pi_F(0) = 0$[3]. The ortho-derivatives of two EA-equivalent quadratic APN functions are EA-equivalent themselves [19] which allows EA-inequivalent functions to be distinguished with very high accuracy by comparing the values of EA-invariants (such as the differential spectrum) of their ortho-derivatives (equivalence relations between (n, n)-functions are discussed in more detail in Section II-D).

C. The Walsh transform

The Walsh transform of an (n, m)-function F is the function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{Z}$ defined by

$$W_F(a, b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{b \cdot F(x) + a \cdot x},$$

where "$\cdot$" is a scalar product on $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$, respectively (the dimension being understood from the context). A scalar product on $\mathbb{F}_2^n$ is a symmetric bivariate function on $\mathbb{F}_2^n$ such that $x \mapsto a \cdot x$ is a non-zero linear form for any $0 \neq a \in \mathbb{F}_2^n$. Using the identification of the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, this is typically defined as $x \cdot y = \mathrm{Tr}(xy)$, with the product xy being computed in the finite field $\mathbb{F}_{2^n}$, and then mapped to $\mathbb{F}_2$ via the absolute trace function. When $n = m$, the Walsh transform $W_F : \mathbb{F}_{2^n}^2 \to \mathbb{Z}$ of an (n, n)-function F can equivalently be written as

$$W_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} \chi(bF(x) + ax),$$

where $\chi : \mathbb{F}_{2^n} \to \mathbb{Z}_2$ is the canonical additive character of $\mathbb{F}_{2^n}$ defined by $\chi(x) = (-1)^{\mathrm{Tr}(x)}$. For convenience, for $a \in \mathbb{F}_{2^n}$, we will also denote by χ_a the character $\chi_a(x) = \chi(ax)$. The values of the Walsh transform W_F are called the **Walsh coefficients** of F. The multiset of all Walsh coefficients is called the **Walsh spectrum** of F; and the multiset of their absolute values is called the **extended Walsh spectrum** of F and denoted by $\mathcal{W}_F$; symbolically:

$$\mathcal{W}_F = [|W_F(a, b)| : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^m].$$

[3]More generally, the ortho-derivative of F can be defined as any (n, n)-function π_F for which $\pi_F(a)$ lies in the orthogonal complement of H_a^0F, which is possible even when F is not generalized crooked (as long as its differential sets H_a^0F are linear hyperplanes). If F is not generalized crooked, however, the ortho-derivative is not uniquely defined, and so we restrict to the case when F is generalized crooked.

The Walsh transform can be a useful theoretical tool for analyzing properties of vectorial Boolean functions, and it can be used to speed up some computations in practice.

There is a number of well-known characterizations of various properties of vectorial Boolean functions in terms of the Walsh transform. For instance, we know that any (n, n)-function F satisfies

$$\sum_{a,b\in\mathbb{F}_{2^n}} W_F^4(a, b) \geq 3 \cdot 2^{4n} - 2^{3n+1},$$

with equality if and only if F is APN [29]. Similarly, we know that any APN (n, n)-function F with $F(0) = 0$ satisfies

$$\sum_{a,b\in\mathbb{F}_{2^n}} W_F^3(a, b) = 3 \cdot 2^{3n} - 2^{2n+1},$$

although, in general, this is only a necessary and not a sufficient condition for a function to be APN.

The Walsh transform allows for the definition of another important class of vectorial Boolean functions, viz. the plateaued functions, that have a close connection to APN functions, and appear in the context of our investigations of triplicate functions as well. We say that an (n, m)-function F is **plateaued** if there exist integers $\lambda_b \in \mathbb{Z}$ for $b \in \mathbb{F}_2^m$ such that

$$W_F(a, b) \in \{0, \pm\lambda_b\}$$

for all $a \in \mathbb{F}_2^n$; we then call λ_b the **amplitude** of the component function F_b. If the amplitudes of all components are equal, i.e. for all $b, b' \in \mathbb{F}_2^m$ we have $\lambda_b = \lambda_{b'}$, we say that F is **plateaued with single amplitude**.

As in the case of the generalized crooked functions, the interest in the study of plateaued functions arises from the behavior of quadratic APN functions. More precisely, we know that any quadratic APN function is plateaued [56], [20], although there exist APN functions that are not plateaued, and plateaued functions that are not APN.

D. Equivalence relations

The number of (n, n)-functions is very large even for small values of n, and for this reason, they are typically only classified up to some notion of equivalence that preserves the properties of interest. In the case of APN functions, the most general known equivalence relation that preserves the differential uniformity (and hence, the property of being APN) is the so-called CCZ-equivalence (or Carlet-Charpin-Zinoviev equivalence) introduced in [25].

The graph Γ_F of an (n, m)-function F is the set $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\} \subseteq \mathbb{F}_2^n \times \mathbb{F}_2^m$. Note that $\mathbb{F}_2^n \times \mathbb{F}_2^m$ can be naturally identified with $\mathbb{F}_2^{n+m}$, and so the set of pairs Γ_F can be seen as a set of elements from $\mathbb{F}_2^{n+m}$. If F and G are two (n, m)-functions, we say that they are **CCZ-equivalent** if there exists an affine permutation A of $\mathbb{F}_2^{n+m}$ mapping Γ_F to Γ_G, i.e. such that $A(\Gamma_F) = \Gamma_G$.

Another widely used equivalence relation is the so-called extended affine equivalence, or EA-equivalence for short. We say that $F, G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are **EA-equivalent** if there exist affine permutations A_1 and A_2 of $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$, respectively, and an affine (n, m)-function A, such that

$$A_1 \circ F \circ A_2 + A = G. \tag{1}$$

We know that EA-equivalence is a special case of CCZ-equivalence; that is, if two functions are EA-equivalent, then they are also CCZ-equivalent. However, CCZ-equivalence is strictly more general than EA-equivalence and taking inverses of permutations [15]. Nonetheless, CCZ-equivalence coincides with EA-equivalence in the case of quadratic APN functions; more precisely, if F and G are quadratic APN (n, n)-functions, then F and G are EA-equivalent if and only if they are CCZ-equivalent [52]. Since almost all of the known APN functions are quadratic, this means that in practice almost all tests for CCZ-equivalence can be reduced to tests for EA-equivalence.

Some special cases of EA-equivalence can be obtained by applying additional constraints to the functions A_1, A_2, and A from (1). If $A = 0$, we say that F and G are **affine equivalent**; and if, in addition, $A_1(0) = A_2(0) = 0$ so that A_1 and A_2 are linear, we say that F and G are **linear equivalent**.

E. Known APN functions

Some of the earliest, and most fascinating in a number of ways, examples of APN functions are given by monomials in their univariate polynomial representation. These functions are referred to as power functions, or monomial functions. At present, we know of six infinite families of monomial APN functions. These are summarized in Table I below. A conjecture of Dobbertin states that any APN monomial is CCZ-equivalent to an instance from one of the families in Table I.

In addition to the six infinite monomial families, a number of infinite polynomial constructions have been discovered; these are summarized in Table II. As we can observe from the table, the univariate polynomial form of these families can be quite varied; and yet, despite this, all of the functions listed in Table II are quadratic. Constructing an infinite family of APN functions CCZ-inequivalent to both monomials and quadratic functions would be a groundbreaking result. Furthermore, it is

TABLE I
KNOWN INFINITE FAMILIES OF APN POWER FUNCTIONS OVER $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	2^i+1	$\gcd(i,n)=1$	2	[39], [47]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1$	$i+1$	[41], [42]
Welch	2^t+3	$n=2t+1$	3	[36]
Niho	$2^t+2^{t/2}-1$, t even $2^t+2^{(3t+1)/2}-1$, t odd	$n=2t+1$	$(t+2)/2$ $t+1$	[35]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	[3], [47]
Dobbertin	$2^{4i}+2^{3i}+2^{2i}+2^i-1$	$n=5i$	$i+3$	[37]

almost certain that the infinite families from Tables I and II constitute only a minuscule portion of the possible constructions; finding new infinite families of APN functions is an important ongoing problem.

We note that the families C14-1 and C14-2 have not been published yet, but univariate and bivariate representations can be found e.g. in the survey [18].

TABLE II
KNOWN INFINITE FAMILIES OF QUADRATIC APN POLYNOMIALS OVER $\mathbb{F}_{2^n}$

ID	Functions	Conditions	Source
C1-C2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12$, u primitive in $\mathbb{F}_{2^n}^*$	[12]
C3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m, \gcd(i,m)=1, c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[10]
C4	$x^3+a^{-1}\mathrm{Tr}_n(a^3x^9)$	$a\neq 0$	[13]
C5	$x^3+a^{-1}\mathrm{Tr}_n^3(a^3x^9+a^6x^{18})$	$3\|n$, $a\neq 0$	[14]
C6	$x^3+a^{-1}\mathrm{Tr}_n^3(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$	[14]
C7-C9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\|(k+s)$, u primitive in $\mathbb{F}_{2^n}^*$	[6]
C10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m, m\geq 2$ even, $\gcd(k,m)=1$ and $i\geq 2$ even, u primitive in $\mathbb{F}_{2^n}^*, u'\in\mathbb{F}_{2^m}$ not a cube	[57]
C11[4]	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd, $L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Theorem VI.3 of [9]	[9]
C12	$u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q=2^m, n=2m, \gcd(i,m)=1$, $x^{2^i+1}+ax+b$ has no roots in $\mathbb{F}_{2^m}$	[50]
C13	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n=2m=10$, $(a,b,c)=(\beta,1,0,0)$, $i=3$, $k=2$, β primitive in $\mathbb{F}_{2^2}$ $n=2m$, m odd, $3\nmid m$, $(a,b,c)=(\beta,\beta^2,1)$, β primitive in $\mathbb{F}_{2^2}, i\in\{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[16]
C14-1	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{2i}+1}+x^{2^{2i}}y+y^{2^{2i}+1})$	$n=2m, \gcd(3i,m)=1$	[5]
C14-2	$(x^{2^i+1}+xy^{2^i}+y^{2^i+1}, x^{2^{3i}}y+xy^{2^{3i}})$	$n=2m, \gcd(3i,m)=1$, m odd	[5]
C15	$a\mathrm{Tr}_m^n(bx^3)+a^q\mathrm{Tr}_m^n(b^3x^9)$	$n=2m$, m odd, $q=2^m$, $a\notin\mathbb{F}_q$, b not a cube	[55]

III. TRIPLICATE FUNCTIONS

In this section, we introduce the class of triplicate functions as a generalization of 3-to-1 functions, and conduct a theoretical study of their basic structural properties and their relation to APN functions. We derive several different characterizations of such functions, and show that 3-to-1 functions among triplicate functions are extremal objects in a number of ways. We also recall, adapt, and generalize some known results on 3-to-1 functions.

[4]We note that C11 is not an infinite family in the strict sense, since Theorem VI.3 of [9] contains complex conditions characterizing when the function in question is APN. These conditions cannot be easily verified, and at the moment we do not even know whether they can be satisfied for infinitely many values of n. In this sense, C11 is a construction that requires non-trivial computation searches to find APN functions, and this makes it difficult to traverse all functions belonging to it, and to characterize when they are 3-to-1 functions. For all of these reasons, we do not consider the functions from C11 in this paper, but still list it in the table for the sake of completeness.

[5]F. Göloglu, private communication

The section is organized as follows. In Subsection III-A, we introduce the classes of triplicate functions and canonical triplicate functions, and some other basic notions that we will use throughout the paper. We recall the most important known results on 3-to-1 functions from [26] and [44], and make some simple but fundamental structural observations on the behavior of triplicate and canonical triplicate functions.

In Section III-B, we show how triplicate functions can be characterized using the Walsh transform. We then characterize 3-to-1 among the triplicate functions, show that they are extremal objects in some sense, and prove that some exponential sums involving the second power moment of the Walsh transform are constant in the case of 3-to-1 functions.

In Section III-D, we show that the image set of any quadratic 3-to-1 function is a partial difference set with prescribed parameters, generalizing a result from [26]. As a consequence of this fact, we compute the exact value of the multiset Π_F from [11] (which is a CCZ-invariant for APN functions) for any quadratic 3-to-1 function, and use it to compute a lower bound on the Hamming distance between any two quadratic 3-to-1 functions, and to give an upper bound on the total number of such functions over $\mathbb{F}_{2^n}$ for any even n.

A. Basic notions

A number of the known APN functions have a univariate polynomial form in which all exponents are multiples of 3. The simplest example is the Gold function x^3, which is known to be APN over $\mathbb{F}_{2^n}$ for any extension degree n; we also know that any APN power function x^d over $\mathbb{F}_{2^n}$ must have $\gcd(d,n)=3$ for n even (see e.g. [23]); and so any power APN function over a finite field of even extension degree must be of this form. Furthermore, one can observe many such instances among the APN functions from the known infinite polynomial families; for example, all the exponents of the binomials from family C1-C2 over $\mathbb{F}_{2^n}$ are divisible by 3 when n is even (we present a formal proof in Proposition 8). In Section VI, we survey the known infinite polynomial families of APN functions with respect to this property. Most of the known families contain functions of this form, and some of them, in fact, consist entirely of such functions.

When n is even, the finite field $\mathbb{F}_{2^2}$ is a subfield of $\mathbb{F}_{2^n}$; let β be a primitive element of $\mathbb{F}_{2^2}$. Suppose that F is a function with no constant term (so that $F(0)=0$) and that all of its exponents are divisible by 3. Since $\beta^3=1$, we have

$$F(x)=F(\beta x)=F(\beta^2 x) \tag{2}$$

for any $x\in\mathbb{F}_{2^n}$. Thus, multiplying the input of the function F by a non-zero element from $\mathbb{F}_{2^2}$ does not change its output. In particular, the non-zero inputs $x\in\mathbb{F}_{2^n}^*$ to F can be partitioned into triples $\{x,\beta x,\beta^2 x\}$ such that $F(x)=F(\beta x)=F(\beta^2 x)$. Note that, depending on the concrete function F, distinct triples may also map to the same image; if all the triples map to distinct images (in which case F is a 3-to-1 function), the image set of F will consist of precisely $1+(2^n-1)/3$ elements, including 0. Another way to look at this is to consider the pre-images $F^{-1}(y)=\{x\in\mathbb{F}_{2^n} : F(x)=y\}$ of the non-zero elements $y\in\mathbb{F}_{2^n}^*$; then the cardinality of each pre-image $F^{-1}(y)$ for $y\in\mathbb{F}_{2^n}^*$ is a multiple of 3; if all the triples map to distinct values, then the size of each pre-image is exactly 3, and so the image set of F consists of precisely $\frac{2^n-1}{3}+1$ elements, which is the minimum possible size of the image set of any APN function in even dimension [24]. We will call functions whose non-zero inputs can be partitioning into triples $\{x,y,z\}$ mapping to the same value triplicate functions. Note that triplicate functions can only exist for even values of n, since 3 is a divisor of 2^n-1 if and only if n is even.

The number of distinct triples of non-zero elements, viz. $(2^n-1)/3$, will appear quite frequently throughout the following discussion; for the sake of simplicity, we will typically denote it by $K=(2^n-1)/3$ when the dimension n is clear from the context. We also introduce the following notion to facilitate the discussion.

Definition 1. Let n be an even natural number and $K=(2^n-1)/3$. We say that a sequence $\mathcal{T}=\{T_i\}_{i=1}^K=\{\{a_i,b_i,c_i\}\}_{i=1}^K$ of unordered triples of elements from $\mathbb{F}_{2^n}^*$ is a **triple partition** of $\mathbb{F}_{2^n}$ if:

1) $\bigcup_{i=1}^K T_i=\mathbb{F}_{2^n}^*$;
2) $T_i\cap T_j=\emptyset$ for $i\neq j$.

If F is a function over $\mathbb{F}_{2^n}$ with $F(0)=0$, we say that $\mathcal{T}$ **corresponds** to F if, for any $\{x,y,z\}\in\mathcal{T}$, we have $F(x)=F(y)=F(z)$.

In the following definition, we consider the slightly more general case of (n,m)-functions (allowing the dimensions m and n to be distinct). While we concentrate primarily on (n,n)-functions throughout the paper, the proof of Proposition 4 for (n,m)-functions proceeds by induction on m (with the proof for (n,n)-functions that we are actually interested in following from this general case by setting $m=n$), and so we need this more general context.

Definition 2. Let m,n be natural numbers with n even, and let F be an (n,m)-function with $F(0)=0$. If $\mathbb{F}_{2^n}^*$ can be partitioned into disjoint triples $T_i=\{a_i,b_i,c_i\}_i$ for $i=1,2,\ldots,K=(2^n-1)/3$ such that $F(a_i)=F(b_i)=F(c_i)$ for $i=1,2,\ldots,(2^n-1)/3$ (equivalently, if there is a triple partition $\mathcal{T}$ that corresponds to F), then we say that F is a **triplicate function**. If $T_i=\{a_i,b_i,c_i\}\in\mathcal{T}$ corresponding to F, we will sometimes write $F(T_i)$ as shorthand for $F(a_i)$ (or, equivalently, $F(b_i)$ or $F(c_i)$).

While any (n, n)-function for even n with exponents divisible by 3 partitions the non-zero inputs of $\mathbb{F}_{2^n}$ into triples, the converse implication is not true; that is, one can easily find triplicate functions whose exponents are not all multiples of 3. Indeed, we can see that when the exponents of F are all divisible by 3, the triples T_i can systematically be taken in the form $\{x, \beta x, \beta^2 x\}$ for $x \in \mathbb{F}_{2^n}^*$. Partitioning $\mathbb{F}_{2^n}^*$ into triples and assigning output values to those triples in an arbitrary way so that e.g. 1 and β lie in triples mapping to distinct output values is then enough to define a triplicate function whose exponents are not all divisible by 3. To differentiate between these two notions, we introduce the following definition. Note that we only define this notion for (n, n)-functions (instead of (n, m)-functions as in Definition 2) since the definition is in terms of the univariate representation.

Definition 3. Let n be an even natural number, and let F be an (n, n)-function with $F(0) = 0$. If every exponent i with a non-zero coefficient a_i in the univariate polynomial form of F is divisible by 3, then we say that F is a **canonical triplicate function**.

Thus, any canonical triplicate function is a triplicate function, but not vice-versa. We note that 3-to-1 functions (as a special subclass of triplicate functions and canonical triplicate functions) and their relation to APN functions have been previously studied in [26]; canonical triplicate functions are also studied in [44] where they are called 3-divisible functions. In particular, in [26] the authors show that any quadratic canonical triplicate function is APN if and only if it is 3-to-1 (in other words, if all triples map to distinct values); and in [44], it is shown that any plateaued (and, in particular, quadratic) 3-to-1 function is APN. Similarly, an important result of [26] is that any quadratic canonical triplicate APN function has a Gold-like Walsh spectrum; and Theorem 11 of [44] extends this to the more general case of any plateaued triplicate function. We thus have the following noteworthy results.

Theorem 1. [26], [44] Let F be an (n, n)-triplicate function for some even natural number n. Then:

1) if F is APN, then F is 3-to-1;
2) if F is plateaued and 3-to-1, then F is APN.

We note that any quadratic function is, in particular, plateaued [56], [20]. Consequently, the notions of 3-to-1-ness and APN-ness coincide in the case of quadratic triplicate functions.

Theorem 2. [26], [44] Let F be a plateaued 3-to-1 APN function over $\mathbb{F}_{2^n}$ with n even. Then

$$W_F(0, b) \in \{(-1)^k 2^k, (-1)^{k+1} 2^{k+1}\} \tag{3}$$

for any $b \in \mathbb{F}_{2^n}^*$, where $n = 2k$, and so

$$W_F(a, b) \in \{0, \pm 2^k, \pm 2^{k+1}\}$$

for any $a \in \mathbb{F}_{2^n}$ and any $b \in \mathbb{F}_{2^n}^*$, i.e. F has a Gold-like Walsh spectrum.

Theorem 2 allows us to give an easy proof that the extended Walsh spectra of functions belonging to a number of the known infinite APN families are Gold-like. Particularly in the case of canonical triplicates, it can be quite easy to show that all the exponents in the univariate representation of some families are divisible by 3; the exact form of the extended Walsh spectrum then follows immediately from Theorem 2. We will see examples of such computations in Section VI, where we study which of the known infinite families of APN polynomials contain, or consist of, triplicate functions.

In particular, the Walsh spectrum of the recently constructed family C13 has not been previously computed; in Proposition 8, we show that all functions belonging to this family are canonical triplicates, and thereby prove that they have a Gold-like Walsh spectrum.

Due to Theorem 1, we will mostly be interested in the properties and behavior of 3-to-1 triplicate functions, whether canonical or not. We can observe that canonical 3-to-1 functions have some useful properties that can be utilized in constructions and proofs; in particular, virtually all proofs related to canonical 3-to-1 functions rely on one of these properties rather than the functions being canonical triplicates per se. At the time of writing, all known 3-to-1 APN functions have these properties. Whether this is true for any 3-to-1 APN function and, indeed, whether any 3-to-1 APN function is linear-equivalent to a canonical one, we do not know at the moment. In order to make the subsequent proofs and arguments as general as possible, we formulate these properties independently of the notion of canonical triplicates.

Recall that the sumset of a set S is the set $2S = \{s_1 + s_2 : s_1, s_2 \in S, s_1 \neq s_2\}$. As observed in [31], a necessary condition for an (n, n)-function F to be APN is that for any $a, b \in \mathrm{Im}(F)$ with $a \neq b$, the sumsets of $F^{-1}(a)$ and $F^{-1}(b)$ should be disjoint. Indeed, if $x_1, x_2 \in F^{-1}(a)$ and $y_1, y_2 \in F^{-1}(b)$ with $x_1 + x_2 = y_1 + y_2$, then $D_w F(x_1) = D_w F(y_1) = 0$ for $w = x_1 + x_2$, which implies that F is not APN. For this reason, we will frequently consider only triple partitions $\mathcal{T}$ for which the sumsets of any two distinct triples T_i and T_j are disjoint. We formalize this as follows.

Definition 4. Let $\mathcal{T} = \{T_i\}_{i=1}^K$ be a triple partition of $\mathbb{F}_{2^n}$ for some even natural number n. We say that $\mathcal{T}$ has **disjoint sumsets** if $2T_i \cap 2T_j = \emptyset$ for any $i, j \in \{1, 2, \ldots, K\}$ with $i \neq j$. If $\mathcal{T}$ corresponds to an (n, n)-function F, then we will say that F has disjoint sumsets.

We can immediately see that any canonical 3-to-1 function has disjoint sumsets. In fact, this is implied by the stronger condition that the elements in any triple $\{x, \beta x, \beta^2 x\}$ corresponding to a canonical 3-to-1 function sum to 0.

Definition 5. Let $\mathcal{T} = \{T_i\}_{i=1}^K = \{\{a_i, b_i.c_i\}\}_{i=1}^K$ be a triple partition of $\mathbb{F}_{2^n}$ for some natural number n. We say that $\mathcal{T}$ has the **zero-sum property** if $a_i + b_i + c_i = 0$ for $i = 1, 2, \ldots, K$. If F corresponds to $\mathcal{T}$, then we say that F has the zero-sum property, or that F is a zero-sum triplicate.

We can easily see that any canonical 3-to-1 function has the zero-sum property since its preimage sets are of the form $\{x, \beta x, \beta^2 x\}$ for $x \in \mathbb{F}_{2^n}^*$. It is also not difficult to see that the zero-sum property is preserved under linear equivalence. Indeed, suppose that we have $L_1 \circ F_1 \circ L_2 = F_2$ for some (n, n)-functions F_1, F_2, L_1, L_2 with L_1, L_2 linear permutations. Suppose, furthermore, that F_1 has the zero-sum property. Since L_1 maps 0 to 0, it cannot possibly affect the zero-sum property, and so we can assume that L_1 is the identity and we have simply $F_1 \circ L_2 = F_2$. Now, consider some distinct $x, y, z \in \mathbb{F}_{2^n}$ such that $F_2(x) = F_2(y) = F_2(z)$. Then $F_1(L_1(x)) = F_1(L_1(y)) = F_1(L_1(z))$, and so $L_1(x) + L_1(y) + L_1(z) = 0$ since F_1 has the zero-sum property. By the linearity of L_1, we get $L_1(x + y + z) = 0$ and hence $x + y + z = 0$. Thus, F_2 has the zero-sum property as well.

According to our computational results, all known 3-to-1 APN functions over $\mathbb{F}_{2^n}$ for $n \leq 14$ have the zero-sum property. We conjecture that this is true in general. Note that we only formulate the conjecture for the quadratic case. In fact, we suspect that it might hold for 3-to-1 APN functions of higher algebraic degree as well; but since at the time of writing we know very few non-quadratic APN functions, we consider that we have sufficient empirical data to state such a conjecture only for the quadratic case.

Conjecture 1. Any quadratic 3-to-1 function (which is then necessarily APN) has the zero-sum property.

We can observe that the canonical 3-to-1 functions have another interesting property: if we consider two distinct preimage sets $\{x, \beta x, \beta^2 x\}$ and $\{y, \beta y, \beta^2 y\}$ for some $x, y \in \mathbb{F}_{2^n}$, we can see that $\{x + y, \beta x + \beta y, \beta^2 x + \beta^2 y\}$ is also a preimage set; and so is e.g. $\{x + \beta y, \beta x + \beta^2 y, \beta^2 x + y\}$. In this sense, the "sum" of two triples T_i and T_j from $\mathcal{T}$ is also a triple T_k from $\mathcal{T}$. We note that two triples can be "summed" like this in $3! = 6$ distinct ways, and precisely 3 of them give triples from $\mathcal{T}$; for instance, if we add x to y but βx to $\beta^2 y$, then $\{x + y, \beta x + \beta^2 y, \beta^2 x + \beta y\}$ is not a triple T_k for any k. We will refer to this as the *triple summation property*.

Definition 6. Let $\mathcal{T} = \{T_i\}_{i=1}^K$ be a triple partition of $\mathbb{F}_{2^n}$ for some even natural number n. We say that $\mathcal{T}$ has the **triple summation property** if, for any two distinct triples of elements $T = \{a, b, c\}$ and $T' = \{x, y, z\}$ from $\mathcal{T}$, the following three conditions are satisfied:

- $\{a + x, b + y, c + z\} \in \mathcal{T}$, or $\{a + x, b + z, c + y\} \in \mathcal{T}$; and
- $\{a + y, b + z, c + x\} \in \mathcal{T}$, or $\{a + y, b + x, c + z\} \in \mathcal{T}$; and
- $\{a + z, b + y, c + x\} \in \mathcal{T}$, or $\{a + z, b + x, c + y\} \in \mathcal{T}$.

Note that if e.g. $\{a + x, b + y, c + z\} \in \mathcal{T}$ in the first condition above, then $\{a + y, b + x, c + z\} \notin \mathcal{T}$ and so necessarily $\{a + y, b + z, c + x\} \in \mathcal{T}$ from the second condition since $c + z$ cannot belong to two distinct triples from $\mathcal{T}$. Following the same logic, we can equivalently say that $\mathcal{T}$ has the triple summation property if

- $\{a + x, b + y, c + z\}, \{a + y, b + z, c + x\}, \{a + z, b + x, c + y\} \in \mathcal{T}$; or
- $\{a + x, b + z, c + y\}, \{a + y, b + x, c + z\}, \{a + z, b + y, c + x\} \in \mathcal{T}$.

If an (n, n)-function F corresponds to $\mathcal{T}$, then we also say that F has the triple summation property.

Just like the zero-sum property, the triple summation property is preserved under linear equivalence. Indeed, we can observe that if $L_1 \circ F_1 \circ L_2 = F_2$ as before, then L_1 does not affect this property since it only changes the image set of the function (and not the way in which the elements of $\mathbb{F}_{2^n}^*$ combine into triples); we can thus assume that L_1 is the identity, so that we have $F_1 \circ L_2 = F_2$. But since L_2 is additive and maps triples from the triple partition corresponding to F_1 to triples from the triple partition corresponding to F_2, we can see that F_1 has the triple summation property if and only if F_2 does.

We can observe that any function having the triple summation property and having disjoint sumsets also has the zero-sum property as follows.

Proposition 1. Let F be a 3-to-1 (n, n)-function with the triple summation property and distinct sumsets. Then F has the zero-sum property.

Proof. Let $\mathcal{T} = \{T_i\}_{i=1}^K$ be a triple partition corresponding to F, and let $\{a, b, c\}$ and $\{x, y, z\}$ be two distinct triples in $\mathcal{T}$. Since F has the triple summation property, then either $\{a + x, b + y, c + z\}$ or $\{a + x, b + z, c + y\}$ must also be a triple in $\mathcal{T}$. We will treat the case when $\{a + x, b + y, c + z\} \in \mathcal{T}$; the other case is handled analogically. Again, since F has the triple summation property, one of $\{a+y, b+z, c+x\}$ or $\{a+y, b+x, c+z\}$ must be a triple in $\mathcal{T}$. But if both $\{a+x, b+y, c+z\}$ and $\{a+y, b+x, c+z\}$ are in $\mathcal{T}$, then they have the element $c+z$ in common, and so $\{a+x, b+y, c+z\} = \{a+y, b+x, c+z\}$ since all distinct triples in $\mathcal{T}$ must be disjoint. If $a+x = a+y$, we get $x = y$ which contradicts $\{x, y, z\} \in \mathcal{T}$; and if $a+x = b+x$, we get $a = b$, which contradicts $\{a, b, c\} \in \mathcal{T}$. So we must have that $\{a + x, b + y, c + z\}$ and $\{a + y, b + z, c + x\}$ are triples

in $\mathcal{T}$. If these two triples are not distinct, then we must have one of $a+x=a+y$, or $a+x=b+z$, or $a+x=c+x$. The first and third case imply $x=y$ and $a=c$, respectively, and give an immediate contradiction; so we must have $a+b+x+z=0$. In this case, however, the sumsets of $\{a,b,c\}$ and $\{x,y,z\}$ are not distinct, which contradicts the hypothesis. The triples $\{a+x,b+y,c+z\}$ and $\{a+y,b+z,c+x\}$ must therefore be distinct. Applying the triple summation property, we see that one of $\{x+y,y+z,x+z\}$ and $\{x+y,b+c,b+c+x+y\}$ must be in $\mathcal{T}$. In the first case, we see that the sumsets of $\{x+y,y+z,x+z\}$ and $\{x,y,z\}$ coincide, and so we must have $\{x,y,z\}=\{x+y,y+z,x+z\}$ which implies $x+y+z=0$. In the second case, the sumset of $\{x+y,b+c,b+c+x+y\}$ intersects those of $\{x,y,z\}$ and $\{a,b,c\}$, which cannot happen since we assume that $\{x,y,z\}$ and $\{a,b,c\}$ are distinct. We have thus shown that for any two distinct triples $\{x,y,z\}$ and $\{a,b,c\}$ in $\mathcal{T}$, we must have $x+y+z=0$. Since this is true for any two distinct triples, we can conclude that F has the zero-sum property as claimed (the only case not handled by the above argument is when $\mathcal{T}$ contains a single triple, which is the case for $n=2$; but then $\mathcal{T}$ contains all non-zero elements of $\mathbb{F}_{2^2}$, and so it has the zero-sum property in this case as well). □

We thus know that any canonical 3-to-1 function has the triple summation property, the zero-sum property, and disjoint sumsets; any 3-to-1 function with the triplicate summation property and disjoint sumsets has the zero-sum property; and any 3-to-1 APN function has disjoint sumsets. We leave open the question of whether these inclusions are strict. Since according to our computational data, all known quadratic 3-to-1 (and hence APN) functions do have the triple summation property, we can formulate the following stronger conjecture. Since any quadratic 3-to-1 function is APN by Theorem 1, we can see by Proposition 1 that Conjecture 2 implies Conjecture 1.

Conjecture 2. Any quadratic 3-to-1 APN function has the triple summation property.

We remark that Theorems 1 and 2 apply to any plateaued (and, in particular, quadratic) 3-to-1 function, regardless of whether it has any of the above properties or not.

As pointed out above, a triplicate function can be constructed by arbitrarily partitioning the non-zero elements of $\mathbb{F}_{2^n}^*$ into triples, and assigning each triple an arbitrary output value; the polynomial form of such a function can then be recovered by e.g. Lagrange interpolation. Since we are mostly interested in constructing APN functions, a natural question would be whether APN-ness might impose some additional restrictions on the way that $\mathbb{F}_{2^n}^*$ is partitioned into triples. As already discussed, the triple partition $\mathcal{T}$ corresponding to an APN 3-to-1 function must have disjoint sumsets; and since the sumsets of $\mathcal{T}$ form a triple partition themselves, this means that any element of $\mathbb{F}_{2^n}^*$ has a unique expression as the sum of two elements belonging to the same triple of $\mathcal{T}$. Since this is an important structural property of 3-to-1 APN functions, we state it as an observation.

Observation 1. Let $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ with $F(0)=0$ be a 3-to-1 APN function for some even natural number n, and let $\mathcal{T}=\{T_i\}_{i=1}^K$ be a triple partition of $\mathbb{F}_{2^n}$ corresponding to F. Then the sumsets $2T_i$ for $i=1,2,\ldots,K$ partition $\mathbb{F}_{2^n}^*$ as well. Furthermore, the sum of each sumset $2T_i$ is equal to 0 (in fact, this is true for any sumset), and so $\{2T_i\}_{i=1}^K$ is a triple partition with the zero-sum property; furthermore, $\{0\}\cup 2T_i$ is a linear plane for $i=1,2,\ldots,K$.

Equivalently, any element $v\in\mathbb{F}_{2^n}^*$ can be uniquely expressed as a sum of two elements from the same triple T_i; that is, for every $v\in\mathbb{F}_{2^n}^*$, there exists a unique index $i\in\{1,2,\ldots,K\}$ such that $a_i+b_i=v$, or $a_i+c_i=v$, or b_i+c_i; and precisely one of these possibilities occurs.

We note that partitioning $\mathbb{F}_{2^n}$ into disjoint two-dimensional linear subspaces is not a trivial problem[6]. A natural idea for constructing such partitions would be to start with all non-zero elements of $\mathbb{F}_{2^n}^*$ and keep removing triples $\{a,b,a+b\}$ of elements from them, until no further elements remain. That is, we would keep track of a set S of elements that remain to be partitioned (initially, we would have $S=\mathbb{F}_{2^n}^*$); and in each step, we would take a pair of distinct elements $a,b\in S$ with $a+b\in S$ at random, and remove $\{a,b,a+b\}$ from S. Using this approach is likely to lead to a "dead end", in the sense that we reach a point where $a+b\notin S$ for any $a,b\in S$. A potentially interesting problem for future work would be to obtain necessary or sufficient conditions allowing us to construct such partitions of $\mathbb{F}_{2^n}$ efficiently; this would then facilitate the search for 3-to-1 APN functions.

Remark 1. We note that Observation 1 allows for a simple direct proof of Theorem 1 in the case of quadratic functions (the proofs in [26] and [44] being consequences of more complex, general statements). For the sake of making the present paper as self-contained as possible, and since the proof in terms of Observation 1 serves as a good illustration of some of the structural properties of triplicate functions, we describe it below.

Let $\mathcal{T}=\{T_i\}_{i=1}^K$ be a triple partition corresponding to F, with $T_i=\{a_i,b_i,c_i\}$ for $i=1,2,\ldots,K$. First, we show that any APN triplicate function F over $\mathbb{F}_{2^n}$ is 3-to-1. Suppose that F is not 3-to-1. Then we must have some $1\le i<j\le K$ such that $F(a_i)=F(a_j)$. Let $w=a_i+a_j$ and find two elements $x,y\in\mathbb{F}_{2^n}^*$ such that $x,y\in T_k$ for some k and $x+y=w$ (which exist and are uniquely defined by Observation 1). Then $D_wF(x)=D_wF(a_i)$. In order for F to be APN, we must have $\{x,y\}=\{a_i,a_j\}$. But if $x=a_i$, then $w=a_i+a_j=x+a_j=x+y$ so $y=a_j$, which cannot be because x and y should belong to the same triple. A similar contradiction follows if $y=a_i$.

[6]When we refer to two linear subspace S_1 and S_2 as "disjoint", we mean that $S_1\cap S_2=\{0\}$, i.e. that they have a trivial intersection.

We now show the converse implication in the case of quadratic functions. Suppose F is a quadratic 3-to-1 function (and, in particular, a triplicate function). Note that every differential set H_aF contains 0 since for any $a \in \mathbb{F}_{2^n}^*$ we can find a triple T_i such that $a \in 2T_i$ by Observation 1. If F is not APN, then the equation $D_aF(x) = 0$ must have at least four solutions for some $a \in \mathbb{F}_{2^n}^*$ since F is quadratic and hence D_aF is affine. Thus, we have four distinct elements $x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^n}$ with $F(x_1) = F(x_2)$, $F(x_3) = F(x_4)$, and $x_1 + x_2 = x_3 + x_4$. Now, if x_1 and x_2 belong to the same triple, then x_3 and x_4 must belong to different triples since $a = x_1 + x_2 = x_3 + x_4$ and by Observation 1, any non-zero element $a \in \mathbb{F}_{2^n}^*$ can be expressed uniquely as a sum of two elements from the same triple. Thus, we necessarily have at least two elements belonging to different triples for which F maps to the same value, and hence F is not 3-to-1. □

An even simpler proof in the more general case of plateaued functions is possible using Theorem 2 of [22]. This proof relies on counting the number of pairs (a, b) for which $F(a) = F(b)$, and so we defer it until after Proposition 5, where we characterize 3-to-1 among triplicate functions as those having the minimum possible number of such pairs. We still consider the direct proof from Remark 1 to be of interest, as it demonstrates how the structure of the triples T_i can be used to prove some important properties of 3-to-1 and triplicate functions. While the proof using Proposition 5 is seemingly shorter, both its complexity and structure are "hidden" in Theorem 2 of [22].

B. Characterization by the Walsh transform

In this section, we show that an (n, m)-function F is triplicate if and only if all of its Walsh coefficients of the form $W_F(0, b)$ for $b \in \mathbb{F}_{2^n}$ are congruent to 1 modulo 3. One of the implications is quite simple; namely, it is easy to see that if F is a triplicate function, then its Walsh coefficients $W_F(0, b)$ are constant modulo 3 as shown in the following proposition.

Proposition 2. Suppose F is a triplicate (n, m)-function for some natural numbers m, n with n even. Then, for any $b \in \mathbb{F}_{2^m}$, we have

$$3 \mid W_F(0, b) - 1. \tag{4}$$

Proof. The Walsh coefficient $W_F(0, b)$ is

$$W_F(0, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{b \cdot F(x)} = (-1)^{b \cdot F(0)} + \sum_{0 \neq x \in \mathbb{F}_{2^n}} (-1)^{b \cdot F(x)}.$$

Since the non-zero elements of $\mathbb{F}_{2^n}$ form triples $\{a_i, b_i, c_i\}$ for $i = 1, 2, \ldots, K = (2^n - 1)/3$ that map to the same value, the above becomes

$$W_F(0, b) = (-1)^{b \cdot F(0)} + 3 \sum_{i=1}^{K} (-1)^{b \cdot F(a_i)},$$

and since $F(0) = 0$ by the definition of a triplicate function, the claim follows immediately. □

We thus have the following immediate corollary.

Corollary 1. All components of a triplicate function are unbalanced.

We note that the property of all components being unbalanced can be rather useful when studying certain properties of functions; in particular, plateaued functions with all components unbalanced have rather nice characterizations that do not hold for the general case of plateaued functions [22].

We now prove the converse statement to Proposition 2 for (n, m)-functions. The proof proceeds by induction on m; we first prove the base case, i.e. we show that any Boolean triplicate $(n, 1)$-function f has Walsh coefficients that satisfy the divisibility property (4).

Proposition 3. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a Boolean function with $f(0) = 0$ for some even natural number n. Suppose that

$$3 \mid W_f(0) - 1.$$

Then f is a triplicate function.

Proof. Let $Z_f = \{x \in \mathbb{F}_{2^n} : x \neq 0, f(x) = 0\}$ and $O_f = \{x \in \mathbb{F}_{2^n} : f(x) = 1\}$ be the pre-images of 0 and 1, respectively, under f. Then f is triplicate if and only if $\#Z_f$ and $\#O_f$ are both multiples of 3. Since n must be even, we have $3 \mid 2^n - 1$, and since $\#Z_f + \#O_f = 2^n - 1$, it is enough to show that $3 \mid \#Z_f$. By definition, the Walsh coefficient $W_f(0)$ is

$$W_f(0) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = (-1)^{f(0)} + \sum_{0 \neq x \in \mathbb{F}_{2^n}} (-1)^{f(x)} = 1 + \#Z_f - \#O_f.$$

Since $\#O_f = 2^n - 1 - \#Z_f$, the above becomes

$$W_f(0) = 2\#Z_f - (2^n - 1) + 1.$$

By assumption, $3 \mid W_f(0)-1$, and so $3 \mid 2\#Z_f-(2^n-1)$. Since 2^n-1 itself is a multiple of three, this implies that $3 \mid \#Z_f$, and thus f is a triplicate function. □

The following proposition then described the induction step, and allows us to show, in particular, that any (n,n)-triplicate function has the divisibility property (4).

Proposition 4. Let F be an (n,m)-function with $F(0)=0$ for some natural numbers n,m such that n is even and

$$3 \mid W_F(0,b)-1$$

for all $b \in \mathbb{F}_{2^n}$. Then F is a triplicate function.

Proof. From the previous proposition, we know that all component functions of F are triplicate functions. We prove the statement by induction on m. If $m=1$, there is nothing to prove. If $m=2$, let A, resp. B, resp. C, resp. D denote the number of pre-images among $\mathbb{F}_{2^n}^*$ of 00, resp. 01, resp. 10, resp. 11 (note that here we make use of the vector space representation, and consider the elements of $\mathbb{F}_2^m=\mathbb{F}_2^2$ as pairs of binary values). Since 00 and 01 exhaust all possible outputs where the first coordinate is zero, and since the first coordinate function is a triplicate function, we must have $3 \mid A+B$. Similarly, we have $3 \mid A+C$, and hence $3 \mid B-C$. On the other hand, 01 and 10 exhaust all possibilities where the sum of the two coordinate functions is equal to 1, and since all component functions are triplicates, we also have $3 \mid B+C$. From this and $3 \mid B-C$ we get $3 \mid B$ and $3 \mid C$. But since $3 \mid A+C$, this implies $3 \mid A$; it is then easy to obtain also $3 \mid D$, so that we have $3 \mid A,B,C,D$.

Now suppose that the statement holds for all dimensions of the co-domain up to m; we will show that it also holds for $m+2$. Let A, resp. B, resp. C, resp. D denote the number of pre-images among $\mathbb{F}_{2^n}^*$ of all elements of the form $00\bar{x}$, resp. $01\bar{x}$, resp. $10\bar{x}$, resp. $11\bar{x}$, for some fixed m-bit vector $\bar{x} \in \mathbb{F}_2^m$. Let G be the $(n,m+1)$-function obtained from F by restricting its output to the last $m+1$ coordinates; that is, if $F=(f_1,f_2,\ldots,f_{m+2})$, then let $G=(f_2,f_3,\ldots,f_{m+2})$. By the induction hypothesis, G is a triplicate function. Since $A+C$ is the number of all elements of $\mathbb{F}_{2^n}^*$ whose last $m+1$ coordinates are of the form $0\bar{x}$, this implies that $3 \mid A+C$; in the same way, $3 \mid B+D$. By restricting F to all coordinates except f_2, we also obtain $3 \mid A+B$ and $3 \mid C+D$ in the same way. From $3 \mid A+B$ and $3 \mid A+C$, we have $3 \mid B-C$. Consider now the function G' obtained from F by summing its first two coordinates, i.e. $G'=(f_1+f_2,f_3,f_4,\ldots,f_{m+2})$. By the induction hypothesis, G' is a triplicate function, and so the number of pre-images of $1\bar{x}$ under G' is a multiple of 3. But this number of pre-images is precisely $B+C$, and so $3 \mid B+C$. Combining this with $3 \mid B-C$, we have $3 \mid 2B$ and hence $3 \mid B$. It is then easy to get $3 \mid A$, $3 \mid C$, and $3 \mid D$ as well. If the same argument is repeated for all possible $\bar{x} \in \mathbb{F}_{2^m}$, we see that the number of pre-images of any element in $\mathbb{F}_{2^{m+2}}$ is a multiple of three, and thus F is a triplicate function. □

We thus obtain the following characterization of triplicate functions.

Theorem 3. Let F be an (n,m)-function with $F(0)=0$ for some natural numbers n and m with n even. Then F is a triplicate function if and only if

$$W_F(0,b) \equiv 1 \pmod 3$$

for every $b \in \mathbb{F}_{2^n}$.

C. Characterization of 3-to-1 among triplicate functions

Since a triplicate function F always maps all elements from a triple $T_i=\{a_i,b_i,c_i\} \in \mathcal{T}$ to the same value, for every i, we have six pairs (a_i,b_i), (a_i,c_i), (b_i,a_i), (b_i,c_i), (c_i,a_i), and (c_i,b_i) that map to the same value under F. Since we have $K=(2^n-1)/3$ triples T_i, there are at least $6K+2^n$ ordered pairs $(x,y) \in \mathbb{F}_{2^n}^2$ that map to the same value (the term 2^n coming from pairs of the form (x,x) for $x \in \mathbb{F}_{2^n}$). As shown in the following proposition, 3-to-1 triplicate functions are precisely those triplicate functions that attain this lower bound with equality; we justify this by observing that if we take some triplicate function F with triples T_i and T_j with $F(T_i) \neq F(T_j)$ and modify it by "merging" the output values on T_i and T_j (so that we obtain a function G with $G(T_i)=G(T_j)$ and $G(T_k)=F(T_k)$ for $k \neq i,j$), the number of pairs (x,y) for which $F(x)=F(y)$ can only increase.

Proposition 5. Let F be a triplicate (n,n)-function for some even natural number n, and let $D_F=\{(x,y): x,y \in \mathbb{F}_{2^n}, F(x)=F(y)\}$ be the set of pairs of (not necessarily distinct) elements of $\mathbb{F}_{2^n}$ that map to the same value under F. Then

$$\#D_F \geq 2^{n+1}+2^n-2.$$

Furthermore, equality occurs if and only if F is a 3-to-1 function.

Proof. Let $K=(2^n-1)/3$ be the number of distinct triples as before. Since $F(0)=0$ for any triplicate function F, in the following we will consider only the values of F on $\mathbb{F}_{2^n}^*$ when discussing its image set. We know that a triplicate (n,n)-function can have at most K distinct elements in its image set (which may also include 0 if $F(a)=0$ for some $a \in \mathbb{F}_{2^n}^*$). Let us consider all triplicate functions whose image set is a subset of some set of elements $\{y_1,y_2,\ldots,y_K\}$. We are interested in how many triples T_i map to each y_j for $j=1,2,\ldots,K$. In order to express this formally, we introduce the notion of a

configuration of triples. More precisely, we call any ordered K-tuple $(k_1, k_2, \ldots, k_K)$ of natural numbers with $k_i \geq 0$ such that $\sum_{i=1}^{K} k_i = K$ a *configuration of triples*. The intuition is that k_i counts the number of triples that map to y_i. If F is 3-to-1, we have $k_i = 1$ for all $1 \leq i \leq K$. Observe that any configuration of triples can be obtained from $(1, 1, \ldots, 1)$ by an iterative sequence of steps in which we "transfer" some elements from k_i to k_j; more formally, such a step consists of taking some natural number $\Delta \leq k_i$, and defining a new configuration $(k'_i)_i$ of triples in which $k'_i = k_i - \Delta$, $k'_j = k_j + \Delta$, and $k'_l = k_l$ for all $l \neq i, j$. Furthermore, we can observe that any configuration of triples can be obtained from $(1, 1, \ldots, 1)$ by always "transferring" elements from k_i to k_j such that $k_i \leq k_j$. It is thus sufficient to show that such an operation never decreases the number of pairs in D_F. Furthermore, we can assume $\Delta = 1$, since for larger values of Δ the transfer can be decomposed into several steps with $\Delta = 1$ for each step.

Suppose $(k_i)_i$ is some configuration of triples in which $k_i = A$ and $k_j = B$. If we have a new configuration of triples $(k'_i)_i$ as above with $k'_i = A - 1$, $k'_j = B + 1$, and $k'_l = k_l$ for all $l \neq i, j$, the number of unordered pairs $\{x, y\}$ for which $F(x) = F(y)$ with respect to $(k'_i)_i$ increases by

$$\begin{aligned}
&\binom{3A-3}{2} + \binom{3B+3}{2} - \binom{3A}{2} - \binom{3B}{2} \\
&= \frac{(3A-3)(3A-4) + (3B+3)(3B+2) - 3A(3A-1) - 3B(3B-1)}{2} = \\
&= 9(B - A + 1)
\end{aligned}$$

as compared to the number of such pairs with respect to $(k_i)_i$. When $A \leq B$, this always leads to a positive increase in the number of pairs since $B - A + 1 > 0$, and thus the uniform configuration of triples $(1, 1, \ldots, 1)$ corresponds to the minimum number of such pairs. □

Remark 2. The above result immediately suggests a comparison with a known characterization of APN functions among plateaued functions. We know from Theorem 6 in [22] that any plateaued (n, n)-function having all of its component functions unbalanced satisfies

$$\#\{(a, b) \in \mathbb{F}_{2^n}^2 : F(a) = F(b)\} \geq 2^{n+1} + 2^n - 2,$$

with equality if and only if F is APN. Recall from Corollary 1 that the component functions of any triplicate functions are necessarily unbalanced. Note that this is almost the same characterization as the one that we have in Proposition 5; in fact, the two characterizations coincide in the case of plateaued (and, in particular, quadratic) functions. Despite this apparent similarity, the two characterizations concern different cases: Theorem 6 in [22] applies to any plateaued function (regardless of whether it is triplicate or not), while Proposition 5 addresses the case of any triplicate function (regardless of whether it is plateaued or not). Furthermore, we know examples of triplicate APN functions that are not plateaued (for instance, the Dobbertin power function over $\mathbb{F}_{2^n}$ for even n), and so the two characterizations do not coincide even in the APN case. In this sense, it is remarkable that 3-to-1 and triplicate functions behave in the same way as APN and plateaued ones with respect to the size of D_F.

Remark 3. As mentioned immediately after Remark 1, we can now combine Corollary 1 (stating that all components of a triplicate function are unbalanced) with Proposition 5 and Theorem 2 of [22] to obtain a very short proof of Theorem 1. Theorem 2 from [22] states that any (n, m)-function F is plateaued with component functions all unbalanced if and only if

$$\#\{(a, b) \in \mathbb{F}_{2^n}^2 : D_a D_b F(x) = v\} = \#\{(a, b) \in \mathbb{F}_{2^n}^2 : F(a) + F(b) = v\} \tag{5}$$

for any $v \in \mathbb{F}_{2^m}$ (for our purposes, of course, we assume that $n = m$). Taking $v = 0$, we can see that F is APN if and only if $D_a D_b F(x) = 0$ only when $a = 0$, $b = 0$, or $a = b$. In total, this amounts to $3 \cdot 2^n - 2$ pairs (a, b). From Proposition 5, we see that the quantity on the right-hand side of (5) is equal to $3 \cdot 2^n - 2$ if and only if F is 3-to-1. The claim follows immediately.

Since the number of elements that map to the same image can be expressed using the second powers of Walsh coefficients of the form $W_F(0, b)$, the characterization from Proposition 5 can be equivalently expressed in terms of the Walsh transform as follows.

Corollary 2. Let F be a triplicate (n, n)-function for some even natural number n. We have

$$\sum_{b \in \mathbb{F}_{2^n}} W_F^2(0, b) \geq 2^{2n+1} + 2^{2n} - 2^{n+1},$$

with equality if and only if F is 3-to-1.

Proof. We have

$$\sum_{b \in \mathbb{F}_{2^n}} W_F^2(0, b) = \sum_{b, x, y \in \mathbb{F}_{2^n}} \chi_b(F(x) + F(y)) = 2^n \#\{(x, y) \in \mathbb{F}_{2^n}^2 : F(x) = F(y)\}.$$

As observed in Proposition 5, the number of ordered pairs (x, y) with $F(x) = F(y)$ is always at least $2^{n+1} + 2^n - 2$, and equality occurs if and only if F is 3-to-1. It then suffices to substitute this number in the above expression. □

In fact, in the case when F is 3-to-1, we can explicitly evaluate the power moment $\sum_{b\in\mathbb{F}_{2^n}} W_F^2(a, b)$ for any $a \in \mathbb{F}_{2^n}^*$ as well; it can only take two possible values, one of which is attained for $a = 0$, and the other is attained for any $a \in \mathbb{F}_{2^n}^*$. This is another remarkable property of triplicate functions, as the values of these power moments can greatly vary in general (even in the case of quadratic APN functions).

Proposition 6. Let F be a 3-to-1 (and hence triplicate) (n, n)-function for some even positive natural number n. Then:

$$\sum_{b\in\mathbb{F}_{2^n}} W_F^2(a, b) = \begin{cases} 2^{2n+1} + 2^{2n} - 2^{n+1} & a = 0 \\ 2^n(2^n - 2) & a \neq 0. \end{cases} \tag{6}$$

Proof. The case for $a = 0$ is contained in the statement of Corollary 2. For any fixed $0 \neq a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}
\sum_{b\in\mathbb{F}_{2^n}} W_F^2(a, b) &= \sum_{b,x,y\in\mathbb{F}_{2^n}} \chi_b(F(x) + F(y))\chi_a(x + y) \\
&= \sum_{x,y\in\mathbb{F}_{2^n}} \chi_a(x + y) \sum_{b\in\mathbb{F}_{2^n}} \chi_b(F(x) + F(y)) \\
&= 2^n \sum_{x\in\mathbb{F}_{2^n}} \sum_{\substack{y\in\mathbb{F}_{2^n} \\ F(x)=F(y)}} \chi_a(x + y) \\
&= 2^n[1 + \sum_{0\neq x\in\mathbb{F}_{2^n}} \sum_{y\in F^{-1}(x)} \chi_a(x + y)] \\
&= 2^n[1 + \sum_{0\neq x\in\mathbb{F}_{2^n}} \chi_a(x + x) + \chi_a(x + y_x) + \chi_a(x + z_x)] \\
&= 2^n[1 + \sum_{0\neq x\in\mathbb{F}_{2^n}} \chi_a(0) + \chi_a(x + y_x) + \chi_a(x + z_x)],
\end{aligned}$$

where y_x and z_x are the two elements forming a triple $T_i = \{x, y_x, z_x\}$ for some $1 \leq i \leq K$ and $x \in \mathbb{F}_{2^n}$. Note that as x runs through all non-zero values $x \in \mathbb{F}_{2^n}^*$, then so do $x + y_x$ and $x + z_x$; and so the above becomes

$$\begin{aligned}
\sum_{b\in\mathbb{F}_{2^n}} W_F^2(a, b) &= 2^n[1 + 2^n - 1 + 2 \sum_{0\neq x\in\mathbb{F}_{2^n}} \chi_a(x)] \\
&= 2^n[2^n - 2] = 2^{2n} - 2^{n+1}
\end{aligned}$$

as claimed. □

Recall from [26] that an (n, n)-function F is called **zero-difference δ-balanced** if the equation $D_aF(x) = 0$ has precisely δ solutions for every $a \in \mathbb{F}_{2^n}^*$. Proposition 5 in [26] (when specialized to the case of $\delta = 2$ and characteristic 2) states that a function F satisfies (6) if and only if F is zero-difference 2-balanced. It has already been observed in [26] that what we call canonical triplicates are zero-difference 2-balanced when they are 3-to-1. Proposition 6 allows us to generalize this to the case of triplicate functions that are not necessarily canonical. We thus have the following corollary.

Corollary 3. Any 3-to-1 function is zero-difference 2-balanced.

Remark 4. For comparison, the quadratic APN $(6, 6)$-function $\alpha^{25}x^5 + x^9 + \alpha^{38}x^{12} + \alpha^{25}x^{18} + \alpha^{25}x^{36}$ can take 9 distinct values of the power moment $\sum_b W_F^2(a, b)$ depending on the value of a.

D. The image of a quadratic 3-to-1 function as a partial difference set

An important result of [26] is that the image set of any quadratic canonical 3-to-1 function is a partial difference set with prescribed parameters. This is a fascinating structural result having fundamental implications about the properties and behavior of such functions. In this section, we generalize this result to the case of any quadratic 3-to-1 function, and investigate some of its consequences.

We recall that a **partial difference set** of an additive group G with parameters (v, k, λ, μ) is a set $D \subseteq G$ with $\#D = k$ such that every non-identity element in D can be represented as $g - h$ for $g, h \in D, g \neq h$ in exactly λ ways; and each non-identity element in $G \setminus D$ can be represented as $g - h$ for $g, h \in D, g \neq h$ in exactly μ different ways.

In order to prove Theorem 4, we will need the following lemma from [46], which was also used in [26] in the proof of Theorem 2 (whose specialization to the case of 3-to-1 functions over fields of even characteristic is essentially the special case of the following Theorem 4 for canonical triplicate 3-to-1 functions).

Lemma 1. [46] Let $\mathcal{G}$ be a group and D be a set of elements in $\mathcal{G}$ with $|D| = k$. Then, if $D = -D$, then D is a (v, k, λ, μ) partial difference set if and only if, for any nonprincipal character χ of $\mathcal{G}$ we have

$$\chi(D) = \sum_{d \in D} \chi(d) = \frac{(\lambda - \mu) \pm \sqrt{(\mu - \lambda)^2 - 4(\mu - k)}}{2}. \tag{7}$$

Since we know that any quadratic 3-to-1 function has a Gold-like Walsh spectrum by Theorem 2, and also that any such function has all components unbalanced by Theorem 3 and that every differential set is a linear (as opposed to merely affine) hyperplane, we can now obtain the following.

Theorem 4. Let F be a 3-to-1 crooked (n, n)-function for some natural number $n = 2k$. Then the set of non-zero elements $D = \mathrm{Im}(F) \setminus \{0\}$ in its image set is a $(2^n, (2^n - 1)/3, \lambda, \mu)$ partial difference set, where

$$(\lambda, \mu) = ((2^k + 4)(2^k - 2)/9, (2^k + 1)(2^k - 2)/9)$$

if k is odd, and

$$(\lambda, \mu) = ((2^k - 4)(2^k + 2)/9, (2^k - 1)(2^k + 2)/9)$$

if k is even.

Proof. By Lemma 1, it is enough to show that $\chi_a(D)$ takes the value on the right-hand side of (7) for any $a \in \mathbb{F}_{2^n}^*$. Observe that

$$\chi_a(D) = \sum_{d \in D} \chi_a(D) = \frac{1}{3} \sum_{x \in \mathbb{F}_{2^n}^*} \chi_a(F(x)) = \frac{1}{3} \left(W_F(0, a) - 1 \right) \tag{8}$$

since we know that F is 3-to-1. Thus, verifying that the hypothesis of Lemma 1 holds amounts to computing the values of $W_F(0, a)$ for all $a \in \mathbb{F}_{2^n}^*$. Since F is crooked and hence plateaued, we know that $W_F(0, a) \in \{0, \pm\lambda_a\}$, where λ_a is the amplitude of F_a. On the other hand, we know that $W_F(0, a)$ is not zero by Theorem 3. From Theorem 2, we know that F has a Gold-like Walsh spectrum, and so $\lambda_a \in \{2^{n/2}, 2^{n/2+1}\}$ for any $a \in \mathbb{F}_{2^n}^*$. In order to finish the proof, it only remains to compute the value on the right-hand side of (7) and to compare it with the two amplitudes. We treat the cases of k odd and k even separately. When k is odd, we have

$$\lambda - \mu = \frac{(2^k + 4)(2^k - 2) - (2^k + 1)(2^k - 2)}{9} = \frac{2^k - 2}{3};$$

$$\mu - k = \frac{(2^k + 1)(2^k - 2)}{9} - \frac{2^{2k} - 1}{3} = \frac{(2^k + 1)(2^k - 2) - 3(2^k + 1)(2^k - 1)}{9} = \frac{(2^k + 1)(2^k - 2 - 3 \cdot 2^k + 3)}{9} = \frac{(2^k + 1)(1 - 2^{k+1})}{9};$$

$$(\mu - \lambda)^2 - 4(\mu - k) = \frac{(2^k - 2)^2 - 4(2^k + 1)(1 - 2^{k+1})}{9} = \frac{2^{2k} - 2^{k+2} + 4 - 4(2^k - 2^{2k+1} + 1 - 2^{k+1})}{9} = \frac{2^{2k} - 2^{k+2} + 4 - 4(1 - 2^k - 2^{2k+1})}{9} = \frac{2^{2k} - 2^{k+2} + 4 - 4 + 2^{k+2} + 2^{2k+3}}{9} = \frac{9 \cdot 2^{2k}}{9} = 2^{2k}.$$

Finally, the right-hand side of (7) becomes

$$\frac{(2^k - 2)/3 \pm 2^k}{2} = \frac{2^k - 2 \pm 3 \cdot 2^k}{6} = \begin{cases} (2^{k+2} - 2)/6 \\ (-2^{k+1} - 2)/6. \end{cases}$$

When k is even, we have

$$\lambda - \mu = \frac{(2^k - 4)(2^k + 2) - (2^k - 1)(2^k + 2)}{9} = \frac{(2^k + 2)(-3)}{9} = \frac{-2^k - 2}{3};$$

$$\mu - k = \frac{(2^k - 1)(2^k + 2)}{9} - \frac{2^{2k} - 1}{3} = \frac{(2^k - 1)(2^k + 2) - 3(2^k - 1)(2^k + 1)}{9} = \frac{(2^k - 1)(2^{k+2} - 3 \cdot 2^k - 3)}{9} = \frac{(2^k - 1)(-1 - 2^{k+1})}{9};$$

$$(\mu - \lambda)^2 - 4(\mu - k) = \frac{(2^k + 2)^2}{9} + \frac{4(2^k - 1)(2^{k+1} + 1)}{9} = \frac{2^{2k} + 2^{k+2} + 4 + 4(2^{2k+1} + 2^k - 2^{k+1} - 1)}{9} = \frac{2^{2k} + 2^{k+2} + +4(2^{2k+1} - 2^k - 1)}{9} = \frac{2^{2k} + 2^{k+2} + 4 + 2^{2k+3} - 2^{k+2} - 4}{9} = \frac{9 \cdot 2^{2k}}{9} = 2^{2k};$$

in this case, (7) becomes

$$\frac{(-2^k-2)/3 \pm 2^k}{2} = \frac{-2^k - 2 \pm 3 \cdot 2^k}{6} = \begin{cases} (-2^{k+2}-2)/6 \\ (2^{k+1}-2)/6. \end{cases}$$

By (8), the values that we obtain above should be multiplied by 3 and incremented by 1; they should then match the value of $W_F(0,a)$. The values become 2^{k+1} and -2^k for k odd, and -2^{k+1} and 2^k for k even. Comparing these with the ones from (3) from Theorem 2, we can see that the values coincide. Consequently, $D = \mathrm{Im}(F) \setminus \{0\}$ is a partial difference set with the prescribed parameters as claimed. □

From this, we can immediately get the following corollary, which counts the multiplicities of the elements in the multiset $M_F = [F(x) + F(x+y) + F(y) : x, y \in \mathbb{F}_{2^n}]$ for some given (n,n)-function F.

Note that the quantities given in Theorem 4 are given in terms of the number of non-zero elements of the image set of F that add up to a given value. The multiplicities in M_F will be larger, since F is a 3-to-1 function, and thus every non-zero value from its image set can be obtained in 3 different ways. This means that the quantities given in the theorem have to be multiplied by 9 (since, if $i_1 + i_2 = v$ for some $v \in \mathbb{F}_{2^n}$ and $i_1, i_2 \in \mathrm{Im}(F)$, then i_1 and i_2 can both be obtained in 3 different ways). Furthermore, the quantities in Theorem 4 only account for combinations involving non-zero elements of $\mathrm{Im}(F)$. If $i_1 + i_2 = v$ with e.g. $i_1 = 0$, then v must be in the image set of F itself; and there are three ways to do this. The same happens if $i_2 = 0$, and so when computing the multiplicities of elements in M_F belonging to the image of F, we have to add 6.

Corollary 4. Let F be a quadratic 3-to-1 function over $\mathbb{F}_{2^n}$ for some natural number $n = 2k$. Then all non-zero elements of $M_F = [F(x) + F(y) + F(x+y) : x, y \in \mathbb{F}_{2^n}]$ have multiplicity in M_F either

$$(2^k+4)(2^k-2)+6 \text{ or } (2^k+1)(2^k-2)$$

when k is odd, or

$$(2^k-4)(2^k+2)+6 \text{ or } (2^k-1)(2^k+2)$$

when k is even. In both the odd and the even case, the number of elements having these two multiplicities is precisely $(2^n-1)/3$ and $2(2^n-1)/3$, respectively; and the (2^n-1) elements having the first multiplicity are precisely the non-zero elements in the image set of F.

As a byproduct, Theorem 4 allows us to compute the multiset Π_F^0 for any generalized crooked (and, in particular, quadratic) 3-to-1 function F; in the case of quadratic F, we can also compute the exact form of the multiset Π_F. These multisets are defined in [11], where it is shown that Π_F is invariant under CCZ-equivalence for APN functions; that is, if F and G are APN and CCZ-equivalent, then $\Pi_F = \Pi_G$. According to Corollary 2 of [11], the minimum value of Π_F gives a lower bound on the Hamming distance $d_H(F,G)$ between a given APN function F and any other APN function G; more precisely, we have $d_H(F,G) \geq \lceil m_F/3 \rceil + 1$, where $m_F = \min \Pi_F$. Furthermore, in the case when F is quadratic, it is shown that it is enough to compute the multiset

$$\Pi_F^0 = [\#\{a \in \mathbb{F}_{2^n} : b \in H_a^0 F\} : b \in \mathbb{F}_{2^n}],$$

which can then be used to immediately recover Π_F. If F is APN, it is easy to see that the number of derivative directions $a \in \mathbb{F}_{2^n}$ for which $b \in H_a^0 F$ for some $b \in \mathbb{F}_{2^n}^*$ is equal to half the number of pairs $(a,x) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $F(x) + F(a+x) + F(a) = b$. Clearly, this is the multiplicity of b in M_F. As we already have these multiplicities computed in Corollary 4, it is straightforward to combine this with Corollary 2 of [11] in order to obtain the following.

Corollary 5. Let F be a quadratic 3-to-1 function over $\mathbb{F}_{2^n}$ for some natural number $n = 2k$. Then

$$\Pi_F^0 = \begin{cases} \left[\underbrace{\frac{(2^k+1)(2^k-2)}{2}}_{\times(2^n-1)/3}, \underbrace{(2^k+4)(2^k-2)/2}_{\times 2(2^n-1)/3}, 2^n \right] & k \text{ odd} \\ \left[\underbrace{\frac{(2^k-4)(2^k+2)}{2}}_{\times(2^n-1)/3}, \underbrace{(2^k-1)(2^k+2)/2}_{\times 2(2^n-1)/3}, 2^n \right] & k \text{ even,} \end{cases}$$

where the multiplicities of the elements in the multiset are given in under-braces; consequently, for any APN function G over $\mathbb{F}_{2^n}$ distinct from F, we have

$$d_H(F,G) \geq \begin{cases} \frac{(2^k+1)(2^k-2)}{6} + 1 & k \text{ odd} \\ \frac{(2^k-4)(2^k+2)}{6} + 1 & k \text{ even.} \end{cases} \tag{9}$$

The same value was obtained in Proposition 6 of [11] for the particular case of the Gold function x^3. We have thus generalized this to any quadratic 3-to-1 triplicate function. As observed in [11], all instances from the known APN polynomial

(as opposed to monomial) families take the same, Gold-like value of Π_F (although Π_F can take thousands of distinct values across the known sporadic APN instances). The preceding discussion explains this phenomenon for the case of those families that contain 3-to-1 functions (or functions equivalent to 3-to-1 functions) among their instances; we refer to Section VI where we survey the functions from the known infinite APN families with respect to the property of their instances being triplicates.

Corollary 5 gives a lower bound on the distance between any quadratic 3-to-1 function T, and any other APN function. In particular, it gives a lower bound on the distance between any two quadratic 3-to-1 functions. We can apply the same approach as in [30] to obtain an upper bound on the number of quadratic 3-to-1 functions over $\mathbb{F}_{2^n}$ for any even natural number n. We can then see that the proportion of quadratic 3-to-1 functions over $\mathbb{F}_{2^n}$ goes to 0 as n approaches infinity; the same was shown for planar and AB functions in [30].

Corollary 6. Let n be an even natural number. Then the number of quadratic 3-to-1 functions over $\mathbb{F}_{2^n}$ is at most

$$\frac{(2^n)^{2^n}}{\sum_{j=0}^{d-1}\binom{2^n}{j}(2^n-1)^j},$$

where d is the value of the lower bound in (9) from Corollary 5. Consequently, the proportion of quadratic 3-to-1 functions over $\mathbb{F}_{2^n}$ to all (n,n)-functions converges to 0 as n approaches infinity.

Since the number of pairs (x,y) or triples $(x,y,x+y)$ satisfying $F(x)+F(y)=v$ or $F(x)+F(y)+F(x+y)=v$, respectively, can be expressed using the Walsh transform, we can obtain the following equivalent form of Theorem 4.

Corollary 7. Let F be a quadratic 3-to-1 (n,n)-function for some even natural number $n=2k$. Then

$$\frac{1}{2^{2n}}\sum_{a,b\in\mathbb{F}_{2^n}}\chi_b(v)W_F^3(a,b)=\frac{1}{2^n}\sum_{b\in\mathbb{F}_{2^n}}\chi_b(v)W_F^2(0,b)=\begin{cases}2^{n+1}+2^n-2 & v=0\\ (2^k+4)(2^k-2)+6 & v\in\mathrm{Im}(F)\setminus\{0\},k \text{ odd}\\ (2^k-4)(2^k+2)+6 & v\in\mathrm{Im}(F)\setminus\{0\},k \text{ even}\\ (2^k+1)(2^k-2) & v\notin\mathrm{Im}(F),k \text{ odd}\\ (2^k-1)(2^k+2) & v\notin\mathrm{Im}(F),k \text{ even.}\end{cases}$$

Expressions of this form can be quite difficult to compute, in general, and we expect that the above expressions might lead to even more insights about the structure of quadratic 3-to-1 functions in the future. We note that we formulate the above results strictly for quadratic 3-to-1 functions, and not for crooked functions as in some other cases; this is because we know that Π_F can be derived from the smaller multiset Π_F^0 only in the case of quadratic APN functions (Proposition 5 of [11]). The proof of this proposition uses the fact that the derivatives of a quadratic function are affine, and so it is not immediately clear whether this result can be generalized to crooked functions.

IV. Number of distinct differential sets

As we have seen above, 3-to-1 functions among the triplicate functions (and, in particular, APN functions among the quadratic triplicate functions) can be interpreted as extremal objects in the sense that they minimize the number of pairs $(x,y)\in\mathbb{F}_{2^n}^2$ such that $F(x)=F(y)$. We note that a tight upper bound on the number of such pairs for APN functions is given in Lemma 2 of [44]. As we know from [27] and [44], 3-to-1 APN functions also attain the smallest possible size of the image set among all APN functions over finite fields of even extension degree. In this section, we show that 3-to-1 functions are extremal objects in yet another sense. More precisely, we study the number of differential sets of canonical triplicate functions, and observe that 3-to-1 functions among the quadratic canonical triplicate functions can also be characterized in terms of having the largest possible number of distinct differential sets. In the course of comparing this with the behavior of APN functions in general, we compute the exact number of distinct differential sets of any APN power function (even over $\mathbb{F}_{2^n}$ for odd n); moreover, we show that for a power APN function F over $\mathbb{F}_{2^n}$, we have $H_aF=H_bF$ if and only if $F(a)=F(b)$ for any $a,b\in\mathbb{F}_{2^n}$.

In Subsection IV-A, we show that for any APN power function $F(x)=x^d$, we have $H_aF=H_bF$ if and only if $F(a)=F(b)$, and use this to compute the exact number of distinct differential sets of F. In Subsection IV-B, we do the same for the case of quadratic canonical triplicate functions, and observe that they act as a generalization of power APN functions over fields of even extension degree in this sense. We note that the directions $a\in\mathbb{F}_{2^n}$ for which H_aF is contained in a given hyperplane have been described for $F(x)=x^{2^i+1}$ (not necessarily APN) in [45], while in our analysis we assume that $F(x)=x^d$ is APN but do not make any additional assumptions about the exponent d.

A. Differential sets of APN power functions

Recall that 3-to-1 APN functions behave like the power APN functions in a number of ways, e.g. with respect to having an image set of size precisely $(2^n-1)/3+1$ elements in the case of even n. It is thus natural to begin our investigation by studying the behaviour of the differential sets of power functions. It is not difficult to see that if $F(x)=F(y)$ for some power function F, then the differential sets H_xF and H_yF coincide.

Proposition 7. Let $F(x) = x^l$ be a power function over $\mathbb{F}_{2^n}$. Let $a, b \in \mathbb{F}_{2^n}^*$ If $F(a) = F(b)$, then $H_aF = H_bF$.

Proof. The derivative of F is simply $D_aF(x) = x^l + (x+a)^l$, and for some given $v = D_aF(x)$, multiplying both sides by $(b/a)^l = 1$ yields $y^l + (y+b)^l = v$ with $y = (xb/a)$. □

What is more surprising is that the converse implication also holds; that is, if $H_aF = H_bF$ for some $a, b \in \mathbb{F}_{2^n}^*$, then $F(a) = F(b)$ for a power function F. Before proceeding to the proof, we need to make the following auxiliary observation.

Lemma 2. Let $F(x) = x^l$ be a power function over $\mathbb{F}_{2^n}$. Then, if $H_aF = H_bF$ for some $a, b \in \mathbb{F}_{2^n}^*$, the maps $x \mapsto (b/a)^l x$ and $x \mapsto (a/b)^l x$ are permutations of $\mathbb{F}_{2^n}$ that fix H_aF.

Proof. That e.g. $x \mapsto (b/a)^l x$ is a permutation of $\mathbb{F}_{2^n}$ is clear; furthermore, for any value $v \in H_aF$, i.e. for any

$$v = x^l + (a+x)^l$$

we have

$$(b/a)^l v = y^l + (b+y)^l$$

for $y = (bx/a)$ so that the image of v lies in $H_bF = H_aF$. Thus, $x \mapsto (b/a)^l x$ does indeed fix $H_bF = H_aF$. □

Then, to show that $H_aF = H_bF$ necessarily implies $F(a) = F(b)$, it suffices to prove that any element c defining a permutation $x \mapsto cx$ of $\mathbb{F}_{2^n}$ that fixes a given differential set must, in fact, be the neutral element of $\mathbb{F}_{2^n}^*$. To this end, we first characterize the cardinality of any set S that is left invariant under a map of the type $x \mapsto cx$.

Lemma 3. Let $c \in \mathbb{F}_{2^n}^*$ and define $\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ by $\varphi(x) = cx$. Furthermore, let $S \subseteq \mathbb{F}_{2^n}^*$ be a non-empty subset of $\mathbb{F}_{2^n}$ such that $\varphi(S) = S$, i.e. $\{\varphi(s) : s \in S\} = S$. Then the cardinality of S can be written in the form

$$\#S = \sum_{i=1}^{k} a_i \cdot g_i$$

for some positive natural number k, where the numbers g_i are the cardinalities of subgroups of $\mathbb{F}_{2^n}^*$ (i.e. divisors of $2^n - 1$) and a_i are natural numbers (that may be zero). Furthermore, the order of c must be a common divisor of the numbers g_i with $i = 1, 2, \ldots, k$ such that $a_i \neq 0$.

Proof. Pick some arbitrary element $s_1 \in S$; denote $s_2 = \varphi(s_1)$, $s_3 = \varphi(s_2)$, etc. After a finite number of such steps we must reach some element s_k with $\varphi(s_k) = s_1$. From the definition of φ this can be written simply as $c^k s_1 = s_1$; since by assumption $s_1 \neq 0$, this implies $c^k = 1$ so that the order of c must be a multiple of k.

Denote $R = \{s_1, s_2, \ldots, s_k\}$. If $R = S$, then we are done; otherwise, take $S' = S \setminus R$ and repeat the same procedure for S', observing that S' satisfies the hypothesis of the proposition as well since $\varphi(S) = S$ and $\varphi(R) = R$ immediately implies $\varphi(S \setminus R) = (S \setminus R)$.

To summarize, $\#S$ can indeed be be written as a sum of group orders, and c raised to the power of each such order must evaluate to 1; hence, the order of c must be a common divisor of all these numbers. □

We thus obtain the following corollary.

Corollary 8. Let F be an APN function over $\mathbb{F}_{2^n}$ and let $c \in \mathbb{F}_{2^n}^*$ be such that the permutation $\varphi(x) = cx$ fixes $S = H_aF$ for some $a \in \mathbb{F}_{2^n}^*$; then $c = 1$.

Proof. Suppose that F is APN and $S = H_aF$ for some $a \in \mathbb{F}_{2^n}^*$ so that $\#S = 2^{n-1}$. If $\varphi(S) = S$ for some $\varphi(x) = cx$ with $\#S = g_1 + g_2 + \cdots + g_l$ and, denoting $k = GCD(g_1, g_2, \ldots, g_k)$, we have $k \mid 2^{n-1}$ or $k \mid (2^{n-1} - 1)$ depending on whether $0 \in H_aF$ (the first case corresponds to $0 \notin H_aF$, while the second one corresponds to $0 \in H_aF$).

However, both cases are impossible for $k \neq 1$. Indeed, in the case $\#S = 2^{n-1}$ only powers of two may divide $\#S$, while $2^n - 1$ is an odd number and thus not divisible by two; in the case $\#S = 2^{n-1} - 1$, assuming $ak = 2^{n-1} - 1$ and $bk = 2^n - 1$ for some $a, b \in \mathbb{Z}$ leads to $(b-a)k = 2^{n-1}$ so that we once again get a contradiction if we assume $k \neq 1$ due to 2^{n-1} being divisible only by powers of two and the other two numbers involved being odd. Consequently, the order of any c such that $\varphi(x) = cx$ fixes H_aF must be 1, i.e. c must be the neutral element. □

From this and from Lemma 2 we obtain the desired result.

Theorem 5. Let F be an APN power function over $\mathbb{F}_{2^n}$. Then, for any $a, b \in \mathbb{F}_{2^n}^*$ we have

$$H_aF = H_bF \iff F(a) = F(b).$$

Proof. By Lemma 2, we have that if $H_aF = H_bF$, then $x \mapsto x(b/a)^l$ is a permutation that fixes $H_a = H_b$. By Corollary 8, we see that $(b/a)^l = 1$, and so $b^l = a^l$, i.e. $F(a) = F(b)$. The converse implication was already observed in Proposition 7. □

This then immediately allows us to compute the number of distinct differential sets of the power APN functions.

Corollary 9. Let F be a power APN function over $\mathbb{F}_{2^n}$. Then the number of distinct differential sets of F is equal to the cardinality of its image over $\mathbb{F}_{2^n}$, i.e.

$$\#\{H_aF : a \in \mathbb{F}_{2^n}\} = \#\{F(x) : x \in \mathbb{F}_{2^n}\}.$$

In particular, a power APN function has 2^n distinct differential sets when n is odd, and $(2^n-1)/3+1$ distinct differential sets when n is even.

Note that Theorem 5 applies to any power APN function, which must then necessarily be a canonical triplicate for an even dimension n; in particular, we do not assume anything about e.g. the algebraic degree. The condition that the power function is APN is, however, necessary: taking e.g. $F(x) = x^5$ over $\mathbb{F}_{2^8}$, we can see that F has an image set consisting of 52 elements, but only 18 distinct differential sets. In the general case of polynomials (as opposed to monomials), neither of the two implications $H_aF = H_bF \iff F(a) = F(b)$ holds (even for quadratic APN functions), and it is easy to find counterexamples among the known polynomial APN instances; for instance, the so-called Kim function $x^3 + x^{10} + \alpha x^{24}$ over $\mathbb{F}_{2^6}$ (where α is a primitive element of $\mathbb{F}_{2^6}$) serves as a simple counterexample to both implications.

B. Differential sets of canonical triplicate functions

We now proceed to the case of triplicate functions. In the case of a canonical triplicate (n,n)-function F, it is easy to observe that $H_aF = H_{\beta a}F = H_{\beta^2 a}F$ for any $a \in \mathbb{F}_{2^n}^*$; in this way, all elements belonging to a triple T_i not only map to the same output, but induce the same differential set as well. This is simply because for any $a, x \in \mathbb{F}_{2^n}$ we have

$$D_{\beta a}F(\beta x) = F(\beta x) + F(\beta(x+a)) = F(x) + F(a+x) = D_aF(x).$$

In the particular case when F is a quadratic APN function so that its ortho-derivative π_F is well-defined, this observation means that π_F is itself a canonical triplicate function.

Observation 2. If F is a canonical triplicate (n,n)-function for some even natural number n, then $H_aF = H_{\beta a}F = H_{\beta^2 a}F$ for any $a \in \mathbb{F}_{2^n}^*$. In particular, the ortho-derivative of a generalized crooked canonical triplicate function is a canonical triplicate function.

We thus know that a canonical triplicate function can have at most $(2^n-1)/3$ distinct non-trivial differential sets (by "non-trivial", we mean that we exclude the differential set $H_0F = \{0\}$). Since 3-to-1 triplicate functions are precisely those triplicate functions that maximize the size of the image set, one would intuitively expect that their differential sets might exhibit a similar behavior; that is, that 3-to-1 functions have precisely $(2^n-1)/3$ distinct non-trivial differential sets. In the following, we prove that this is indeed so for the case of quadratic canonical triplicates.

Recall that $[H_bF]$ is the set of all $a \in \mathbb{F}_{2^n}$ for which $H_aF = H_bF$. Recall also the symplectic form $(\Delta_aF)^*(x) = F(x)+F(a+x)+F(a)+F(0)$, which in our case becomes simply $(\Delta_aF)^*(x) = F(x)+F(a+x)+F(a)$ since any triplicate function F satisfies $F(0) = 0$ by definition.

Lemma 4. For any quadratic APN function F with $F(0) = 0$ and even n, we have

$$W_F^2(0,\beta) = 2^n(1 + \#[\mathcal{H}(\beta)]).$$

Proof. We have

$$\begin{aligned}
W_F^2(0,\beta) &= \sum_{x,a\in\mathbb{F}_{2^n}} \chi_\beta(F(x)+F(x+a)) = \sum_{x,a\in\mathbb{F}_{2^n}} \chi_\beta(F(x)+F(x+a)+F(a)+F(a)) \\
&= \sum_{x,a\in\mathbb{F}_{2^n}} \chi(\beta(\Delta_aF)^*(x)+\beta F(a)) = \sum_{x,a\in\mathbb{F}_{2^n}} \chi(\Delta_a^*F(\beta)x+\beta F(a)) \\
&= \sum_{a\in\mathbb{F}_{2^n}} \chi(\beta F(a)) \sum_x \chi_x(\Delta_a^*F(\beta)) \\
&= 2^n \sum_{a\in\mathbb{F}_{2^n}:\Delta_a^*F(\beta)=0} \chi(\beta F(a)),
\end{aligned}$$

where Δ_a^*F is the adjoint operator[7] of $(\Delta_aF)^*$. We thus need to find all roots of $\Delta_a^*F(\beta)$. Since $\mathrm{Ker}(L^*) = \mathrm{Im}(L)^\perp$ for any linear (n,n)-function L, we have that $\Delta_a^*F(\beta) = 0$ if and only if $H_aF = \mathcal{H}(\beta)$. The statement follows immediately, bearing in mind that 0 is a trivial root of Δ_a^*F. □

[7]The adjoint of a linear function L is the linear function L^* satisfying $\mathrm{Tr}(xL(y)) = \mathrm{Tr}(L^*(x)y)$ for any $x, y \in \mathbb{F}_{2^n}$.

We can now show that a canonical quadratic 3-to-1 function has precisely $(2^n-1)/3$ distinct non-trivial differential sets. We know that any generalized crooked function is also plateaued (see e.g. [23], p.278) which is a property that we need in the proof.

Theorem 6. Let F be a quadratic canonical 3-to-1 (n,n)-function. Then F has at most $(2^n-1)/3$ distinct non-trivial differential sets, with equality if and only if F is 3-to-1. In the latter case, the ortho-derivative π_F is a canonical triplicate 3-to-1 function as well.

Proof. From Observation 2, we already know that F has at most $(2^n-1)/3$ distinct non-trivial differential sets (in fact, this is true for any canonical triplicate function, regardless of whether it is crooked or not). We now show that, in the crooked case, if F is 3-to-1, then all of the $(2^n-1)/3$ differential sets corresponding to distinct triples T_i are distinct. Since F is crooked, we know that it is plateaued [23]; let λ_b denote the amplitude of the component function F_b for $b \in \mathbb{F}_{2^n}^*$. Since F_b is unbalanced by Corollary 1, we must have $W_F(0,b) \in \{\pm\lambda_b\}$, and thus $W_F^2(0,b) = \lambda_b^2$ for all $b \in \mathbb{F}_{2^n}^*$. Since by Theorem 2 F has a Gold-like Walsh spectrum, we know that λ_b, and hence $W_F^2(0,b)$, takes precisely two values across all $b \in \mathbb{F}_{2^n}^*$, viz. 2^n and 2^{n+2}. By Lemma 4 we then have that the hyperplane $\mathcal{H}(b)$ corresponds to 3 differential sets H_a if $W_F^2(0,b) = 2^{n+2}$; and that it corresponds to no differential set if $W_F^2(0,b) = 2^n$. Thus, $H_aF = H_bF$ for some $a,b \in \mathbb{F}_{2^n}^*$ implies $b \in \{a, \beta a, \beta^2 a\}$, and so π_F is 3-to-1 as claimed. Conversely, if $H_aF = H_bF$ for some $b \notin \{a, \beta a, \beta^2 a\}$, then we must have $W_F^2(0,b) \notin \{2^n, 2^{n+2}\}$ by Lemma 4, and so F does not have a Gold-like Walsh spectrum. We thus obtain a contradiction to Theorem 2. □

Based on some limited computational experiments, we suspect that the same is true for triplicate functions that are not necessarily canonical and not necessarily quadratic; in other words, that a triplicate function has $(2^n-1)/3+1$ distinct differential sets if and only if it is 3-to-1. We leave this as an open question.

In light of the analogy that we make between 3-to-1 (n,n)-functions for even n and permutations for odd n, we remark that an analogical results is know for quadratic APN permutations over $\mathbb{F}_{2^n}$ with odd n [45]; in fact, Proposition 2 of that paper shows that any generalized crooked function in an odd number of variables has all differential sets distinct.

C. Other extremal properties of 3-to-1 functions

As we have seen above, 3-to-1 functions can be characterized among quadratic canonical triplicate functions by minimizing or maximizing the value of certain parameters (such as the size of the image set, or the number of distinct differential sets). In this section, we formulate several more characterizations of this form and show, in particular, that 3-to-1 functions can be characterized by their number of bent components, and their number of components having non-zero linear structures.

1) Linear structures: Recall that $a \in \mathbb{F}_{2^n}^*$ is called a **linear structure** of $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ if D_af is constant. If F is an APN function all of whose differential sets are linear hyperplanes, then we can observe that $H_aF = \mathcal{H}(b)$ for some $a,b \in \mathbb{F}_{2^n}^*$ if and only if a is a linear structure of F_b. Indeed, if $H_aF = \mathcal{H}(b)$, then we have $\mathrm{Tr}(bD_aF(x)) = 0$ for all $x \in \mathbb{F}_{2^n}$ by the definition of $\mathcal{H}(b)$; but from the additivity of the trace function, we can write this as $\mathrm{Tr}(bD_aF(x)) = \mathrm{Tr}(bF(x) + bF(a+x)) = F_b(x) + F_b(a+x) = D_aF_b(x) = 0$ for any $x \in \mathbb{F}_{2^n}$. We thus know that some linear hyperplane $\mathcal{H}(b)$ corresponds to a differential set of F if and only if F_b has non-zero linear structures. The number of components with non-zero linear structures of a crooked triplicate function is thus equal to the number of distinct differential sets. Theorem 6 can then be equivalently formulated as follows.

Corollary 10. Let F be a generalized crooked canonical triplicate (and hence 3-to-1) (n,n)-function. Then F has at most $(2^n-1)/3$ components having non-zero linear structures. Furthermore, this bound is met with equality if and only if F is 3-to-1.

2) Bent components: Continuing from the above, we can see from Proposition 29 on page 100 of [23] that the derivative D_ef a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is equal to 0 if and only if the support $\mathrm{Supp}(W_f)$ of its Walsh transform is contained in $\{0,e\}^\perp = \mathcal{H}(e)$. Applying this to the components of an (n,n)-function F, we see that $e \in \mathbb{F}_{2^n}$ is a linear structure of F_b for some $b \in \mathbb{F}_{2^n}^*$ if and only if $H_e = \mathcal{H}(b)$ if and only if $\mathrm{Supp}(W_{F_b}) \subseteq \mathcal{H}(e)$. On other hand, if $\mathbb{F}_b$ is bent for some $b \in \mathbb{F}_{2^n}$, then we have $\mathrm{Supp}(W_{F_b}) = \mathbb{F}_{2^n}$, and so the hyperplane $\mathcal{H}(b)$ does not correspond to any differential set. Thus, the number of distinct differential sets of F is equal to the number of non-bent components. From the preceding discussion, we know that this number is no greater than $(2^n-1)/3$ for any triplicate function, and is attained by the 3-to-1 functions; we thus obtain yet another alternative expression of Theorem 6. We remark that this is known from [2].

Corollary 11. Let F be a generalized crooked canonical triplicate (and hence 3-to-1) (n,n)-function. Then F has as most $(2^n-1)/3$ non-bent components. Furthermore, this bound is met with equality if and only if F is 3-to-1.

V. Inequivalence of quadratic 3-to-1 APN functions to permutations

One of the main motivations for searching for new instances of APN functions is the hope that some of them may be CCZ-equivalent to permutations, and help shed new light on the so-called "big APN problem", i.e. the problem of the existence of APN permutations over finite fields of even extension degree greater than 6. This naturally raises the question of whether

3-to-1 APN functions can be CCZ-equivalent to permutations. In this section, we partially answer this question by showing that quadratic 3-to-1 APN functions over fields of doubly-even extension degree cannot be CCZ-equivalent to a permutation. In order to do this, we use a necessary condition from [40] and generalize a proof from the same paper showing that the functions from family C4 are CCZ-inequivalent to permutations in the case of doubly-even extension degrees.

Let F be an (n,n)-function for some natural number n, and let $\mathrm{NB}(F)$ denote the set of non-bent components of F, i.e. the set of all elements $a \in \mathbb{F}_{2^n}^*$ for which the component function F_a is not bent. The necessary condition derived in [40] states that if F is CCZ-equivalent to a permutation, then $\{0\} \cup \mathrm{NB}(F)$ must contain a linear subspace of dimension $n/2$. This condition is used in [40] both computationally and theoretically to show that certain APN functions cannot be CCZ-equivalent to permutations. In the following, we will show that this necessary condition is violated by any quadratic 3-to-1 APN function over a field of doubly-even extension degree, and conclude that such functions cannot be CCZ-equivalent to permutations.

We begin by generalizing a classical result due to Carlitz [28] that gives the exact value of exponential sums of the form $\sum_x \chi(ax^3)$; this is also given as Lemma 1 in [40], and is an integral part of the proof of the CCZ-inequivalence of C4 to permutations. In our generalization, we interpret the elements x^3 as the images of the Gold function $x \mapsto x^3$, and replace x^3 with $F(x)$ in the exponential sum, where F is some quadratic 3-to-1 APN function. The actual proof of the generalized statement is a simple corollary of our observations on the values of the Walsh transform of quadratic 3-to-1 functions.

Corollary 12. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic 3-to-1 APN function for some natural number $n = 2m$. Denoting $q = 2^m$, we have

$$\sum_{x \in \mathbb{F}_{2^n}} \chi(aF(x)) = \begin{cases} q^2 & a = 0 \\ (-1)^{m+1} 2q & a \in \mathrm{NB}(F) \\ (-1)^m q & a \in \mathbb{F}_{2^n}^* \setminus \mathrm{NB}(F), \end{cases} \tag{10}$$

where $\mathrm{NB}(F)$ is the set of non-bent components of F.

Proof. For any $a \in \mathbb{F}_{2^n}$, the exponential sum $\sum_x \chi(ax^3)$ is simply the Walsh coefficient $W_F(0,a)$. If $a = 0$, the result is obvious. From the discussion in Section IV-C2, we know that the non-bent components of F are precisely those elements $a \in \mathbb{F}_{2^n}$ for which the hyperplane $\mathcal{H}(a)$ is a differential set of F; and from Lemma 4, we know that $W_F(0,a)^2 = 2^n$ if $a \notin \mathrm{NB}(F) \cup \{0\}$ and $W_F(0,a)^2 = 2^{n+2}$ if $a \in \mathrm{NB}(F)$, whence we can derive the absolute value of $W_F(0,a)$. The signs can be inferred from Theorem 2. □

We also recall the following well-known observation (see e.g. Proposition 10 on pp. 74-75 in [23] for a proof).

Lemma 5. Let $W \subseteq \mathbb{F}_{2^n}$ be a subspace of $\mathbb{F}_{2^n}$ (using the identification of $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$) for some natural number n. Then for any $a \in \mathbb{F}_{2^n}$, we have

$$\sum_{w \in W} \chi(aw) = \begin{cases} 0 & a \notin W^\perp \\ \#W & a \in W^\perp, \end{cases} \tag{11}$$

where $W^\perp$ is the orthogonal complement of W.

We are now ready to prove the following theorem.

Theorem 7. Let F be a quadratic 3-to-1 (and hence APN) (n,n)-function for some natural number $n = 2m = 4k$. Let $\mathrm{NB}(F)$ be the set of non-bent components of F, and let W be any linear subspace contained in $\mathrm{NB}(F) \cup \{0\}$. Then the dimension of W is at most $m-1$. In particular, F is not CCZ-equivalent to a permutation.

Proof. Denote $q = 2^m$. Following the proof of Lemma 3 in [40], we evaluate the sum

$$\sum_{w \in W} \sum_{x \in \mathbb{F}_{2^n}} \chi(wF(x)) \tag{12}$$

in two ways.

First, we apply (11) to (12), and obtain

$$\sum_{w \in W} \sum_{x \in \mathbb{F}_{2^n}} \chi(wF(x)) = \#W \#\{x : F(x) \in W^\perp\} = \#W(3\#(W^\perp \cap \mathrm{Im}(F)) + 1).$$

The second identity follows from the fact that any non-zero element in the image of F has precisely 3 preimages, while 0 has precisely one preimage, viz. 0 itself. Note that $(W^\perp \cap \mathrm{Im}(F))$ does not contain 0.

On the other hand, applying (10) to (12), we get

$$\sum_{w \in W} \sum_{x \in \mathbb{F}_{2^n}} \chi(wF(x)) = q^2 + (\#W - 1)(-1)^{m+1} 2q$$

since $W \subseteq \{0\} \cup \mathrm{NB}(F)$ by assumption.

Under the assumption that m is even, and denoting $X = \#(W^{\perp} \cap \mathrm{Im}(F))$, we now have

$$\#W(3X+1) = q^2 - 2q(\#W - 1),$$

which becomes

$$3\#WX + \#W = q^2 - 2\#Wq + 2q,$$

that is,

$$X = (q^2 - 2\#Wq + 2q - \#W)/(3\#W).$$

Let us assume that the dimension of W is at least $m-1$ (otherwise there is nothing to prove). The number of elements in W is thus $2^{m-1} + c = q/2 + c$ for some natural number c (possibly equal to zero). Substituting $q/2 + c$ for $\#W$ in the above equation, we get

$$X = (q^2 - q^2 - 2qc + 2q - q/2 - c)/(3/2q + 3c) = (3/2q - 2qc - c)/(3/2q + 3c) = 1 - (4c + 2qc)/(3/2q + 3c).$$

The quotient $(4c + 2qz)/(3/2q + 3c)$ is clearly non-negative for any choice of c, and so we get $X \leq 1$. Since X must be a natural number, we have $X \in \{0, 1\}$. If $X = 0$, then we must have

$$\frac{4c + 2qc}{3/2q + 3c} = 1,$$

that is,

$$2c + 4qc - 3q = 0,$$

which leads to

$$c = \frac{3q}{2 + 4q} = \frac{3 \cdot 2^m}{2 + 2^{m+2}}.$$

This expression is clearly less than 1 for any choice of m, and since c must be a natural number, we obtain a contradiction to $X = 0$. Thus, we must have $X = 1$.

If $X = 1$, then we must have

$$\frac{4c + 2qc}{3/2q + 3c} = 0.$$

Since the denominator is positive (due to both q and c being natural numbers, and $q = 2^m$ being non-zero), the above fraction is equal to zero if and only if $4c + 2qc = 0$, i.e. $2c(2 + q) = 0$, which is only possible if $c = 0$. Thus, the size of W is precisely $q/2 = 2^{m-1}$, and the dimension of W is precisely $m - 1$. Since this was done under the assumption that the dimension of W is at least $m - 1$, we can conclude that the dimension of any linear subspace W contained in $\mathrm{NB}(F) \cup \{0\}$ is at most $m - 1$. The CCZ-inequivalence to permutations then follows immediately by Corollary 1 of [40]. □

We note that Theorem 7 significantly simplifies the proof of the CCZ-inequivalence of C4 to permutations from [40], and generalizes it to any quadratic 3-to-1 APN function. The question remains open of whether quadratic 3-to-1 functions can be equivalent to permutations in the case of singly-even dimensions. In this regard, we recall that the Kim function over $\mathbb{F}_{2^6}$ is not equivalent to a 3-to-1 function.

VI. Triplicates in the infinite families

In this section, we demonstrate that triplicate and canonical triplicate functions are heavily represented among the instances of the known infinite APN families. More precisely, we observe the following. Note that in all cases we consider even dimensions n.

(i) all power APN functions are canonical triplicates;
(ii) family C1-C2 consists entirely of canonical triplicates;
(iii) the functions of family C3 are not canonical triplicates (as observed in [44]); however, we can computationally verify that they are linear-equivalent to canonical 3-to-1 functions for dimensions up to 12;
(iv) families C4, C5, C6 consist entirely of canonical triplicates;
(v) the only canonical triplicates in C7-C9 are the ones that intersect C1-C2; the remaining functions from C7-C9 are not triplicates;
(vi) the functions from C10 are not triplicates;
(vii) some of the functions in families C10 and C12 are non-canonical triplicates, and the remaining ones are not triplicates;
(viii) family C13 consists entirely of canonical triplicates;
(ix) family C14 consists entirely of canonical triplicates when $n/2$ is odd [44];
(x) family C15 consists entirely of canonical triplicates.

Proposition 8. All functions belonging to families C1-C2, C4, C5, C6, C13, C14, or C15, as well as any monomial APN function over $\mathbb{F}_{2^n}$ for even n, is a canonical triplicate. The only functions from family C7-C9 that are canonical triplicates are the ones that intersect C1-C2.

Proof. The functions from family C1-C2 have the polynomial form

$$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}},$$

so that the exponents in their univariate form are 2^s+1 and $2^{ik}+2^{mk+s}$. One of the conditions for such functions to be APN is $\gcd(s,3k) = \gcd(s,n) = 1$, and since n is even, we must have that s is odd. Hence 2^s+1 is a multiple of 3. When considering the other exponent, we consider the cases $p=3$ and $p=4$ separately. In both cases, we have $m = p-i$, i.e. $m+i=p$. In the case when $p=3$, this means that we have either $(i,m)=(1,2)$, or $(i,m)=(2,1)$. In the first case, the exponent becomes $2^k+2^{2k+s} = 2^k(1+2^{k+s})$, which is divisible by 3 if and only if $3 \mid 1+2^{k+s}$, which is true if and only if $k+s$ is odd; since we know that s must be odd, this means that the second exponent is a multiple of 3 if and only if k is even. Similarly, if $(i,m)=(2,1)$, the second exponent becomes $2^{2k}+2^{k+s} = 2^{2k}(1+2^{s-k})$, which is divisible by 3 if and only if $3 \mid (1+2^{s-k})$ which, in turn, occurs if and only if $s-k$ is odd; as before, we know that s is odd; we thus conclude that when $p=3$, the second exponent is divisible by 3 if and only if k is even. On the other hand, we have $n = pk = 3k$, and since n is even by assumption, k must necessarily be even as well. Thus, all functions from C1-C2 for $p=3$ are canonical triplicates. When $p=4$, we have three possibilities for the values of (i,m), viz. $(1,3)$, $(2,2)$, and $(3,1)$. The second exponent, $2^{ik}+2^{mk+s}$, then becomes $2^k+2^{3k+s} = 2^k(1+2^{2k+s})$ in the first case; $2^{2k}+2^{2k+s} = 2^{2k}(1+2^s)$ in the second case; and $2^{3k}+2^{k+s} = 2^{k+s}(2^{2k-s}+1)$ in the third case. Since s is odd, we can immediately see that this exponent is divisible by 3 in all three cases, and so the functions from C1-C2 are canonical triplicates when $p=4$ as well.

To see that the functions from C3 are canonical 3-to-1 functions when $n = 2m = 4k$, we refer to the bivariate representation of these functions given in [21], viz.

$$F(x,y) = (c+c^q)x^{2^i+1} + (w^{2^i} + w^{2^iq} + cw^{2^iq} + c^qw^{2^i})xy^{2^i} + (w+w^q+cw+c^qw^q)x^{2^i}y + (w^{2^i+1} + w^{(2^i+1)q} + cw^{2^iq+1} + c^qw^{2^i+q})y^{2^i+1} + (w+w^q)xy + s(w^{2^i}+w^{2^iq})(xy)^{2^i},$$

where $w \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $q = 2^m$, and $c, s \in \mathbb{F}_{2^n}$ satisfy the conditions given in Table II. The sum of the last two terms in the above expression, i.e. $(w+w^q)xy + s(w^{2^i}+w^{2^iq})(xy)^{2^i}$, is linear, and can be ignored up to EA-equivalence. If $n = 4k$, so that m is even, then we have that i must be odd thanks to the condition $\gcd(i,m)=1$. Consequently, we can see that in all of the terms x^{2^i+1}, xy^{2^i}, $x^{2^i}y$, and y^{2^i+1}, the total degree is always a multiple of 3, and so (x,y), $(\beta x, \beta^2 y)$, and $(\beta^2 x, \beta y)$ always map to the same output for any $x,y \in \mathbb{F}_{2^m}$. Consequently, the functions are triplicates, and thanks to Theorem 1, they are 3-to-1. Clearly, the elements of $\mathbb{F}_{2^n}$ represented by the pairs e.g. (x,y) and $(\beta x, \beta^2 y)$ from $\mathbb{F}_{2^m}^2$ are not multiples of β, and so these functions are not canonical.

The functions from families C4, C5, and C6 are obviously canonical triplicates since the composition $L \circ C$ of a canonical (n,n)-triplicate C with any linear function L (and, in particular, any trace function Tr_m^n for $m \mid n$) is a canonical triplicate as well.

Similarly, as we know from e.g. [23], any power APN function x^e over a field of even extension degree n must satisfy $\gcd(e, 2^n-1) = 3$ and, in particular, e must be a multiple of 3.

The functions from family C13 are of the form

$$x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k},$$

and we can clearly ignore the value of k since e is divisible by 3 if and only if $e \cdot 2^k$ is divisible by 3 for any natural numbers e and k. For the same reason, $3 \cdot 2^m$ is always a multiple of 3, and $2^{i+m}+2^m$ is a multiple of 3 if and only if the same is true for 2^i+1. We thus only have to consider the exponent 2^i+1. According to the conditions for family C13, we must have $i \in \{m-2, m, 2m-1, (m-2)^{-1} \mod n\}$, and m must be odd. We then immediately see that 2^i+1 is a multiple of 3 in all cases, and so all functions from family C13 are indeed canonical triplicates.

A proof of the fact that the functions from C14 are 3-to-1 is given in [44].

The functions from family C15 have the univariate representation

$$a\mathrm{Tr}_m^n(bx^3) + a^q\mathrm{Tr}_m^n(b^3x^9),$$

and, as remarked above, the property of a function being a canonical triplicate is invariant under composition with linear functions; it is thus obvious that C15 consists of canonical 3-to-1 functions.

The functions from family C3 are not canonical 3-to-1 functions as observed already in [44]; however, we computationally confirm that they are linearly-equivalent to canonical functions for $n \leq 12$, and believe that this is the case in general.

The functions from family C7-C9 have the univariate form

$$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}.$$

We can observe that $2^{-k}+1 = 2^{2k}+1$ is never a multiple of 3, and so we must have $v = 0$. Furthermore, if $3 \mid 2^s + 2^{k+s} = 2^s(1+2^k)$, then k must be odd; and $3 \mid 2^s + 1$ implies that s is odd as well so that $s-k$ is even. But then

$$2^{-k} + 2^{k+s} = 2^{2k} + 2^{k+s} = 2^{2k}(1+2^{s-k})$$

cannot be a multiple of 3, and so we must have $w = 0$ if the function is a canonical triplicate. When $v = w = 0$, all functions from C7-C9 are, in fact, contained in C1-C2.

The functions from C10 have a univariate representation of the form

$$(x+x^{2^m})^{2^k+1} + u'(ux + u^{2^m}x^{2^m})^{(2^k+1)2^i} + u(x+x^{2^m})(ux+u^{2^m}x^{2^m}).$$

One of the conditions states that u should be a primitive element of $\mathbb{F}_{2^n}$, and so in particular $u \neq 0$. The last term from the above expression expands to

$$u(ux^2 + (u^{2^m}+u)x^{2^m+1} + x^{2^{m+1}}),$$

and so these functions are clearly not canonical triplicates. □

Remark 5. As demonstrated in the previous proposition, the functions from families C14-1 and C14-2 as given by the bivariate representation from Table II are canonical triplicate functions. On the other hand, it is easy to see that the univariate representation of these functions found in e.g. [18] does not correspond to a canonical triplicate function. This suggests that it may be possible to find a simple canonical form for these functions directly from their bivariate form. In the case of $n = 2m$ with m odd, we can easily obtain such a representation for C14-1 and C14-2 by writing every element $X \in \mathbb{F}_{2^n}$ as $X = x + \beta y$ for $x, y \in \mathbb{F}_{2^m}$ where $x, y \in \mathbb{F}_{2^m}$ and β is primitive in $\mathbb{F}_4$. This is possible only when m is odd due to $\beta \notin \mathbb{F}_{2^m}$. The advantage in this case is that we have $\beta^k \in \{1, \beta, \beta^2\}$ for any natural number k, which greatly simplifies the resulting univariate translation. Denoting $\overline{x} = x^{2^m}$, we obtain:

- for m odd and i odd, the functions from C14-1 take the univariate form
$$x^{2^i+1} + \beta^2\overline{x}^{2^i+1} + \beta x^{2^{2i}}\overline{x} + x\overline{x}^{2^{2i}};$$
- for m odd and i even, they take the form
$$x\overline{x}^{2^i} + \beta^2 x^{2^i}\overline{x} + \beta x^{2^{2i}}\overline{x} + x\overline{x}^{2^{2i}};$$
- for i odd, the functions from C14-2 take the univariate form
$$x^{2^i+1} + \beta^2\left(\overline{x}^{2^i+1} + x^{2^{3i}+1} + \overline{x}^{2^{3i}+1}\right);$$
- for i even, they take the form
$$x\overline{x}^{2^i} + \beta^2\left(x^{2^i}\overline{x} + x^{2^{3i}}\overline{x} + x\overline{x}^{2^{3i}}\right).$$

For the sake of completeness, we show how to derive the univariate form for C14-2 and i odd; the remaining three cases are handled in the same way. Recall that any $X \in \mathbb{F}_{2^n}$ can be written as $X = x + \beta y$ with $x, y \in \mathbb{F}_{2^m}$. Raising both sides to the power 2^m, we obtain $\overline{X} = x + \beta^2 y$, and so $y = X + \overline{X}$ and hence $x = \beta^2 X + \beta\overline{X}$. Observe that for i odd, we have $\beta^{2^i} = \beta^2$ and $\beta^{2^i+1} = 1$. In the bivariate expression of C14-2, viz.

$$F(x,y) = (F_1(x,y), F_2(x,y)) = (x^{2^i+1} + xy^{2^i} + y^{2^i+1}, x^{2^{3i}}y + x^{2^{3i}}),$$

we can first express the left-hand side as

$$\begin{aligned}
F_1(x,y) &= (\beta^2 X + \beta\overline{X})^{2^i+1} + (\beta^2 X + \beta\overline{X})(X+\overline{X})^{2^i} + (X+\overline{X})^{2^i+1} \\
&= X^{2^i+1} + \beta^2 X^{2^i}\overline{X} + \beta X\overline{X}^{2^i} + \overline{X}^{2^i+1} + \beta^2 X^{2^i+1} + \beta^2 X\overline{X}^{2^i} \\
&\quad + \beta X^{2^i}\overline{X} + \beta\overline{X}^{2^i+1} + X^{2^i+1} + X^{2^i}\overline{X} + X\overline{X}^{2^i} + \overline{X}^{2^i+1} \\
&= \beta^2 X^{2^i+1} + \beta\overline{X}^{2^i+1}.
\end{aligned}$$

Similarly, we get

$$\begin{aligned}
F_2(x,y) &= (\beta^2 X + \beta\overline{X})^{2^{3i}}(X+\overline{X}) + (\beta^2 X + \beta\overline{X})(X+\overline{X})^{2^{3i}} \\
&= \beta X^{2^{3i}+1} + \beta X^{2^{3i}}\overline{X} + \beta^2 X X^{2^{3i}} + \beta^2\overline{X}^{2^{3i}+1} + \beta^2 X^{2^{3i}+1} + \beta^2 X\overline{X}^{2^{3i}} + \beta X^{2^{3i}}\overline{X} + \beta\overline{X}^{2^{3i}+1} \\
&= X^{2^{3i}+1} + \overline{X}^{2^{3i}}.
\end{aligned}$$

Combining the two, we get

$$F(x,y) = F_1(x,y) + \beta F_2(x,y) = \beta^2 X^{2^i+1} + \beta\overline{X}^{2^i+1} + \beta X^{2^{3i}+1} + \beta\overline{X}^{2^{3i}+1};$$

it then suffices to divide by β^2 in order to obtain the univariate representation above.

In the case where m is even, we have to decompose $X \in \mathbb{F}_{2^n}$ as $X = x + wy$ with $x, y \in \mathbb{F}_{2^m}$ for some $w \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. We then get $x = (\overline{w}X + w\overline{X})/(w + \overline{w})$ and $y = (X + \overline{X})/(w + \overline{w})$. By substituting this into the bivariate representation of C14-1, we can obtain a univariate expression by following the same strategy as above. However, since the order of w will be greater than 3, this expression will not be as compact in general as the one that we give above for m odd.

Remark 6. For functions from C3 in doubly even dimensions $n = 2m = 4k$, we see in the proof above that the elements (x, y), $(\beta x, \beta^2 y)$, and $(\beta^2 x, \beta y)$ map to the same output for any $x, y \in \mathbb{F}_{2^m}$. Such functions are clearly not canonical triplicates, but could potentially be used to define a variation of the notion of a canonical triplicate for functions in bivariate representation. Namely, we could say that a function $F(x, y)$ for $x, y \in \mathbb{F}_{2^m}$ with $2 \mid m$ is "bivariate canonical" if the total degree of every term in its bivariate representation is a multiple of 3; that is, if for every $x^i y^j$, we have $3 \mid i+j$. This is equivalent to saying that $F(x, y) = F(\beta x, \beta^2 y) = F(\beta^2 x, \beta y)$ for all $x, y \in \mathbb{F}_{2^m}$. Note that a canonical triplicate function also satisfies this condition (except that for canonical triplicates, not only the total degree, but the individual degrees of x and y must be multiples of 3 for each term) but not vice-versa. We leave the investigation of triplicate functions in bivariate form as a problem for future work. We also conduct an ad-hoc computational search, in which we take functions from $C3$ for $n = 8$, and attempt to compose them with linear permutations on the right in order to obtain canonical 3-to-1 functions. According to our computations, all such "bivariate canonical" functions for $n = 8$ are linear-equivalent to canonical ones.

Remark 7. By Theorem 2, we now obtain a very simple proof that these families have a Gold-like Walsh spectrum. Computing the Walsh spectra of the infinite families from first principles can be quite technical; one can find proofs that the known infinite families have Gold-like Walsh spectrum in [5] (for C1-C2), [7] (for C7-C9), [39] (for the Gold functions), [49] (for C10), [17] (for C4, C5, C6).

In particular, we obtain the first (to the best of our knowledge) proof of the fact that families C13, C14, and C15 have a Gold-like Walsh spectrum. We formulate this as a corollary.

Corollary 13. All functions from families C13, and C15 in Table II have a Gold-like Walsh spectrum.

VII. Conclusion and future work

We have introduced the classes of triplicate functions and canonical triplicate functions, and expressed 3-to-1 functions as extremal objects among them in several ways. We have investigated the properties of such functions, with a particular focus on quadratic 3-to-1 APN functions. We have computed the exact number of distinct differential sets of power APN functions, and of quadratic canonical 3-to-1 functions.

The topic of triplicate functions, 3-to-1 functions, and their relation to APN-ness appears to be very deep and quite promising, and there are many avenues for future research remaining to be investigated. For one thing, all of the currently known quadratic 3-to-1 functions are canonical, or linear-equivalent to canonical. It would be very interesting to find examples of triplicate 3-to-1 APN functions linear-inequivalent to canonical ones, or to show that such functions do not exist. In the former case, we will obtain a 3-to-1 APN instance behaving in a completely different way than all the know ones. In the same vein, it would be useful to resolve the inclusions between the classes of 3-to-1 functions having the zero-sum property and the triple summation property.

Another interesting question would be to try to find non-quadratic 3-to-1 APN functions CCZ-inequivalent to monomials, or to show that such functions do not exist. Regardless of whether the answer is positive or negative, this would be a step towards resolving the problem of finding APN functions CCZ-inequivalent to quadratic functions and monomials.

Many of the properties derived in our investigation are proved for the case of quadratic 3-to-1 functions, or for canonical 3-to-1 functions. We suspect that many of them also hold for 3-to-1 functions of higher algebraic degree, but were not able to prove or disprove this. For instance, we have proved that any quadratic canonical 3-to-1 function over $\mathbb{F}_{2^n}$ has precisely $(2^n - 1)/3$ distinct differential sets. We suspect that this is true for 3-to-1 triplicate functions in general, but it is not clear to us at the moment how one could prove this.

Acknowledgments

This research is sponsored by the Trond Monh foundation. We thank Claude Carlet and Lukas Kölsch for their helpful comments which have improved the quality of the draft.

References

[1] Encyclopedia of Boolean functions. http//boolean.h.uib.no/mediawiki/index.php/Main_Page.

[2] Thierry P. Berger, Anne Canteaut, Pascale Charpin, and Yann Laigle-Chapuy. On almost perfect nonlinear functions over $\mathbb{F}_{2^n}$. *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

[3] Thomas Beth and Cunsheng Ding. On almost perfect nonlinear permutations. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 65–76. Springer, 1993.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4(1):3–72, Jan 1991.

[5] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. Fourier spectra of binomial APN functions. *SIAM Journal on Discrete Mathematics*, 23(2):596–608, 2009.

[6] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 2011.

[7] Carl Bracken and Zhengbang Zha. On the Fourier spectra of the infinite families of quadratic apn functions. *arXiv preprint arXiv:0811.4718*, 2008.

[8] Marcus Brinkmann and Gregor Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography*, 49:273–288, 2008.

[9] Lilya Budaghyan, Marco Calderini, Claude Carlet, Robert S Coulter, and Irene Villa. Constructing APN functions through isotopic shifts. *IEEE Transactions on Information Theory*, 66(8):5299–5309, 2020.

[10] Lilya Budaghyan and Claude Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. *IEEE Transactions on Information Theory*, 54(5):2354–2357, 2008.

[11] Lilya Budaghyan, Claude Carlet, Tor Helleseth, and Nikolay Kaleyski. On the distance between APN functions. *IEEE Transactions on Information Theory*, 66(9):5742–5753, 2020.

[12] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Transactions on Information Theory*, 54(9):4218–4229, 2008.

[13] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Constructing new APN functions from known ones. *Finite Fields and Their Applications*, 15(2):150–159, 2009.

[14] Lilya Budaghyan, Claude Carlet, and Gregor Leander. On a construction of quadratic APN functions. In *2009 IEEE Information Theory Workshop*, pages 374–378, 2009.

[15] Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[16] Lilya Budaghyan, Tor Helleseth, and Nikolay Kaleyski. A new family of APN quadrinomials. *IEEE Transactions on Information Theory*, 66(11):7081–7087, 2020.

[17] Lilya Budaghyan, Tor Helleseth, Nian Li, and Bo Sun. Some results on the known classes of quadratic APN functions. In *International Conference on Codes, Cryptology, and Information Security*, pages 3–16. Springer, 2017.

[18] Marco Calderini, Lilya Budaghyan, and Claude Carlet. On known constructions of APN and AB functions and their relation to each other. *Rad HAZU, Matematike znanosti*, 2021. to appear.

[19] Anne Canteaut, Alain Couvreur, and Léo Perrin. Recovering or testing extended-affine equivalence. *arXiv preprint arXiv:2103.00078*, 2021.

[20] Claude Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3(2):135–145, 1993.

[21] Claude Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. *Designs, Codes and Cryptography*, 59(1):89–109, 2011.

[22] Claude Carlet. Boolean and vectorial plateaued functions and APN functions. *IEEE Transactions on Information Theory*, 61(11):6272–6289, 2015.

[23] Claude Carlet. *Boolean functions for cryptography and coding theory*. Cambridge University Press, 2021.

[24] Claude Carlet. Bounds on the nonlinearity of differentially uniform functions by means of their image set size, and on their distance to affine functions. *IEEE Transactions on Information Theory*, 67(12):8325–8334, 2021.

[25] Claude Carlet, Pascale Charpin, and Victor A. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[26] Claude Carlet, Guang Gong, and Yin Tan. Quadratic zero-difference balanced functions, APN functions and strongly regular graphs. *Designs, Codes and Cryptography*, 78(3):629–654, 2016.

[27] Claude Carlet, Annelie Heuser, and Stjepan Picek. Trade-offs for S-boxes: Cryptographic properties and side-channel resilience. In *International Conference on Applied Cryptography and Network Security*, pages 393–414. Springer, 2017.

[28] Leonard Carlitz. Explicit evaluation of certain exponential sums. *Mathematica Scandinavica*, 44:5–16, 1979.

[29] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In *Workshop on the Theory and Application of Cryptographic Techniques, EUROCRYPT 94*, volume 950, pages 356–365, 1994.

[30] Robert Coulter and Nikolay Kaleyski. Further observations on the distance invariant. Boolean functions and their application (BFA 2021), to be presented, 2021.

[31] Ingo Czerwinski. On the minimal value set size of APN functions. *IACR Cryptol. ePrint Arch.*, 2020:705, 2020.

[32] Joan Daemen and Vincent Rijmen. AES proposal: Rijndael, 1999.

[33] Joan Daemen and Vincent Rijmen. *The design of Rijndael*, volume 2. Springer, 2002.

[34] Itai Dinur and Adi Shamir. Breaking Grain-128 with dynamic cube attacks. In *International Workshop on Fast Software Encryption*, pages 167–187. Springer, 2011.

[35] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Information & Computation*, 151(1):57–72, 1999.

[36] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[37] Hans Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5. *International Conference on Finite Fields and Applications*, pages 113–121, 2001.

[38] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1):59–81, 2009.

[39] Robert Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.). *IEEE Transactions on Information Theory*, 14(1):154–156, 1968.

[40] Faruk Göloğlu and Ji Pavl. On CCZ-inequivalence of some families of almost perfect nonlinear functions to permutations. *Cryptography and Communications*, pages 1–15, 2021.

[41] Heeralal Janwa and Richard M Wilson. Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 180–194. Springer, 1993.

[42] Tadao Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. *Information & Computation*, 18(4):369–394, 1971.

[43] Lars R Knudsen. Truncated and higher order differentials. In *International Workshop on Fast Software Encryption*, pages 196–211. Springer, 1994.

[44] Lukas Kölsch, Björn Kriepke, and Gohar M Kyureghyan. Image sets of perfectly nonlinear maps. *arXiv preprint arXiv:2012.00870*, 2020.

[45] Gohar M. M. Kyureghyan. Crooked maps in $\mathbb{F}_{2^n}$. *Finite Fields and Their Applications*, 13(3):713–726, 2007.

[46] Siu Lun Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, 4(4):221–261, 1994.

[47] Kaisa Nyberg. Differentially uniform mappings for cryptography. *Lecture Notes in Computer Science*, 765:55–64, 1994.

[48] Ana Salagean. Discrete antiderivatives for functions over fpn. 2019.

[49] Yin Tan, Longjiang Qu, San Ling, and Chik How Tan. On the fourier spectra of new apn functions. *SIAM journal on discrete mathematics*, 27(2):791–801, 2013.

[50] Hiroaki Taniguchi. On some quadratic APN functions. *Designs, Codes and Cryptography*, pages 1–11, 2019.

[51] Guobiao Weng, Yin Tan, and Guang Gong. On quadratic almost perfect nonlinear functions and their related algebraic object. In *Workshop on Coding and Cryptography*, pages 57–68. Citeseer, 2013.

[52] Satoshi Yoshiara. Equivalences of quadratic APN functions. *Journal of Algebraic Combinatorics*, 35(3):461–475, 2012.
[53] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions.
[54] Yuyin Yu, Mingsheng Wang, and Yongqiang Li. A matrix approach for constructing quadratic APN functions. *Designs, codes and cryptography*, 73(2):587–600, 2014.
[55] Lijing Zheng, Haibin Kan, Yanjun Li, Jie Peng, and Deng Tang. Constructing new APN functions through relative trace functions. *arXiv preprint arXiv:2101.11535*, 2021.
[56] Yuliang Zheng and Xian-Mo Zhang. Plateaued functions. In *ICICS '99 Proceedings of the Second International Conference on Information and Communication Security*, 1999.
[57] Yue Zhou and Alexander Pott. A new family of semifields with 2 parameters. *Advances in Mathematics*, 234:43–60, 2013.