Differentially 2^t-uniform quadrinomials with high nonlinearity

Niki Spithaki*[1], Enrico Piccione[2], Lilya Budaghyan[1], and Alexander Kholosha[1]

[1]University of Bergen, Bergen, Norway,
{niki.spithaki, lilya.budaghyan, oleksandr.kholosha}@uib.no
[2]Ruhr University Bochum, Bochum, Germany,
enrico.piccione@rub.de

Abstract

In this paper, we discuss some cryptographic properties of a family of quadrinomials constructed as a generalization of a known family of APN quadrinomials. In particular, we show that this family produces differentially 2^t-uniform quadrinomials with the same Walsh spectrum as the Gold power function x^{2^t+1} over $\mathbb{F}_{2^n}$. We also discuss whether this family provides permutations.

Keywords: Differential uniformity, Nonlinearity, Walsh spectrum, S-boxes, Vectorial Boolean functions, Permutation

1 Introduction

Symmetric ciphers use S-boxes, functions from $\mathbb{F}_{2^n}$ to itself, to reinforce security by adding nonlinearity to the system. Such functions should possess high resistance to differential and linear attacks, and for that purpose it is crucial they have low differential uniformity and high nonlinearity, respectively. The functions that attain the minimum differential uniformity are considered optimal in terms of resistance against differential attacks and are called *almost perfect nonlinear (APN)*.

We say that two functions F and F' are *extended affine equivalent* (EA-equivalent) if there exist affine permutations A_1, A_2 and an affine mapping A such that $F' = A_1 \circ F \circ A_2 + A$. Until recently, all known APN functions were

*Corresponding author.

EA-equivalent to one of the known power functions over finite fields, namely the Gold, Kasami, Welch, Niho, inverse and Dobbertin functions [11, Chapter 11.5.2]. It was, in fact, conjectured that the above was the complete list of APN functions up to EA-equivalence.

In [12], Carlet, Charpin and Zinoviev introduced a new equivalence relation of functions, referred to as *CCZ-equivalence*. Two functions are called CCZ-equivalent if the graph of one can be obtained from the graph of the other by an affine permutation of the product space. Functions that are CCZ-equivalent have the same differential uniformity and the same extended Walsh spectrum. EA-equivalence is a special case of CCZ-equivalence. More specifically, in [9], it is proven that CCZ-equivalence is more general than EA-equivalence and taking inverses of permutations, and classes of APN functions that are CCZ-equivalent to Gold functions but EA-inequivalent to power functions are constructed. This disproved the original conjecture and instead opened the question of whether there exist APN functions that are CCZ-inequivalent to power functions.

Two early sporadic examples of quadratic APN functions that are CCZ-inequivalent to power mappings were given in [17]. The question of whether there exists an infinite class of APN functions CCZ-inequivalent to power functions was answered in [8], where the authors introduce two infinite classes of quadratic APN functions for n divisible by 3 or 4 that are, for $n \geq 12$, CCZ-inequivalent to power mappings. They are proven to be permutations for n odd, and almost 3-to-1 for n even. Furthermore, their Walsh spectrum and nonlinearity are the same as those of the Gold APN functions.

For the case of a field with even degree, there is only one known example of an APN permutation for $n = 6$, presented by Dillon et al. [16]. The existence of more APN permutations on a field of even degree remains a big open problem. It is natural, then, given the lack of APN permutations, that researchers turn their attention towards finding differentially δ-uniform permutations, with δ as small as possible. For example, the AES (Advanced Encryption Standard) S-box is obtained by composing the inverse function, a differentially 4-uniform permutation on $\mathbb{F}_{2^8}$, with an affine permutation. As noted by Carlet [10, Chapter 9], the alternatives for the inverse function are very rare and it is a main challenge to find more candidates for good S-boxes.

A few 4-uniform permutations have been found [5, 6, 21]. In [6], Bracken, Tan and Tan generalize one of the infinite families of APN binomials found in [8], and construct a class of binomial 4-uniform permutations on $\mathbb{F}_{2^n}$, where $n = 3k$, k is an even integer, $3 \nmid k$ and $k/2$ is odd. More generally, they prove that, if u is a primitive element of $\mathbb{F}_{2^{3k}}$, the function

$$G(x) = ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} \tag{1}$$

is a differentially two-valued 2^t-uniform permutation, where $3 \mid (k+s)$ and $t = \gcd(3k, s)$ is a divisor of k with k/t odd. Furthermore, they show that, for any $a \in \mathbb{F}_{2^{3k}}$ and $b \in \mathbb{F}^*_{2^{3k}}$, the Walsh coefficients of G are bounded by $2^{(n+t)/2}$ if $n+t$ is even. We should note here that the case $n+t$ odd can never occur because of the assumption n/t odd.

The class in (1) is a family of binomials with 2^t-to-1 derivatives that are permutations when k/t is odd and almost (2^t+1)-to-1 when k/t is even. Furthermore, it is proven in [14] that its Walsh spectrum is of the form $\{0, \pm 2^{\frac{n+t}{2}}\}$ for $n+t$ even and n/t odd. This shows that APN binomials admit an extension that is similar to Gold functions.

A generalization of the second infinite family of APN binomials in [8], for $n = 4k$, was studied in [15]. More specifically, the authors proved that this family can also be generalized to a family of differentially 2^t-uniform functions, in a similar way as in the case $n = 3k$.

After studying the quadratic APN functions listed in [4], the authors of [6] also found a class of quadrinomials that may have the same properties as function (1). However, they did not manage to prove this claim, and instead posed it as an open problem. The quadrinomial class in question is an extension of the binomial family in (1) and is obtained by adding two extra terms to the initial function. We explicitly define this function F in Theorem 3.1.

This paper is dedicated to providing an answer to this open problem. Previously, part of this was considered in [22], where the authors focus on the special case $t = 2$. There they claim that, while F can be proven to be a differentially 4-uniform function with high nonlinearity, it is not generally a permutation, thus giving a negative answer to the problem for $t = 2$. More specifically, they prove that F is a permutation for $t = 2$ and $k < 22$ if and only if one of the following two conditions holds:

1. $v = w = 0$ (in which case F is simply the binomial (1)).
2. $k = 2$ and $s \equiv 4 (\mathrm{mod} 6)$.

In this paper, we focus on the problem covering the general case $t \geq 2$. More specifically, we prove that the function F is differentially two-valued (with values 0 and 2^t) with differential uniformity 2^t. Furthermore, we characterize the Fourier spectrum of F, showing that its structure depends on the parity of n/t. It is important to mention here that the proof for the Fourier spectrum is not simply an easy generalization of the proof for the APN quadrinomial case presented in [7], as there were many technical steps. Moreover, for the case n/t even, given the form of the Fourier spectrum of F, we prove that it is not a permutation. This was not easy to see initially because, unlike the case of the monomial and binomial families, we have that $F(\alpha x) = \alpha^2 F(x)$ for all $\alpha \in \mathbb{F}_{2^t}$. Consequently, n/t odd is a necessary condition for F to be a permutation.

The paper is structured as follows. In Section 2, we present basic definitions and results that were used in our work. In Section 3, we present some observations on the quadrinomial family and formally state and prove our main theorem. More specifically, in Subsection 3.1 we prove that F is a differentially two-valued function with differential uniformity 2^t, in Subsection 3.2 we determine its Walsh spectrum, and finally in Subsection 3.3 we present a report on our computational results regarding the question of whether F is a permutation (in the case n/t odd). We summarize our results in the conclusion.

2 Preliminaries

Let n be a positive integer. The finite field with 2^n elements is then denoted as $\mathbb{F}_{2^n}$. For any positive integer k that is a divisor of n, the *trace function* $\mathrm{Tr}_k^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ is defined as

$$\mathrm{Tr}_k^n(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{2^{ik}}.$$

For $k = 1$, the function $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called the *absolute trace* over $\mathbb{F}_{2^n}$ and is denoted simply by $\mathrm{Tr}_n(x)$, or simply $\mathrm{Tr}(x)$ if the dimension n is clear from context.

For n, m positive integers, the functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are called *vectorial functions*. If $m = 1$, the functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ are called *Boolean functions*.

Identifying $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$, we can uniquely represent any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ as a polynomial of the form

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

where $a_j \in \mathbb{F}_{2^n}$. This representation is called the *univariate representation of* F.

The *algebraic degree of* F can be expressed using the 2-weight of the exponents of the univariate representation. Any integer j with $0 \leq j \leq 2^n - 1$ can be represented as a sum of powers of two, that is, we can write $j = \sum_{i=0}^{n-1} j_i \cdot 2^i$ for $j_i \in \{0, 1\}$. Then, the 2-weight of j is $w_2(j) = \sum_{i=0}^{n-1} j_i$. The algebraic degree of F can then be written as $\max_{0 \leq j \leq 2^n-1 | a_j \neq 0} w_2(j)$.

Let F be a function over $\mathbb{F}_{2^n}$. If $F(x) = x^d$ for some exponent d, then F is called a *power function*. F is called *linear* if its univariate representation is of the form $F(x) = \sum_{i=0}^{n-1} b_i x^{2^i}$, for $b_i \in \mathbb{F}_{2^n}$. It is called *affine* if it can be written as the sum of a linear function and a constant. A function F of the form

$$F(x) = \sum_{i,j=0}^{n-1} b_{ij} x^{2^i+2^j} + b,$$

where $b_{ij}, b \in \mathbb{F}_{2^n}$, is called *quadratic*. Finally, F is called a *Dembowski-Ostrom (DO) polynomial* if it is of the form

$$F(x) = \sum_{0 \leq i \neq j < n} b_{ij} x^{2^i+2^j},$$

where $b_{ij} \in \mathbb{F}_{2^n}$.

Let F be a function on $\mathbb{F}_{2^n}$. Then F is *d-to-1* if every element in the image of F has exactly d preimages. Additionally, we will call F *almost d-to-1* if $F^{-1}(0) = \{0\}$ and $|F^{-1}(x)| = d$ for all $x \in \mathrm{im}(F) \setminus \{0\}$. Power functions are a primary example of almost d-to-1 functions. If an integer m divides $2^n - 1$, F

will be called *m-divisible* if the exponent of every nonzero term of F is divisible by m.

For $a \in \mathbb{F}_{2^n}$, the function $D_aF(x) = F(x+a) + F(x)$ is called the *derivative of F in the direction a*. For any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, define

$$\delta_F(a,b) = |\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}|.$$

The *differential uniformity* of F is then defined as

$$\Delta_F := \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_F(a,b).$$

It is easy to see that $\Delta_F \geq 2$ and Δ_F is even. A function is then called *almost perfect nonlinear* (APN) if its differential uniformity attains the minimum value $\Delta_F = 2$. We say that the function F is *differentially two-valued* if $\delta_F(a,b)$ can take only the two values $\{0, 2^s\}$ for some positive integer s and any $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n}$.

If $\Delta_F = \delta$, so that the polynomial $F(x+a) + F(x) + b$ has at most δ roots in $\mathbb{F}_{2^n}$ for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, then F is *differentially δ-uniform*. In the special case of a quadratic function F, it is enough to count the number of roots of $F(x+a) + F(x) + F(a) + F(0)$, because each derivative $D_aF(x)$ is an affine function. By this definition, F is APN on $\mathbb{F}_{2^n}$ if and only if it is differentially 2-uniform on $\mathbb{F}_{2^n}$.

The nonlinearity of a function can be defined via its Walsh transform. For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, we define the *Walsh (Fourier) transform* $\mathcal{W}_F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^* \to \mathbb{Z}$ as

$$\mathcal{W}_F(a,b) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_n(ax) + \mathrm{Tr}_m(bF(x))}, \quad a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_{2^m}^*.$$

The set $S_F := \{\mathcal{W}_F(a,b) : \ a \in \mathbb{F}_{2^n},\ b \in \mathbb{F}_{2^m}^*\}$ is called the Walsh spectrum of F.

The nonlinearity of F is defined as

$$N_F := 2^{n-1} - \frac{1}{2} \max_{s \in S_F} |s|.$$

Let F be an (n,n)-function. It is known that, if n is odd, then N_F is upper bounded by $2^{n-1} - 2^{(n-1)/2}$ [13]. Functions attaining this bound are called *almost bent* (AB). Almost bent functions exist only for odd values of n. When n is even, it is conjectured that N_F is upper bounded by $2^{n-1} - 2^{n/2}$. For the remainder of this paper, we will call a function *highly nonlinear* if its nonlinearity attains one of these bounds (depending on the parity of n).

Since they achieve the highest possible nonlinearity, AB functions provide optimal security against linear cryptanalysis when n is odd. Moreover, it is proven that all AB functions are APN [13], thus AB functions are optimal against differential cryptanalysis as well.

A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is *bent* when n is even and its Walsh transform takes values in $\{\pm 2^{n/2}\}$. It is *plateaued* when either it is bent or

its Walsh transform takes values in $\{0, \pm 2^{(n+s)/2}\}$, where s is an integer such that $1 \leq s \leq n$ and $n+s$ is even. The value $2^{(n+s)/2}$ is called the *amplitude* of f. A vectorial function F over $\mathbb{F}_{2^n}$ is called *plateaued* if its components are plateaued Boolean functions. It is called *plateaued with single amplitude* when all its components have the same amplitude. It is known that all quadratic functions are plateaued.

3 On cryptographic properties of the quadrinomial family

The main result of this paper is presented in the following theorem:

Theorem 3.1. *Let $n = 3k$, s and k be positive integers with $k+s$ divisible by 3, $\gcd(s,k) = t$ and $\gcd(3,s) = \gcd(3,k) = 1$. Let u be a primitive element of $\mathbb{F}_{2^{3k}}$ and let $v, w \in \mathbb{F}_{2^k}$ with $vw \neq 1$. Define the function $F : \mathbb{F}_{2^{3k}} \to \mathbb{F}_{2^{3k}}$ by*

$$F(x) = ux^{2^s+1} + u^{2^k} x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1} x^{2^{k+s}+2^s}. \tag{2}$$

Then F is differentially two-valued with differential uniformity 2^t. Moreover, the Walsh spectrum of F is $\{0, \pm 2^{\frac{n+t}{2}}\}$ when n/t is odd and $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2t}{2}}\}$ when n/t is even.

Consider the following class of quadratic functions over $\mathbb{F}_{2^n}$ of the form

$$F(x) = \sum_{0 \leq i < j < n/t} c_{i,j} x^{2^{it}+2^{jt}}, \tag{3}$$

where t is a positive divisor of n and $c_{i,j} \in \mathbb{F}_{2^n}$. An important observation is that both the binomials (1) and the quadrinomials (2) belong to this class. Functions of this form were first studied in [14]. The following property will be used later in our proof for the form of the Walsh spectrum of function (2):

Theorem 3.2 ([14, Theorem 8])**.** *Let F be any function of the form (3). If F is differentially two-valued with differential uniformity 2^t and F does not have bent components, then F is plateaued with single amplitude $2^{(n+t)/2}$.*

Using Theorem 3.2, the authors further proved in [14, Theorem 9] that when n/t is odd the binomial permutations F in (1) are plateaued with a single amplitude $2^{(n+t)/2}$ because F is differentially two-valued with differential uniformity 2^t [6, Lemma 3.1] and F cannot have bent components since it is a permutation. Regarding the Walsh spectrum of F when n/t is even, we can show that it is equal to $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2t}{2}}\}$ by using known results.

Proposition 3.1. *Let F be a binomial as in (1) where $n = 3k$, $k+s$ is divisible by 3, $\gcd(3,k) = \gcd(3,s) = 1$, $t = \gcd(n,s)$ and u is a primitive element of $\mathbb{F}_{2^n}$.*

1. *If n/t is odd, then F is a permutation and its Walsh spectrum is equal to* $\{0, \pm 2^{\frac{n+t}{2}}\}$.

2. *If n/t is even, then F is almost (2^t+1)-to-1 and its Walsh spectrum is equal to* $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2t}{2}}\}$.

Proof. Item 1 was proved in [6, Lemma 2.1] and [14, Theorem 9]. Let us prove item 2. First, since s/t is odd, it follows that 2^t+1 divides 2^s+1 and thus F is a (2^t+1)-divisible DO polynomial. Furthermore, since k/t is even and $\gcd(s/t, k/t) = 1$, s/t is odd. Hence $(s+2k)/t$ is also odd and consequently $2^{2k} + 2^{k+s} = 2^{2k}(1 + 2^{s+2k}) \mod 2^n - 1$. By [18, Corollary 3], we have that F is almost (2^t+1)-to-1 because F is a (2^t+1)-divisible DO polynomial and F is 2^t-uniform [6, Lemma 3.1]. Finally, we can conclude that the Walsh spectrum is equal to $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2t}{2}}\}$ by using [20, Theorem 5.2] because F is almost (2^t+1)-to-1 and F is plateaued (since it is quadratic). □

On the other hand, the quadrinomials of the form (2) are not necessarily permutations when n/t is odd. Consequently, we cannot exclude the existence of bent components when n is even and n/t odd. Regarding the case when n/t is even, it does not seem likely that the function is almost (2^t+1)-to-1 because it is not (2^t+1)-divisible and so we cannot use [18, Corollary 3]. Indeed, observe that since t is a divisor of k and $n/t = 3k/t$ is even, we have that 2^t+1 does not divide $2^{2k}+1$ and $2^{k+s} + 2^s = 2^s(2^k+1)$, which are the exponents of the terms with coefficients v and wu^{2^k+1} in (2), respectively. Note that if both coefficients are zero, then the family reduces to the binomials (1).

In conclusion, investigating the Walsh spectrum of the quadrinomials (2) is much more complicated than the one of the binomials (1) because, in addition to their value distribution being completely different, the permutation argument and the divisibility criterion used for the binomials are no longer applicable.

In the next two subsections, we prove that F is differentially 2^t-uniform with differential spectrum $\{0, 2^t\}$ (Proposition 3.2) and determine its Walsh spectrum (Proposition 3.3). The proof of Theorem 3.1 follows from Propositions 3.2 and 3.3.

3.1 F is differentially two-valued

We begin by proving that the function F is differentially 2^t-uniform. Our proof adapts [4, Theorem 2.1] to fit our case for general t.

Proposition 3.2. *Let F be the function defined as in Theorem 3.1. Then F is differentially two-valued with differential uniformity 2^t.*

Proof. Since F is quadratic, it is enough to show that, for every $a \in \mathbb{F}_{2^{3k}}^*$, the equation

$$F(x) + F(x+a) + F(a) = 0$$

has exactly 2^t solutions.

We have

$$u^{2^k}(x^{2^{k+s}}a^{2^{-k}} + a^{2^{k+s}}x^{2^{-k}}) + u(x^{2^s}a + a^{2^s}x) + v(x^{2^{-k}}a + a^{2^{-k}}x) + \\ + wu^{2^k+1}(x^{2^s}a^{2^{k+s}} + a^{2^s}x^{2^{k+s}}) = 0$$

and by replacing x with ax and collecting terms in x we get

$$(va^{2^{-k}+1} + ua^{2^s+1})x + (va^{2^{-k}+1} + u^{2^k}a^{2^{-k}+2^{k+s}})x^{2^{-k}} + \\ +(wu^{2^k+1}a^{2^{k+s}+2^s} + ua^{2^s+1})x^{2^s} + (wu^{2^k+1}a^{2^{k+s}+2^s} + u^{2^k}a^{2^{-k}+2^{k+s}})x^{2^{k+s}} = 0.$$

We write

$$Ax + Bx^{2^{-k}} + Cx^{2^s} + Dx^{2^{k+s}} = 0, \tag{4}$$

where

$$A = va^{2^{-k}+1} + ua^{2^s+1},\ B = va^{2^{-k}+1} + u^{2^k}a^{2^{-k}+2^{k+s}},$$
$$C = wu^{2^k+1}a^{2^{k+s}+2^s} + ua^{2^s+1},\ D = wu^{2^k+1}a^{2^{k+s}+2^s} + u^{2^k}a^{2^{-k}+2^{k+s}}.$$

We claim that none of A, B, C, D vanish for any nonzero values of a. The sketch of the proof is that, if we suppose that any one of A, B, C, D is zero, then we can write u as a product of an element of $\mathbb{F}_{2^k}$ and a^e, where e is divisible by 7. This would imply that u is a 7-th power, which is not possible since u is primitive. We will explicitly prove here that $B \neq 0$, and similarly A, C and D are all nonzero.

If $B = 0$, then $va^{2^{-k}+1} = u^{2^k}a^{2^{-k}+2^{k+s}}$, which means $u^{2^k} = va^{1-2^{k+s}}$. Since $k + s$ is divisible by 3, it is evident that $1 - 2^{k+s}$ is divisible by 7, and thus $a^{1-2^{k+s}}$ is a 7-th power in $\mathbb{F}_{2^{3k}}$. Now, since 3 does not divide k, 7 does not divide $2^k - 1$, and thus the map $x \mapsto x^7$ is a permutation on $\mathbb{F}_{2^k}$. This means that v can be expressed as a 7-th power. We deduce that u^{2^k} and hence u is a 7-th power in $\mathbb{F}_{2^{3k}}$, which gives us a contradiction since 7 divides $2^{3k} - 1$ and u is a primitive element of $\mathbb{F}_{2^{3k}}$. We then have $B \neq 0$.

We now define the linearized polynomial:

$$L_\alpha(Y) := Y + \alpha Y^{2^k} + \alpha^{2^k+1}Y^{2^{-k}}.$$

Observe that, when $Y = \alpha x + x^{2^{-k}}$ and α is a non-zero $(2^k - 1)$-th power, we have $L_\alpha(Y) = 0$ for all $x \in \mathbb{F}_{2^{3k}}$.

Now,

$$\frac{A}{B} = \frac{va^{2^{-k}+1} + ua^{2^s+1}}{va^{2^{-k}+1} + u^{2^k}a^{2^{-k}+2^{k+s}}} = \frac{v + ua^{2^s-2^{-k}}}{v + u^{2^k}a^{2^{k+s}-1}} = (v + ua^{2^s-2^{-k}})^{1-2^k},$$

which means that $L_{\frac{A}{B}}(\frac{A}{B}x + x^{2^{-k}}) = 0$.

We return to (4) and divide by B:

$$\left(\frac{A}{B}x + x^{2^{-k}}\right) + \left(\frac{C}{B}x^{2^s} + \frac{D}{B}x^{2^{k+s}}\right) = 0.$$

Applying the linearized polynomial, we have

$$L_{\frac{A}{B}}\Big(\frac{A}{B}x + x^{2^{-k}}\Big) + L_{\frac{A}{B}}\Big(\frac{C}{B}x^{2^s} + \frac{D}{B}x^{2^{k+s}}\Big) = 0,$$

and since $L_{\frac{A}{B}}(\frac{A}{B}x + x^{2^{-k}}) = 0$ we get the equation

$$L_{\frac{A}{B}}\Big(\frac{C}{B}x^{2^s} + \frac{D}{B}x^{2^{k+s}}\Big) = 0,$$

or equivalently

$$\Big(\frac{C}{B} + \frac{A^{2^k+1}D^{2^{-k}}}{B^{2^k+2^{-k}+1}}\Big)x^{2^s} + \Big(\frac{D}{B} + \frac{AC^{2^k}}{B^{2^k+1}}\Big)x^{2^{k+s}} + \Big(\frac{AD^{2^k}}{B^{2^k+1}} + \frac{A^{2^k+1}C^{2^{-k}}}{B^{2^k+2^{-k}+1}}\Big)x^{2^{-k+s}} = 0.$$

We multiply both sides by $B^{2^k+2^{-k}+1}$ to obtain

$$(B^{2^k+2^{-k}}C + D^{2^{-k}}A^{2^k+1})x^{2^s} + (B^{2^k+2^{-k}}D + B^{2^{-k}}AC^{2^k})x^{2^{k+s}} + +(B^{2^{-k}}AD^{2^k} + A^{2^k+1}C^{2^{-k}})x^{2^{-k+s}} = 0.$$

We substitute the values of A, B, C, D and after simplifying we obtain:

$$\begin{aligned}(vw+1)ua^{2^k+2^s+1}(va^{2^{-k}} + ua^{2^s})(u^{2^k}a^{2^{k+s}+2^k} + u^{2^{-k}}a^{2^{-k+s}+1})x^{2^s} + \\ +(vw+1)u^{2^k}a^{2^{k+s}+2^k+1}(va^{2^{-k}} + ua^{2^s})(ua^{2^k+2^s} + u^{2^{-k}}a^{2^{-k+s}+2^{-k}})x^{2^{k+s}} + \\ +(vw+1)u^{2^{-k}}a^{2^{-k+s}+2^k+1}(va^{2^{-k}} + ua^{2^s})(u^{2^k}a^{2^{k+s}+2^{-k}} + ua^{2^s+1})x^{2^{-k+s}} = 0.\end{aligned}$$

Since we chose v and w such that $vw \neq 1$, and as $A \neq 0$, we can divide the above equation by $(vw+1)a^{2^k}Au^{2^{-k}+1}a^{2^{-k+s}+2^s+1} \neq 0$, or equivalently, $(vw+1)a^{2^k+1}(va^{2^{-k}} + ua^{2^s})u^{2^{-k}+1}a^{2^{-k+s}+2^s+1} \neq 0$, and raise both sides to the power 2^{-s} to obtain

$$(1 + b^{-2^{k-s}})x + (b^{2^{-s}} + b^{-2^{k-s}})x^{2^k} + (1 + b^{2^{-s}})x^{2^{-k}} = 0, \tag{5}$$

where $b = u^{2^k-1}a^{2^{-k}+2^{k+s}-2^s-1}$.

We now return to (4), divide by C and apply the linearized polynomial $L_{\frac{D}{C}}$:

$$L_{\frac{D}{C}}\Big(\frac{A}{C}x + \frac{B}{C}x^{2^{-k}}\Big) + L_{\frac{D}{C}}\Big(x^{2^s} + \frac{D}{C}x^{2^{k+s}}\Big) = 0.$$

We have $L_{\frac{D}{C}}\Big(x^{2^s} + \frac{D}{C}x^{2^{k+s}}\Big) = 0$, since

$$\frac{D}{C} = \frac{wu^{2^k+1}a^{2^{k+s}+2^s} + u^{2^k}a^{2^{-k}+2^{k+s}}}{wu^{2^k+1}a^{2^{k+s}+2^s} + ua^{2^s+1}} = (w + u^{-1}a^{2^{-k}-2^s})^{1-2^k}.$$

This means that $L_{\frac{D}{C}}\left(\frac{A}{C}x + \frac{B}{C}x^{2^{-k}}\right) = 0$, or

$$\left(\frac{A}{C} + \frac{DB^{2^k}}{C^{2^k+1}}\right)x + \left(\frac{DA^{2^k}}{C^{2^k+1}} + \frac{D^{2^k+1}B^{2^{-k}}}{C^{2^k+2^{-k}+1}}\right)x^{2^k} + \left(\frac{B}{C} + \frac{D^{2^k+1}A^{2^{-k}}}{C^{2^k+2^{-k}+1}}\right)x^{2^{-k}} = 0.$$

We multiply both sides by $C^{2^k+2^{-k}+1}$ to obtain

$$(C^{2^{-k}+2^k}A + C^{2^{-k}}DB^{2^k})x + (C^{2^{-k}}DA^{2^k} + D^{2^k+1}B^{2^{-k}})x^{2^k} + +(C^{2^{-k}+2^k}B + D^{2^k+1}A^{2^{-k}})x^{2^{-k}} = 0.$$

A similar computation to the previous case will yield the equation

$$(1 + b^{-2^{-k}})x + (1 + b)x^{2^k} + (b + b^{-2^{-k}})x^{2^{-k}} = 0. \tag{6}$$

We combine equations (5) and (6) in such a way that the terms containing $x^{2^{-k}}$ vanish:

$$((1 + b^{-2^{k-s}})(b + b^{-2^{-k}}) + (1 + b^{-2^{-k}})(1 + b^{2^{-s}}))x + +((b^{2^{-s}} + b^{-2^{k-s}})(b + b^{-2^{-k}}) + (1 + b)(1 + b^{2^{-s}}))x^{2^k} = 0$$

or, equivalently,

$$((1 + b^{-2^{k-s}})(b + b^{-2^{-k}}) + (1 + b^{-2^{-k}})(1 + b^{2^{-s}}))(x + x^{2^k}) = 0.$$

We will now show that $(1 + b^{-2^{k-s}})(b + b^{-2^{-k}}) + (1 + b^{-2^{-k}})(1 + b^{2^{-s}}) \neq 0$ for all b arising from the above definition and thus conclude that $x \in \mathbb{F}_{2^k}$.

Suppose, for a contradiction, that this coefficient is zero. Then

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

Rearranging the terms and observing that $b^{-2^{-k}} = b^{2^k+1}$ we obtain

$$b = \frac{(1 + b^{-1})^{2^{-k}}(1 + b)^{2^{-s}}}{(1 + b^{-1})^{2^{k-s}}(1 + b)^{2^k}} = ((1 + b^{-1})^{-2^k}(1 + b))^{2^{-s}-2^k}.$$

This implies that b is a $(2^{k+s} - 1)$-th power, which in turn means that it is a 7-th power. Since $b = u^{2^k-1}a^{2^{-k}+2^{k+s}-2^s-1} = u^{2^k-1}a^{(2^{k+s}-1)(1-2^{-k})}$, it is evident that if b is a seventh power then so is u^{2^k-1}, but this is not possible since k is not divisible by 3 and u is primitive. We can now conclude that $x \in \mathbb{F}_{2^k}$. Applying this to equation (4), we get

$$(ua^{2^s+1} + u^{2^k}a^{2^{-k}+2^{k+s}})(x + x^{2^s}) = 0.$$

If $ua^{2^s+1} + u^{2^k}a^{2^{-k}+2^{k+s}} = 0$, then $b = 1$, which is impossible because 1 is a 7-th power and b is not (since u^{2^k-1} is not). Hence, $x + x^{2^s} = 0$, which implies $x \in \mathbb{F}_{2^{3k}} \cap \mathbb{F}_{2^s} = \mathbb{F}_{2^t}$, since $(3k, s) = t$. Conversely, every $x \in \mathbb{F}_{2^t}$ satisfies (4), since $A + B + C + D = 0$. Thus the original equation has kernel $a\mathbb{F}_{2^t}$, and every nonempty solution set of the derivative equation has 2^t elements. □

3.2 On the Walsh spectrum of F

For the proof of Proposition 3.3, we will use the following two lemmas. The first one is a generalization of [1, Corollary 1]:

Lemma 3.1. *Let n, d, s be positive integers, let $t = \gcd(n, s)$ and let L be a non-zero polynomial with $L(x) = \sum_{i=0}^{d} r_i x^{2^{si}} \in \mathbb{F}_{2^n}[x]$. Then the equation $L(x) = 0$ has at most 2^{dt} solutions.*

Proof. Observe that L is $\mathbb{F}_{2^t}$-linear because s is divisible by t and therefore each monomial in $L(x)$ is of the form $x^{2^{tj}}$ for some non-negative integer j. Let $V = \ker(L)$ and v be the $\mathbb{F}_{2^t}$-dimension of V. We claim that $v \leq d$. Let V' be the $\mathbb{F}_{2^s}$-vector subspace of $\mathbb{F}_{2^{sn}}$ generated by V. By [3, Lemma 3.1], we have that the $\mathbb{F}_{2^s}$-dimension of V' is v. The polynomial L has degree at most 2^{sd}, so the number of zeros of L in the extension field $\mathbb{F}_{2^{sn}}$ is at most 2^{sd}. Since the elements of V' are zeroes of the polynomial L, we have $v \leq d$. □

Lemma 3.2. *Let n and t be positive integers such that t divides n. Let $\beta\colon (\mathbb{F}_{2^n})^2 \to \mathbb{F}_{2^t}$ be an alternating $\mathbb{F}_{2^t}$-bilinear form. Its radical is the subspace*

$$\mathrm{rad}(\beta) = \{x \in \mathbb{F}_{2^n} : \beta(x, y) = 0 \text{ for every } y \in \mathbb{F}_{2^n}\}.$$

Then

$$\dim_{\mathbb{F}_{2^t}} \mathrm{rad}(\beta) \equiv \frac{n}{t} \pmod 2.$$

Proof. We first recall why an alternating bilinear form has even rank. If β is nonzero, choose u, v with $\beta(u, v) \neq 0$. The restriction of β to $U = \langle u, v\rangle_{\mathbb{F}_{2^t}}$ is nondegenerate, and $\mathbb{F}_{2^n} = U \oplus U^\beta$ where $U^\beta = \{x : \beta(x, z) = 0 \text{ for every } z \in U\}$. Consequently,

$$\mathrm{rank}_{\mathbb{F}_{2^t}}(\beta) = \mathrm{rank}_{\mathbb{F}_{2^t}}(\beta|_U) + \mathrm{rank}_{\mathbb{F}_{2^t}}(\beta|_{U^\beta}) = 2 + \mathrm{rank}_{\mathbb{F}_{2^t}}(\beta|_{U^\beta}).$$

By induction on the dimension n, starting with the zero form, we have that $\mathrm{rank}_{\mathbb{F}_{2^t}}(\beta)$ is even. By applying the rank-nullity Theorem on the $\mathbb{F}_{2^t}$-linear function T_β that maps $x \in \mathbb{F}_{2^n}$ to $T_\beta(x) = \beta(x, \cdot)$, we have that

$$\dim_{\mathbb{F}_{2^t}} \mathrm{rad}(\beta) = \frac{n}{t} - \mathrm{rank}_{\mathbb{F}_{2^t}}(\beta) \equiv \frac{n}{t} \pmod 2.$$

□

Proposition 3.3. *Let F be the function defined as in Theorem 3.1. Then the Fourier spectrum of F is $\{0, \pm 2^{\frac{n+t}{2}}\}$ when n/t is odd and $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2t}{2}}\}$ when n/t is even.*

Proof. For any $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^n}^*$, the Walsh coefficient of F is

$$\mathcal{W}_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}(ax + bF(x))}.$$

Squaring $\mathcal{W}_F(a,b)$ gives

$$\begin{aligned}\mathcal{W}_F(a,b)^2 &= \sum_{x\in\mathbb{F}_{2^n}}\sum_{y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(ax+bF(x)+ay+bF(y))}\\ &= \sum_{x\in\mathbb{F}_{2^n}}\sum_{y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(ax+bF(x)+a(x+y)+bF(x+y))}\\ &= \sum_{y\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(ay+bF(y))}\sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(xL_b(y))},\end{aligned}$$

where

$$\begin{aligned}L_b(y) = b^{2^k}u^{2^{-k}}y^{2^{-k+s}} + b^{2^{-k-s}}u^{2^{-s}}y^{2^{k-s}} + b^{2^{-s}}u^{2^{-s}}y^{2^{-s}} + buy^{2^s} + b^{2^k}vy^{2^k}\\ + bvy^{2^{-k}} + b^{2^{-k-s}}w^{2^{-s}}u^{2^{-s}+2^{-k-s}}y^{2^{-k}} + b^{2^{-s}}w^{2^{-s}}u^{2^{-s}+2^{k-s}}y^{2^k}\end{aligned}$$

is a linearized polynomial such that $\mathrm{Tr}(b(F(x+y)+F(x)+F(y))) = \mathrm{Tr}(xL_b(y))$ for all $x,y\in\mathbb{F}_{2^n}$. Since $\sum_x(-1)^{\mathrm{Tr}(cx)} = 0$ when $c\neq 0$ and 2^n otherwise, we have

$$\mathcal{W}_F(a,b)^2 = 2^n\sum_{y\in\ker(L_b)}(-1)^{\mathrm{Tr}(ay+bF(y))}.$$

We claim that $|\mathcal{W}_F(a,b)|^2$ is either zero or equal to $2^n|\ker(L_b)|$. The Boolean function $\ell_{a,b}(y) = \mathrm{Tr}(ay+bF(y))$ restricted to the domain $\ker(L_b)$ is linear because $\ell_{a,b}(x+y)+\ell_{a,b}(x)+\ell_{a,b}(y) = \mathrm{Tr}(b(F(x+y)+F(x)+F(y))) = \mathrm{Tr}(xL_b(y)) = 0$. So we have that either $\ell_{a,b}(y) = 0$ for all $y\in\ker(L_b)$ and $|\mathcal{W}_F(a,b)|^2 = 2^n|\ker(L_b)|$, or the restriction of $\ell_{a,b}$ to $\ker(L_b)$ is nonzero, in which case its character sum vanishes and $|W_F(a,b)|^2 = 0$.

Suppose $L_b(y) = 0$, and thus $b^{2^{-k}}L_b(y)$ is equal to

$$\begin{aligned}&b^{2^{-k}}(b^{2^k}u^{2^{-k}}y^{2^{-k+s}} + b^{2^{-k-s}}u^{2^{-s}}y^{2^{k-s}} + b^{2^{-s}}u^{2^{-s}}y^{2^{-s}} + buy^{2^s} + b^{2^k}vy^{2^k}\\ &+ bvy^{2^{-k}} + b^{2^{-k-s}}w^{2^{-s}}u^{2^{-s}+2^{-k-s}}y^{2^{-k}} + b^{2^{-s}}w^{2^{-s}}u^{2^{-s}+2^{k-s}}y^{2^k}) = 0.\end{aligned}$$

The above is equivalent to

$$\begin{aligned}&b^{2^{-k}-2^{k-s}}u^{2^{-s}}(b^{2^{-s}+2^{k-s}}y^{2^{-s}} + b^{2^{k-s}+2^{-k-s}}y^{2^{k-s}} + b^{2^{-s}+2^{k-s}}w^{2^{-s}}u^{2^{k-s}}y^{2^k}\\ &+ b^{2^{k-s}+2^{-k-s}}w^{2^{-s}}u^{2^{-k-s}}y^{2^{-k}}) + b^{2^k+2^{-k}}u^{2^{-k}}y^{2^{-k+s}} + b^{2^{-k}+1}uy^{2^s}\\ &+ b^{2^k+2^{-k}}vy^{2^k} + b^{2^{-k}+1}vy^{2^{-k}} = 0.\end{aligned} \tag{7}$$

Let $\theta = u^{2^{-s}}b^{2^{-k}-2^{k-s}}$, $l = l(y) = b^{2^{-s}+2^{k-s}}(y^{2^{-s}} + w^{2^{-s}}u^{2^{k-s}}y^{2^k})$ and $r = r(y) = b^{2^k+2^{-k}}(vy^{2^k} + u^{2^{-k}}y^{2^{-k+s}})$. Equation (7) then becomes

$$b^{2^{-k}}L_b(y) = r + r^{2^k} + \theta(l + l^{2^k}) = 0. \tag{8}$$

Since $l^{2^{k+s}} = b^{2^k+2^{-k}}(y^{2^k} + wu^{2^{-k}}y^{2^{-k+s}})$, we have

$$l^{2^{k+s}} + wr = b^{2^k+2^{-k}}(wv+1)y^{2^k}. \tag{9}$$

Furthermore, notice that

$$vl^{2^{k+s}} + r = b^{2^k+2^{-k}}(wv+1)u^{2^{-k}}y^{2^{-k+s}}. \tag{10}$$

Equation (9) implies

$$y = (l^{2^s} + wr^{2^{-k}})b^{-1-2^k}(1+wv)^{-1}, \tag{11}$$

while equation (10) implies

$$y = (v^{2^{-s}}l^{2^{-k}} + r^{2^{k-s}})b^{-2^{-k-s}-2^{-s}}(1+vw)^{-2^{-s}}u^{-2^{-s}}. \tag{12}$$

Combining these two expressions for y we get

$$\theta z(l^{2^s} + wr^{2^{-k}}) = v^{2^{-s}}l^{2^{-k}} + r^{2^{k-s}},$$

where $z = (1+vw)^{2^{-s}-1}(b^{2^{-k}+2^k+1})^{2^{-s}-1}$. Note that z is an element of $\mathbb{F}_{2^k}$. We raise the above relation to the power of 2^k, rearrange and multiply by $\theta + \theta^{2^{-k}}$ to obtain

$$(\theta+\theta^{2^{-k}})(wz\theta^{2^k}r + v^{2^{-s}}l) = (\theta+\theta^{2^{-k}})(\theta^{2^k}zl^{2^{k+s}} + r^{2^{-k-s}}). \tag{13}$$

We claim that $\theta+\theta^{2^{-k}}$ is not zero. Indeed, if $\theta = \theta^{2^{-k}}$, then $\theta^{2^{k+s}} = \theta^{2^s}$ and $u^{2^k-1} = b^{(2^{k+s}-1)(2^k-2^{-k})}$. Since $k+s$ is divisible by 3, $2^{k+s}-1$ is divisible by 7, which implies that u is a 7th power, which is a contradiction as u is primitive.

From Equation (8) we have

$$r + r^{2^k} = \theta(l + l^{2^k}).$$

From this equation and using the fact that the relative trace mapping $\mathrm{Tr}_k^n(x) = x + x^{2^k} + x^{2^{-k}}$ from $\mathbb{F}_{2^{3k}}$ to $\mathbb{F}_{2^k}$ is zero for any field element of the form $\delta + \delta^{2^k}$, we derive the following:

$$\mathrm{Tr}_k(\theta(l+l^{2^k})) = \mathrm{Tr}_k((r+r^{2^k})) = 0.$$

As $\mathrm{Tr}_k(cg) = c\mathrm{Tr}_k(g)$ for every $c \in \mathbb{F}_{2^k}$, and $\theta^{2^{-k}+2^k+1} \in \mathbb{F}_{2^k}$, we obtain

$$\mathrm{Tr}_k((\theta+\theta^{2^{-k}})l) = \mathrm{Tr}_k(\theta^{2^k}(\theta+\theta^{2^{-k}})r) = 0. \tag{14}$$

Therefore, the left hand side of Equation (13) has relative trace zero, which implies the same is true for the right hand side. That is,

$$\mathrm{Tr}_k((\theta+\theta^{2^{-k}})(\theta^{2^k}zl^{2^{k+s}} + r^{2^{-k-s}})) = 0.$$

Let $\Theta = \theta + \theta^{2^{-k}}$. We write the above equation as

$$\begin{aligned} &z(\Theta\theta^{2^k} l^{2^{k+s}} + \Theta^{2^k}\theta^{2^{-k}} l^{2^{-k+s}} + \Theta^{2^{-k}}\theta l^{2^s}) \\ &= \Theta r^{2^{-k-s}} + \Theta^{2^k} r^{2^{-s}} + \Theta^{2^{-k}} r^{2^{k-s}}. \end{aligned} \tag{15}$$

From Equation (14) we obtain:

$$\begin{aligned} &\Theta l + \Theta^{2^k} l^{2^k} + \Theta^{2^{-k}} l^{2^{-k}} = 0 \\ &\Rightarrow l^{2^{-k+s}} = \Theta^{2^s - 2^{-k+s}} l^{2^s} + \Theta^{2^{k+s} - 2^{-k+s}} l^{2^{k+s}} \end{aligned}$$

and

$$\begin{aligned} r^{2^{-k-s}} &= \theta^{2^{k-s} - 2^{-s}} \Theta^{2^{-s} - 2^{-k-s}} r^{2^{-s}} \\ &\quad + \theta^{2^{-k-s} - 2^{-s}} \Theta^{2^{k-s} - 2^{-k-s}} r^{2^{k-s}}. \end{aligned}$$

We substitute these expressions for $l^{2^{-k+s}}$ and $r^{2^{-k-s}}$ into Equation (15) and get

$$\begin{aligned} &z((\Theta\theta^{2^k} + \Theta^{2^k}\theta^{2^{-k}}\Theta^{2^{k+s} - 2^{-k+s}}) l^{2^{k+s}} \\ &+ (\Theta^{2^{-k}}\theta + \Theta^{2^k}\theta^{2^{-k}}\Theta^{2^s - 2^{-k+s}}) l^{2^s}) \\ &= (\Theta^{2^k} + \Theta\theta^{2^{k-s} - 2^{-s}}\Theta^{2^{-s} - 2^{-k-s}}) r^{2^{-s}} \\ &+ (\Theta^{2^{-k}} + \Theta\theta^{2^{-k-s} - 2^{-s}}\Theta^{2^{k-s} - 2^{-k-s}}) r^{2^{k-s}}. \end{aligned}$$

We multiply across by $\Theta^{2^{-k-s} + 2^{-k+s}}\theta^{2^{-s}}$ and obtain

$$\begin{aligned} &z\Theta^{2^{-k-s}}\theta^{2^{-s}}((\Theta^{2^{-k+s}+1}\theta^{2^k} + \Theta^{2^{k+s}+2^k}\theta^{2^{-k}}) l^{2^{k+s}} \\ &+ (\Theta^{2^{-k+s}+2^{-k}}\theta + \Theta^{2^s+2^k}\theta^{2^{-k}}) l^{2^s}) \\ &= \Theta^{2^{-k+s}}((\Theta^{2^{-k-s}+2^k}\theta^{2^{-s}} + \Theta^{2^{-s}+1}\theta^{2^{k-s}}) r^{2^{-s}} \\ &+ (\Theta^{2^{-k-s}+2^{-k}}\theta^{2^{-s}} + \Theta^{2^{k-s}+1}\theta^{2^{-k-s}}) r^{2^{k-s}}). \end{aligned}$$

Let $P(\theta) = \Theta^{2^{-k+s}+1}\theta^{2^k} + \Theta^{2^{k+s}+2^k}\theta^{2^{-k}}$. Then the above equation becomes

$$\begin{aligned} &z\Theta^{2^{-k-s}}\theta^{2^{-s}}(P(\theta) l^{2^{k+s}} + P(\theta)^{2^{-k}} l^{2^s}) \\ &= \Theta^{2^{-k+s}}(P(\theta)^{2^{-k-s}} r^{2^{-s}} + P(\theta)^{2^{k-s}} r^{2^{k-s}}). \end{aligned} \tag{16}$$

We claim that $P(\theta)$ is a non-zero element of $\mathbb{F}_{2^k}$. Indeed, if $P(\theta) = 0$, then

$$\Theta^{2^{-k+s}+1}\theta^{2^k} = \Theta^{2^{k+s}+2^k}\theta^{2^{-k}}.$$

This implies

$$\theta^{2^k - 2^{-k}} = \Theta^{(2^{k+s}-1)(1-2^k)},$$

therefore $\theta^{2^k-2^{-k}}$ is a 7th power. But $\theta^{2^k-2^{-k}} = (ub^{2^k(2^{k+s}-1)})^{2^{-s}(2^k-2^{-k})}$, which would imply that u is also a 7th power, a contradiction.

To see that $P(\theta) \in \mathbb{F}_{2^k}$, first we rewrite the expression as follows:

$$P(\theta) = \Theta^{2^{-k+s}}\Theta\theta^{2^k} + \Theta^{2^{k+s}}\Theta^{2^k}\theta^{2^{-k}}.$$

This implies

$$P(\theta) = (\theta^{2^{-k+s}} + \theta^{2^{k+s}})(\theta^{2^k+1} + \theta^{2^{-k}+2^k}) + (\theta^{2^s} + \theta^{2^{k+s}})(\theta^{2^{-k}+1} + \theta^{2^{-k}+2^k}),$$

which in turn becomes

$$P(\theta) = \theta^{2^s}(\theta^{2^{-k}+1}+\theta^{2^{-k}+2^k})+\theta^{2^{k+s}}(\theta^{2^k+1}+\theta^{2^{-k}+1})+\theta^{2^{-k+s}}(\theta^{2^k+2^{-k}}+\theta^{2^k+1}).$$

The above can be written as

$$P(\theta) = \mathrm{Tr}_k(\theta^{2^{2s}}(\theta^{2^{-k}+1} + \theta^{2^{-k}+2^k})),$$

which is an element of $\mathbb{F}_{2^k}$. The claim is thus proved.

Now, Equation (16) becomes

$$z\Theta^{2^{-k-s}-2^{-k+s}}P(\theta)^{1-2^{-s}}(l + l^{2^k})^{2^s} = \theta^{-2^{-s}}(r + r^{2^k})^{2^{-s}}.$$

Using Equation (8) we obtain an equation in $(l + l^{2^k})$,

$$z\Theta^{2^{-k-s}-2^{-k+s}}P(\theta)^{1-2^{-s}}(l + l^{2^k})^{2^s} + (l + l^{2^k})^{2^{-s}} = 0.$$

Raising both sides to the power 2^s we get

$$z^{2^s}\Theta^{2^{-k}-2^{-k+2s}}P(\theta)^{2^s-1}(l + l^{2^k})^{2^{2s}} + (l + l^{2^k}) = 0. \tag{17}$$

If n/t is odd, we can apply Lemma 3.1 with $d = 1$ and $2s$ in place of s, since $\gcd(n, 2s) = \gcd(n, s) = t$, and then Equation (17) has at most 2^t solutions in the variable $\lambda(l) = l + l^{2^k}$. We claim that the number of solutions is either 1 or 2^t. If $\lambda(l) = l + l^{2^k}$ is a solution of (17), then for all $\beta \in \mathbb{F}_{2^t}$ we have that $\beta\lambda(l) = \lambda(\beta l)$ is a solution. Indeed, $\beta^{2^k} = \beta$ because t divides k and $\beta^{2^{2s}} = \beta$ because $\gcd(n, 2s) = t$. If n/t is even, again by Lemma 3.1, Equation (17) has either 1, 2^t or 2^{2t} solutions in the variable $\lambda(l) = l + l^{2^k}$.

Consider now the following two expressions derived from Equations (11) and (12), where $B = b^{1+2^k}(wv + 1)$:

$$By = l^{2^s} + wr^{2^{-k}}$$

$$u^{2^{-s}}B^{2^{-k-s}}y = v^{2^{-s}}l^{2^{-k}} + r^{2^{k-s}}.$$

From these, we can obtain

$$By + B^{2^k}y^{2^k} = (l + l^{2^k})^{2^s} + w(r + r^{2^k})^{2^{-k}}$$

$$u^{2^{-s}}B^{2^{-k-s}}y + u^{2^{k-s}}B^{2^{-s}}y^{2^k} = v^{2^{-s}}(l + l^{2^k})^{2^{-k}} + (r + r^{2^k})^{2^{k-s}}.$$

We eliminate the term y^{2^k} and get

$$\begin{aligned}(u^{2^{k-s}}B^{2^{-s}+1} + u^{2^{-s}}B^{2^{-k-s}+2^k})y = B^{2^k}(v^{2^{-s}}(l + l^{2^k})^{2^{-k}} + (r + r^{2^k})^{2^{k-s}}) \\ + u^{2^{k-s}}B^{2^{-s}}((l + l^{2^k})^{2^s} + w(r + r^{2^k})^{2^{-k}}).\end{aligned} \tag{18}$$

Let $D = u^{2^{k-s}}B^{2^{-s}+1} + u^{2^{-s}}B^{2^{-k-s}+2^k}$. Then D is not zero, since $D = 0$ would imply that $u^{2^{k-s}-2^{-s}} = B^{2^{-k-s}+2^k-2^{-s}-1} = B^{(2^{k+s}-1)(2^{-s}-2^{-k-s})}$, which, like in previous arguments, would contradict the fact that u is primitive.

We can, therefore, divide Equation (18) by D and get

$$\begin{aligned}y = D^{-1}(B^{2^k}(v^{2^{-s}}(l + l^{2^k})^{2^{-k}} + (r + r^{2^k})^{2^{k-s}}) \\ + u^{2^{k-s}}B^{2^{-s}}((l + l^{2^k})^{2^s} + w(r + r^{2^k})^{2^{-k}})).\end{aligned}$$

Using Equation (8) to substitute $r + r^{2^k}$ with $\theta(l + l^{2^k})$, we obtain

$$\begin{aligned}y = D^{-1}(B^{2^k}(v^{2^{-s}}(l + l^{2^k})^{2^{-k}} + (\theta(l + l^{2^k}))^{2^{k-s}}) \\ + u^{2^{k-s}}B^{2^{-s}}((l + l^{2^k})^{2^s} + w(\theta(l + l^{2^k}))^{2^{-k}})).\end{aligned}$$

With the above equation, we have proved that the map $\lambda(y) = l(y) + l(y)^{2^k}$ is injective from $\ker(L_b)$ to $\mathbb{F}_{2^n}$ because for any $y \in \ker(L_b)$ we have found an expression of y in terms of elements in the image of λ. So we have that $|\ker(L_b)| = |\mathrm{im}(\lambda)|$ is either 1 or 2^t when n/t is odd and either 1, 2^t or 2^{2t} when n/t is even.

We now use the fact that F is differentially two-valued with differential uniformity 2^t. If n/t is odd, then $|\mathcal{W}_F(a, b)|$ is at most $2^{\frac{n+t}{2}}$ and by applying [14, Theorem 6], we can conclude that the Fourier spectrum of F is $\{0, \pm 2^{\frac{n+t}{2}}\}$. Finally, for n/t even we claim that $|\ker(L_b)| \neq 2^t$ for all $b \neq 0$. Let us fix $b \neq 0$. Since F has the form (3), the map

$$H_b(x, y) = \mathrm{Tr}_t^n\big(b(F(x + y) + F(x) + F(y))\big)$$

is an alternating $\mathbb{F}_{2^t}$-bilinear form and $\ker(L_b)$ is the radical of H_b. By Lemma 3.2, we have that

$$\dim_{\mathbb{F}_{2^t}} \ker(L_b) = \frac{n}{t} \equiv 0 \pmod 2.$$

In particular, $|\ker(L_b)| \neq 2^t$. We can exclude the spectrum $\{0, \pm 2^{\frac{n+2t}{2}}\}$ by [14, Theorem 8] because if F does not have bent components, then it must have spectrum $\{0, \pm 2^{\frac{n+t}{2}}\}$ instead, but we have shown that $|\ker(L_b)| \neq 2^t$ for all $b \neq 0$. Consequently, when n/t is even, the Walsh spectrum is of the form $\{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2t}{2}}\}$. □

3.3 F is not a permutation? A computational report

In the case n/t even, given the form of the Walsh spectrum resulting from Proposition 3.3, we can draw the conclusion that F cannot be a permutation. The condition n/t odd (or k/t odd) is therefore a necessary condition for F to be bijective. Unfortunately, through our computational experiments we have discovered that it is not a sufficient condition, unlike the binomial case discussed in [6].

Using MAGMA code, we tested for all triples (k, s, t) where $k \leq 10$. We also attempted, but could not finish, computations for $k = 11$. In all experiments we assumed that k/t is odd, which is a necessary, but unfortunately not a sufficient condition for our case.

For each triple, we conducted 100 tests for each of the three following cases:

Test 1: $v = 0, w \in \mathbb{F}_{2^k}^*$.

Test 2: $w = 0, v \in \mathbb{F}_{2^k}^*$.

Test 3: $v, w \in \mathbb{F}_{2^k}^*$, with $vw \neq 1$.

The case $v = w = 0$ is covered in [6], where it is proven that the binomials appearing are permutations when k/t is odd.

Based on our findings, we believe that F is a permutation if and only if one of the following two conditions holds:

1. $v = w = 0$, where we have the binomial case studied in [6].
2. $t = k$ and $s \equiv 2k (\mathrm{mod} n)$, where F is a monomial of the form $cx^{2^{-k}+1}$ for some nonzero coefficient c.

We should note here that, due to computational limitations, we tested sampled functions F not satisfying Condition 2 only for $t \leq 2$. Since k is not divisible by 3, the same is true for t. For $t = 4$, the first case where the second condition does not hold occurs for $k = 20$, while for $t = 5$ we must go up to $k = 25$.

4 Conclusion

In this paper, we prove differential and linear properties of a family of quadrinomials obtained as a generalization of a known family of APN functions [4]. We also discuss permutation properties of this family. Our computational and theoretical data show that, with the exception of the trivial cases (when F is a binomial or a monomial), these functions are most likely never permutations.

Use of AI The authors used ChatGPT (OpenAI, GPT-6) to proofread the manuscript. No AI tools were used to generate computational data or develop mathematical proofs. The authors assume full responsibility for the accuracy and integrity of the scientific content presented in this work.

Acknowledgments Enrico Piccione is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. Lilya Budaghyan and Alexander Kholosha are funded by Norges forskningsråd (NFR, Research Council of Norway) under the FRIPRO programme - Cryptographic Elements of Trustworthy AI - 353785. Additionally, Lilya Budaghyan is funded by the LEAD AI programme at the University of Bergen, co-funded by the European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie grant agreement no. 101126560.

References

[1] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. Determining the nonlinearity of a new family of apn functions. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 72–79, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[2] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. *Finite Fields and Their Applications*, 14(3):703–714, 2008.

[3] 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.

[4] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire. A few more quadratic APN functions. *Cryptography and Communications*, 3(1):43–53, 05 2011.

[5] Carl Bracken and Gregor Leander. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. *Finite Fields and Their Applications*, 16(4):231–242, 2010.

[6] Carl Bracken, Chik How Tan, and Yin Tan. Binomial differentially 4-uniform permutations with high nonlinearity. *Finite Fields and Their Applications*, 18(3):537–546, 2012.

[7] Carl Bracken and Zhengbang Zha. On the Fourier spectra of the infinite families of quadratic APN functions. *Advances in Mathematics of Communications*, 3(3):219–226, 2009.

[8] Lilya Budaghyan, Claude Carlet, and Gregor Leander. Two classes of quadratic APN binomials inequivalent to power functions. *Information Theory, IEEE Transactions on*, 54:4218 – 4229, 10 2008.

[9] 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, 07 2006.

[10] Claude Carlet. *Vectorial Boolean Functions for Cryptography*, chapter 9, page 398–470. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010.

[11] Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

[12] Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.

[13] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 356–365, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[14] Pascale Charpin and Jie Peng. New links between nonlinearity and differential uniformity. *Finite Fields and Their Applications*, 56:188–208, 2019.

[15] Diana Davidova and Nikolay Kaleyski. Generalization of a class of APN binomials to Gold-like functions. In *International Workshop on the Arithmetic of Finite Fields*, pages 195–206. Springer, 2021.

[16] John F. Dillon. Almost perfect nonlinear polynomials: An update. Invited Talk at the 9th International Conference on Finite Fields and Their Applications (Fq9), July 2009.

[17] Yves Edel, Gohar M. M. Kyureghyan, and Alexander Pott. A new APN function which is not equivalent to a power mapping. *IEEE Transactions on Information Theory*, 52:744–747, 2006.

[18] Lukas Kölsch, Björn Kriepke, and Gohar M Kyureghyan. Image sets of perfectly nonlinear maps. *Designs, Codes and Cryptography*, 91(1):1–27, 2023.

[19] Lukas Kölsch and Alexandr Polujan. Value distributions of perfect nonlinear functions. *Combinatorica*, 44(2):231–268, 2024.

[20] Lukas Kölsch and Alexandr Polujan. The combinatorial structure and value distributions of plateaued functions. *Journal of Cryptology*, 39(2):21, 2026.

[21] Yongqiang Li and Mingsheng Wang. Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2m}}$ from quadratic APN permutations over $\mathbb{F}_{2^{2m+1}}$. Cryptology ePrint Archive, Paper 2011/642, 2011.

[22] Longjiang Qu, Hai Xiong, and Chao Li. A negative answer to Bracken–Tan–Tan's problem on differentially 4-uniform permutations over $\mathbb{F}_{2^n}$. *Finite Fields and Their Applications*, 24:55–65, 2013.