On the Properties of the Ortho-Derivatives of Quadratic Functions

Alain Couvreur, Anne Canteaut, Léo Perrin

On the Properties of the Ortho-Derivatives of Quadratic Functions

Alain Couvreur[1,2], Anne Canteaut[1], Léo Perrin[1]

[1] Inria, France
[2] LIX, CNRS UMR 7161, École Polytechnique,
Institut Polytechnique de Paris, France
{anne.canteaut, alain.couvreur, leo.perrin}@inria.fr

Abstract. Quadratic APN vectorial functions are under intense scrutiny due to their role e.g. in the big APN problem. Recently, a new tool has emerged to investigate their differential properties: the ortho-derivative. We present new results about this object. We first generalize it as a family of functions that can be defined for any quadratic function, even if not APN. We highlight a relation between the preimages sets of the ortho-derivative and the set of bent components, and between the ortho-derivative and some EA-invariants recently introduced by Kaleyski. We also show it is possible to reconstruct a quadratic function given its ortho-derivative.
In the APN case, we prove that its algebraic degree is always at most equal to $n-2$ using a previously unknown relation between the ortho-derivatives and cofactor matrices.

Keywords: Boolean Functions · Quadratic · APN · Ortho-derivative

1 Introduction

Let $\mathbb{F}_2 = \{0,1\}$ be the field with two elements and $n > 0$ be an integer. We use $x \cdot y = \sum_{i=0}^{n-1} x_i y_i$ to denote the scalar product of two elements of $\mathbb{F}_2^n$. The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are *Boolean functions*, and those mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are *vectorial Boolean functions*. In this article, we only consider the case where $m = n$. We let $\mathcal{F}_n$ denote the set of all functions from $\mathbb{F}_2^n$ to itself. Each of the coordinates of a vectorial Boolean function has a unique representation as a polynomial of n variables in $\mathbb{F}_2$ called its *algebraic normal form*. The degree of this representation is the *algebraic degree* of the Boolean function, and the algebraic degree of a function of $\mathcal{F}_n$ is the maximum algebraic degree of its coordinates.

A linear combination of some coordinates is a *component*, and the distance between a component $x \mapsto b \cdot F(x)$ and a linear function $x \mapsto a \cdot x$ is given by the *Walsh coefficient* $\mathcal{W}_F(a,b) = \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b \cdot F(x)}$. The maximum of $|\mathcal{W}_F(a,b)|$ taken over all $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2^n \backslash \{0\}$ is the *linearity* of F, denoted $\mathcal{L}(F)$.

The *derivative* of a vectorial Boolean function F is defined for any $a \in \mathbb{F}_2^n$ and is the function $\Delta_a F$ mapping x to $F(x+a)+F(x)$. The number of solutions x of

the equation $\Delta_a F(x) = b$ is denoted by $\delta_F(a, b)$ and its maximum, taken over all $a \neq 0$ and all b in $\mathbb{F}_2^n$, is called the differential uniformity [19] of the function F and is denoted by u_F. When $u_F = 2$, we say that F is *Almost Perfect Nonlinear (APN)*. The existence of APN permutations when n is even is an open problem (known as *the* big APN problem), except when $n = 6$ where a sporadic solution was found by Dillon *et al.* [6].

A function $F \in \mathcal{F}_n$ is a collection of n *coordinates*, each being a Boolean function mapping $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Each of these coordinates has a unique representation as a polynomial of n variables in $\mathbb{F}_2$ called its *algebraic normal form*. Its degree is the *algebraic degree* of the Boolean function, and the algebraic degree of a function of $\mathcal{F}_n$ is the maximum algebraic degree of its coordinates.

Let $F \in \mathcal{F}_n$ be a quadratic APN function. Then there exists a unique function $\pi_F \in \mathcal{F}_n$ such that $\pi_F(0) = 0$, $\pi_F(a) \neq 0$ for $a \neq 0$, and

$$\text{for any } \ (a, x) \in (\mathbb{F}_2^n)^2, \ \pi_F(a) \cdot \big(F(x) + F(x + a) + F(0) + F(a)\big) = 0. \qquad (1)$$

Functions corresponding to such π_F have been studied before [3,20,17,13,14,11], and π_F was called the *ortho-derivative of* F in [8]. In that paper, the authors showed that the ortho-derivative was a powerful tool to investigate the CCZ- and EA-equivalence of quadratic APN functions, as shown by its later use in [2,21].

In this article, we present some new results on the ortho-derivative. First, we generalize it to any quadratic function, and in particular to non-APN ones (Section 2). The non-trivial ortho-derivatives of a quadratic function F then form a family of functions that reduces to a single function if and only if F is APN. We then discuss the algebraic degree of ortho-derivatives, and in particular prove that this degree is at most equal to $n - 2$ for APN functions (Section 3).

We then shift our focus to more practical aspects. First, we prove that some EA- and CCZ-invariants introduced in [7,16] can be derived from the Hamming weight of the ortho-derivative in the case of quadratic APN functions. Then, we show that it is possible to define and to implement an operation that is the inverse of ortho-derivation, namely the *ortho-integration* (Section 4).

2 The Ortho-Derivatives of any Quadratic Function

We first recall the definition of the ortho-derivative, generalize it to any quadratic function, and describe some basic properties (Section 2.1). Then, we investigate the values an ortho-derivative can take, and highlight some simple relations between those and the Walsh spectrum of the function in Section 2.2.

2.1 Definition and Basic Properties

Definition 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function. We say that $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an* ortho-derivative for F *if, for any x and a in $\mathbb{F}_2^n$,*

$$\pi(a) \cdot \big(F(x) + F(x + a) + F(0) + F(a)\big) = 0 \, .$$

The set of all ortho-derivatives for a given F is denoted by $\Pi(F)$.

It is worth noting that $\Pi(F)$ always contains several ortho-derivatives since $\pi(0)$ can take any value and, for any $a \neq 0$, 0 is a valid value for $\pi(a)$. Therefore, we say in the following that an ortho-derivative $\pi \in \Pi_F$ is *non-trivial* if $\pi(0) = 0$ and $\pi(a) \neq 0$ for all nonzero a.

Among all quadratic functions, APN functions are characterized by the fact that they have a single non-trivial ortho-derivative. More generally, the number of ortho-derivatives depends on the differential spectrum of the quadratic function. In order to establish this, we need the following properties (the proof is omitted due to the page-count limitation).

Proposition 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function. For any nonzero $a \in \mathbb{F}_2^n$, we define*

$$P_F(a) = \{x : \exists \pi \in \Pi(F) \text{ with } \pi(a) = x\}.$$

Then, for any $a \in \mathbb{F}_2^n$, $P_F(a)$ is a linear space and $\#P_F(a) = \max_{b \in \mathbb{F}_2^n} \delta_F(a, b)$. Moreover,

$$\#\{(a, b) : \pi(a) = b \text{ for some } \pi \in \Pi(F)\} = 2^{-n} \sum_{a,b \in \mathbb{F}_2^n} \delta_F(a, b)^2.$$

We can then easily establish a link between the APN property and the number of ortho-derivatives.

Corollary 1. *Let $F \in \mathcal{F}_n$ be a quadratic function. Then, the following conditions are equivalent:*

(i) *F is APN.*
(ii) *There exists a unique nontrivial $\pi \in \Pi(F)$.*
(iii) *$\#\{(a, b) : \pi(a) = b \text{ for some } \pi \in \Pi(F)\} = 2^n + 2(2^n - 1)$.*

If we do not assume that F is quadratic, a similar characterization holds for generalized crooked functions (see Definition 4.2 in [9]).

2.2 On the values an ortho-derivative can take

In the following, we study the set

$$\mathcal{S} = \{(a, b) : \pi(a) = b \text{ for some } \pi \in \Pi(F)\} .$$

This set can be partitioned into linear spaces $P_F(a)$ whose dimensions are determined by the differential spectrum of F. The existence of vector space partitions with a given *type*, i.e., such that the dimensions of the involved vector spaces are given, is a well-known problem studied by many authors, see [15] for a survey.

We can also partition the same set according to the values of b, i.e. into sets

$$T_F(b) = \{a : \exists \pi \in \Pi(F) \text{ with } \pi(a) = b\}.$$

This provides another partition of $\mathcal{S}$ into vector spaces, as already established by Gorodilova in [14].

Proposition 2. *Let $F \in \mathcal{F}_n$ be a quadratic function. For any $b \in \mathbb{F}_2^n$, we define*

$$T_F(b) = \{a : \exists \pi \in \Pi(F) \text{ with } \pi(a) = b\} .$$

Then, $T_F(b) = \mathsf{LS}(F_b)$ where $\mathsf{LS}(F_b)$ denotes the set of all linear structures of the component $x \mapsto b \cdot F(x)$. It follows that, for any b, $T_F(b)$ is a linear subspace of $\mathbb{F}_2^n$ whose dimension has the same parity as n.

We deduce that the partition of $\mathcal{S}$ into $T_F(b), b \in \mathbb{F}_2^n$ is derived from the Walsh spectrum of F, while the partition into $P_F(a), a \in \mathbb{F}_2^n$ corresponds to its differential spectrum.

Proposition 3. *Let $F \in \mathcal{F}_n$ be a quadratic function. Then, for any of its nontrivial component F_b, we have $\mathcal{L}(F_b) = 2^{\frac{n+\dim T_F(b)}{2}}$.*

We then easily recover the characterization of APN functions from their Walsh spectrum (see e.g [4, Corollary 1]):

$$\sum_{\mu \neq 0} \sum_{\lambda \in \mathbb{F}_2^n} \mathcal{W}_F^4(\lambda, \mu) = (2^n - 1)2^{3n+1} .$$

Indeed, Proposition 3 combined with Corollary 1 leads to the following equivalent formulation.

Corollary 2. *Let $F : \mathcal{F}_n$ be a quadratic function and, for any $d, 0 \leqslant d \leqslant n$,*

$$\begin{aligned} B_d &= \#\{b \neq 0 : \mathcal{L}^2(F_b) = 2^{n+d}\} \\ &= \#\{b \neq 0 : b \text{ has } 2^d \text{ preimages by some } \pi \in \Pi(F)\} . \end{aligned}$$

Then, $\sum_{d=1}^n B_d(2^d - 1) \geqslant 2^n - 1$, with equality if and only if F is APN.

Proof. Recall that $\pi(0)$ can take any value, and that $\pi(a) = 0$ is a valid value for any a. Let $\widetilde{B_d} = \#\left\{b : b \text{ has } 2^d \text{ preimages by some } \pi \in \Pi(F)\right\}$, and consider the set $\mathcal{S} = \{(a, b) : \pi(a) = b \text{ for some } \pi \in \Pi(F)\}$. Then, the size of $\mathcal{S}$ is given by $\sum_b T_F(b) = \sum_{d=0}^n \widetilde{B_d} 2^d$. Using that $\mathcal{L}(F_0) = 2^n$, we get $\sum_{d=0}^n \widetilde{B_d} 2^d = \sum_{d=0}^n B_d 2^d + 2^n$. Moreover,

$$\sum_{d=0}^n B_d 2^d = \sum_{d=0}^n B_d(2^d - 1) + \sum_{d=0}^n B_d = \sum_{d=1}^n B_d(2^d - 1) + (2^n - 1) .$$

It follows that $\#\mathcal{S} = \sum_{d=1}^n B_d(2^d - 1) + 2^{n+1} - 1$. From Corollary 1, we know that $\#\mathcal{S} \geqslant 2^n + 2(2^n - 1)$ with equality if and only if F is APN. Equivalently, $\sum_{d=1}^n B_d(2^d - 1) \geqslant 2^n - 1$ with equality if and only if F is APN. □

2.3 Relations between the properties of a function and those of its ortho-derivative

n odd. When n is odd, all $T_F(b)$ have an odd dimension, implying that they can never have dimension zero. Then, if F is APN, we have that $B_1 = 2^n - 1$, or equivalently that the only nontrivial π is a permutation. It follows that F is almost bent, as proved in [10].

n even. When n is even, the values taken by $(B_0, \ldots, B_n)$ are not unique. Some conditions on B_0 can be deduced from Corollary 2.

Corollary 3. *Let $n \geqslant 4$ be an even integer and $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function. Let B_0 denote the number of bent components of F. Then $B_0 \geqslant 2 \times \frac{(2^n-1)}{3}$, with equality if and only if $B_2 = \frac{(2^n-1)}{3}$ and all other B_d vanish.*
Moreover, $B_0 \equiv 2 \bmod 4$, and $B_n = 0$.

Proof. The first statement corresponds to Corollary 3 in [4]. It is a straightforward consequence of $\sum_{d=1}^{n} B_d(2^d - 1) = 2^n - 1$, where $B_d = 0$ for all odd d. Therefore

$$2^n - 1 \geqslant 3\left(\sum_{d=2}^{n} B_d\right) = 3(2^n - 1 - B_0),$$

leading to $B_0 \geqslant 2 \times (2^n - 1)/3$ with equality if and only if $B_d = 0$ for all $d > 2$.

Also, from

$$\sum_{d=2}^{n} B_d(2^d - 1) \;=\; \sum_{d=2}^{n} B_d 2^d - \sum_{d=2}^{n} B_d = 2^n - 1,$$

we deduce that

$$4\sum_{d=2}^{n} B_d 2^{d-2} - (2^n - 1 - B_0) \;=\; 2^n - 1$$

which implies that $B_0 \equiv 2 \bmod 4$. We can also use the same characterization to prove that a quadratic APN function cannot have linearity 2^n. Indeed, if $B_n > 0$, then the only possibility is $B_n = 1$ and $B_0 = 2^n - 2$. Let us assume w.l.o.g that the component of F with linearity 2^n corresponds to the last coordinate. Then, the function F' from $\mathbb{F}_2^n$ into $\mathbb{F}_2^{n-1}$ derived from F by removing the last coordinate is bent, i.e. all its components are bent. However, bent functions only exist if the number of outputs is at most half of the number of inputs, i.e. $n - 1 \leqslant \frac{n}{2}$ [18]. This cannot occur if $n \geqslant 4$. □

The previous corollary shows that, for any quadratic APN function F, $\mathcal{L}(F) \leqslant 2^{n-1}$. It is worth noticing that such quadratic APN functions have been exhibited for $n = 6, 8$. All classes of quadratic APN functions of 6 variables have the lowest possible value of B_0, i.e. $B_0 = 42$, except one which satisfies

$$B_0 = 46,\ B_2 = 16 \text{ and } B_4 = 1\ .$$

For $n = 8$ variables, the quadratic APN functions exhibited in [22,2,1] have six different spectra corresponding to the following $(B_d)_{d \leqslant n}$:

$B_0 = 170,\ B_2 = 85,$
$B_0 = 174,\ B_2 = 80,\ B_4 = 1,$
$B_0 = 178,\ B_2 = 75,\ B_4 = 2,$
$B_0 = 182,\ B_2 = 70,\ B_4 = 3,$
$B_0 = 186,\ B_2 = 65,\ B_4 = 4,$
$B_0 = 190, B_2 = 64, B_4 = 0, B_6 = 1.$

Thanks to Corollary 2, we can deduce some properties of the differential spectrum of the ortho-derivative π_F from the Walsh spectrum of a quadratic APN function F.

Corollary 4. *Let $F \in \mathcal{F}_n$ be a quadratic APN function, π_F be its nontrivial ortho-derivative, and B_d be the number of components of F with squared linearity 2^{n+d}. Then, for all d, we have that at least $B_d(2^d-1)$ entries in the DDT of π_F are greater than or equal to 2^d-2. In particular,*

$$B_d > 0 \implies u_{\pi_F} \geqslant 2^d - 2 \ .$$

For instance, it can be checked that the nontrivial ortho-derivative of the previously mentioned 8-bit APN function with $B_6 = 1$ has differential uniformity 62. The converse statement of this corollary is false: there are 8-bit APN functions with an ortho-derivative with a differential uniformity of 30 but for which $B_d = 0$ for all $d \geqslant 3$, whereas a true converse statement would have implied that $B_4 > 0$.

3 On the degree of the ortho-derivative(s)

In [14], Gorodilova studied the ortho-derivatives of quadratic APN functions and identified several of their properties. In particular, she proved that the algebraic degree of a nontrivial ortho-derivative is either n or at most $n-2$, and as an immediate corollary, that the nontrivial ortho-derivative is of degree at most $n-2$ when n is odd (because then the ortho-derivative is a permutation).

In the case where n is even, she could only conjecture that all nontrivial components of the ortho-derivative have algebraic degree exactly equal to $n-2$ (Conjecture 2 of [14]). In this section, we show that a nontrivial ortho-derivative of an APN function is always of degree at most $n-2$.

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic APN function. We define J as the function mapping an element of $\mathbb{F}_2^n$ to the binary $n \times n$ matrix such that, for all $x \in \mathbb{F}_2^n$, $J_{i,j}(x) = \Delta_{e_j} F_i(x) + \Delta_{e_j} F_i(0)$. If F is quadratic, then J is the linear part of its Jacobian matrix. From [8, Prop. 14], we know that, for every x and a,

$$J(x) \times a = J(a) \times x = \Delta_a F(x) + \Delta_a F(0) \ . \tag{2}$$

As established in [8], F is APN if and only if $\mathrm{Rank}(J(a)) = n-1$ for all $a \neq 0$. It is a direct consequence of the fact that a function is APN if and only if the image of $\Delta_a F$ is of dimension $n-1$. We deduce that both the left and the right kernels of $J(a)$ contain a single non-trivial element. First, we remark that Equation (2) immediately implies

$$J(a) \times a \ = \ \Delta_a F(a) + \Delta_a F(0) = F(a+a) + F(a) + F(a+0) + F(0) = 0 \ ,$$

meaning that the right kernel of $J(a)$ is $\{0, a\}$. On the other hand, for any $c \in \mathbb{F}_2^n$, we have that $c^T J(a) x$ is the scalar product of c with an element in the image of $\Delta_a F$. Let π be the nontrivial ortho-derivative of F. By definition, we then have

$\pi(a)^T J(a)x = 0,\ \forall x \in \mathbb{F}_2^n$. We deduce that $\pi(a)^T J(a) = 0$, meaning that the left kernel of $J(a)$ consists of $\{0, \pi(a)^T\}$.

For any $n \times n$ binary matrix M, we denote $\mathsf{Cof}(M)$ its cofactors matrix:

$$\mathsf{Cof}(M) = \begin{bmatrix} \det(C_{0,0}) & \cdots & \det(C_{0,n-1}) \\ \vdots & & \vdots \\ \det(C_{n-1,0}) & \cdots & \det(C_{n-1,n-1}) \end{bmatrix} ,$$

where $\det(C_{i,j})$ is the (i,j) minor of M, *i.e.* the determinant of the submatrix obtained by removing Row i and Column j from M. Furthermore, it is well-known that

$$\mathsf{Cof}(M)^T M \ = \ M\mathsf{Cof}(M)^T \ = \ \mathrm{Id} \times \det(M) \ .$$

Let us apply this equality to $J(a)$. As it is of rank $n-1 < n$, we have that

$$\mathsf{Cof}(J(a))^T J(a) = J(a)\mathsf{Cof}(J(a))^T = 0 \ . \tag{3}$$

Lemma 1. *The cofactors matrix of $J(a)$ can be written*

$$\mathsf{Cof}\left(J(a)\right) \ = \ \begin{bmatrix} \pi_0(a)a_0 & \cdots & \pi_0(a)a_{n-1} \\ \vdots & & \vdots \\ \pi_{n-1}(a)a_0 & \cdots & \pi_{n-1}(a)a_{n-1} \end{bmatrix} \ = \ \begin{bmatrix} \pi_0(a) \\ \vdots \\ \pi_{n-1}(a) \end{bmatrix} [a_0, \ldots, a_{n-1}] \ .$$

Proof. As we have established, the right kernel of $J(a)$ contains only 0 and a. This implies that the row space of $\mathsf{Cof}(J(a))$ is contained in $\{0, a\}$. On the other hand, since the left kernel of $J(a)$ is $\{0, \pi(a)\}$, we have that the column space of $\mathsf{Cof}(J(a))$ must be contained in that space.

Since $J(a)$ has rank $n-1$, it has at least one nonzero minor. Hence, its cofactor matrix is nonzero. Thus, the only possibility is $\mathsf{Cof}(J(a)) = \pi(a) \cdot a^T$. □

A direct corollary of this lemma is that each minor of $J(a)$ is equal to $\det(C_{i,j}) = \pi_i(a)a_j$.

Since F is quadratic, the entries in $J(a)$ are linear functions in a. Next, from Leibniz' formula on an $(n-1) \times (n-1)$ binary matrix M:

$$\det(M) = \sum_{\sigma \in \mathfrak{S}_{n-1}} \prod_{i=0}^{n-2} m_{i,\sigma(i)} \ , \tag{4}$$

we deduce that the degree of each entry in $\mathsf{Cof}(J(a))$ is a Boolean function of degree at most $n-1$ in a as it is a sum of products of $n-1$ linear functions.

We deduce that $\deg(\pi_i(a)a_j)$ is at most $n-1$, for all j. Indeed, suppose that there exists a term of degree $n-1$ in the ANF of π_i for some i, and that it corresponds to $\prod_{k \neq j} a_k$. Then the entry at position (i,j) in the cofactors matrix $\mathsf{Cof}(J(a))$ would be a function of degree n, which is impossible. The next theorem follows.

Theorem 1. *If π is the nontrivial ortho-derivative of a quadratic APN function of $\mathbb{F}_2^n$, then* $\deg(\pi) \leqslant n-2$.

Corollary 5. *Let $F \in \mathcal{F}_n$ be a quadratic function. Then it is not APN if and only if at least one of its nontrivial ortho-derivatives is of algebraic degree n.*

4 On Ortho-Integration

We call *ortho-integration* the process that is the inverse of ortho-derivation.

Definition 2 (Ortho-Integral). *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic function, and let $\Pi(F)$ be the set of its ortho-derivatives. For all $\pi \in \Pi(F)$, we say that F is an* ortho-integral *of π.*

An ortho-integral is not unique: for any affine function A of $\mathbb{F}_2^n$, F and $F+A$ have the same ortho-derivatives. This does not necessarily imply that their DDTs are identical, though it is worth noting that all known examples of APN functions with the same DDT differ from an affine function [5,13]. In general, it is unclear whether there exists other "collisions", i.e. distinct functions with identical ortho-derivatives.

Recall that, for any π in $\Pi(F)$ and any $x \in \mathbb{F}_2^n$, it holds that $\pi(a)^T J(a) x = 0$. Since this equation is linear in x for all a, it is sufficient to consider elements x in a basis of $\mathbb{F}_2^n$. Then, recovering $J(a)$ for all a can be achieved by solving a linear system with $n(2^n-1)$ equations (one per basis vector and per value $a \neq 0$) and $n\binom{n}{2}$ unknowns in $\mathbb{F}_2$, each modeling the presence of a specific degree 2 product in a specific output coordinate.

We have implemented such an algorithm and included it in `sboxU`.[3] Using it, we could verify that the ortho-derivative of F where F is any of the known quadratic APN functions on 6, 7, and 8 bits has a single ortho-integral (up to the addition of an affine function), namely F itself. Computing all the ortho-integrals of 25,624 8-bit quadratic APN functions takes about 20min on a regular desktop computer, meaning roughly half a second per function.

5 Relation with some EA- and CCZ-Invariants

Kaleyski and his coauthors, motivated by two different problems, introduced several invariants for Sboxes in [7] and [16]. The CCZ-invariant presented in [7], called *distance invariant*, applies to APN functions and provides a lower bound on the distance between two APN functions. It has a simplified form in the case of quadratic APN functions. It is observed that this CCZ-invariant takes many distinct values for APN functions in dimension 8, while it takes the same value for all APN functions in dimension 7 constructed in [12]. *Zero-sum invariants* are EA-invariant presented in [16], and are denoted by $\Sigma_k^F(0)$. It turns out that

[3] `https://github.com/lpp-crypto/sboxU`, see in particular file `quadratic.py` starting from line 62.

they are closely related to ortho-derivatives, as we will see below. First, we recall both definitions.

Proposition 4 (Zero-sum invariants [16]). *Let $\Sigma_k^F(t)$ be the multiset defined by $\Sigma_k^F(t) = \left\{\sum_{i=1}^k F(x_i) : x_1 + \cdots + x_k = t\right\}$. Then, for any $G = A_1 \circ F \circ A_2 + A_3$, where A_1 and A_2 are affine permutations and A_3 an affine function, we have*

$$\Sigma_k^G(0) = \begin{cases} \{A_1(s) + A_1(0) : s \in \Sigma_k^F(0)\} & \text{if } k \text{ is even} \\ \{A_1(s) + A_3(0) : s \in \Sigma_k^F(A_2(0))\} & \text{if } k \text{ is odd.} \end{cases}$$

It follows that the multiplicities of the elements in $\Sigma_k^F(0)$, i.e. the values $M_k^F(s) = \#\{(x_1, \ldots, x_k) : x_1 + \cdots + x_k = 0 \text{ and } \sum_{i=1}^k F(x_i) = s\}$ where $s \in \mathbb{F}_2^n$ are an EA-invariant for any even k. The same property holds for odd k if A_2 is linear.

Proposition 5 (Distance invariant [7]). *Let Φ_F be the multiset defined as $\Phi_F = \{\phi_F(b, c) : b, c \in \mathbb{F}_2^n\}$ where*

$$\phi_F(b, c) = \#\{a \in \mathbb{F}_2^n : \exists x \in \mathbb{F}_2^n,\ F(x) + F(x + a) + F(a + c) = b\}\ .$$

Then Φ_F is invariant under CCZ-equivalence. Moreover, if F is quadratic, then Φ_F is equal to the multiset $\Phi_F^0 = \{\phi_F(b, 0) : b \in \mathbb{F}_2^n\}$ where each element is repeated 2^n times.

In the case of quadratic functions, and when $k = 4$, it holds that these invariants are related with each other, and with the ortho-derivative. To establish this, we first re-write the definition of $M_4^F(s)$ and obtain the following lemma.

Lemma 2. *It holds that $M_4^F(s) = \#\{(x, a, b) : \Delta_a\Delta_b F(x) = s\}$.*

The following proposition then links $M_4^F(s)$ to $\phi_F(s, 0)$, i.e. it links the zero-sum invariant to the distance invariant.

Proposition 6. *F is APN if and only if $M_4(0) = 2^{2n+1} + 2^{2n} - 2^{n+1}$. Moreover, if $\deg F = 2$,*

$$M_4^F(s) = 2^n \#\{(a, b) : \Delta_a\Delta_b F(0) = s\},$$

and if F is a quadratic APN function with $F(0) = 0$, then for any nonzero $s \in \mathbb{F}_2^n$ we have $\phi_F(s, 0) = 2^{-(n+1)} M_4^F(s)$.

Proof. Because of Lemma 2, $M_4^F(s) = \#\{(x, a, b) : \Delta_a\Delta_b F(x) = s\}$.

APN functions are characterized by the fact that their second-order derivatives $\Delta_b\Delta_a F(x)$ never take the value 0 unless $\langle a, b\rangle$ does not form a 2-dimensional vector space, which occurs if $a = 0$, or $b = 0$ or $a = b$, *i.e.* $2(2^n - 1) + 2^n = 3 \times 2^n - 2$ times. For each such case, $\Delta_a\Delta_b F$ is the all-zero function, implying that

$$M_4^F(0) \geqslant 2^{2n+1} + 2^{2n} - 2^{n+1}\ ,$$

with equality if and only if F is APN.

When F is quadratic, all its second-order derivatives are constant, implying that $\Delta_b\Delta_a F(x)$ takes the same value for all $x \in \mathbb{F}_2^n$. Moreover, if $F(0) = 0$, then

$$\phi_F(s, 0) = \#\{a \in \mathbb{F}_2^n : \exists b \in \mathbb{F}_2^n, \Delta_a F(b) + \Delta_a F(0) = s\} .$$

Then, if F is a quadratic APN function, each function $b \mapsto \Delta_a F(b) + \Delta_a F(0)$ is a linear 2-to-1 function when $a \neq 0$, which implies that, for any $s \neq 0$,

$$\begin{aligned} 2^{-n} M_4^F(s) &= \#\{(a, b) : \Delta_a F(b) + \Delta_a F(0) = s\} \\ &= 2\#\{a : \exists b \in \mathbb{F}_2^n, \Delta_a F(b) + \Delta_a F(0) = s\} . \end{aligned}$$

Up to a factor 2^{n+1}, the values in Φ_F^0 then correspond to the values $M_4^F(s)$ when s varies in $\mathbb{F}_2^n \setminus \{0\}$. □

We are now ready to describe the connection between the invariants of Kaleyski and the ortho-derivative. It is described by the following proposition.

Proposition 7. *Let F be a quadratic APN function, and π be its nontrivial ortho-derivative. Then, for any $s \in \mathbb{F}_2^n \setminus \{0\}$, $M_4^F(s) = 2^{n+1}(2^n - 1 - wt(\pi_s))$ where π_s denotes the component function $x \mapsto s \cdot \pi(x)$. Most notably, if n is odd, then π is a permutation, which implies the following equivalent statements:*

$$M_4^F(s) = \begin{cases} 2^{2n+1} + 2^{2n} - 2^{n+1} & \text{if } s = 0 \\ 2^{2n} - 2^{n+1} & \text{if } s \neq 0 \end{cases}, \quad \phi_F(b, 0) = \begin{cases} 2^n & \text{if } b = 0 \\ 2^{n-1} - 1 & \text{if } b \neq 0 . \end{cases}$$

Proof. By definition of π, when F is a quadratic APN function, for any nonzero $a \in \mathbb{F}_2^n$, the image set of $b \mapsto \Delta_a\Delta_b F(0)$ is the hyperplane composed of all elements orthogonal to $\pi(a)$. It follows that, when $s \neq 0$,

$$\begin{aligned} M_4^F(s) &= 2^n\#\{(a, b) : \Delta_a\Delta_b F(0) = s\} = 2^n\#\{(a, b), a \neq 0 : \Delta_a\Delta_b F(0) = s\} \\ &= 2^{n+1}\#\{a \neq 0 : s \in \langle \pi(a) \rangle^{\perp}\} = 2^{n+1}\#\{a \neq 0 : s \cdot \pi(a) = 0\} \\ &= 2^{n+1}(2^n - 1 - wt(\pi_s)) . \end{aligned}$$

□

Thus, for quadratic APN functions, up a to simple transformation, the multiset $\{M_4^F(s) : s \neq 0\}$ (and the equivalent invariant Φ_F^0) used in [7,16] is included in the multiset formed by the Walsh spectrum of the ortho-derivative.

6 Conclusion

The practical usefulness of the ortho-derivative was established in [8], and then confirmed in [2] and [21]. In this work, we have shed some more light on the properties of this object, and in particular established an upper bound on its degree. We also showed how to obtain a function given its ortho-derivative, which begs the question: what makes a function an ortho-derivative? It indeed remains an open problem to find other properties to efficiently determine whether a given function may be an ortho-derivative, since such a result could now allow us to construct new quadratic APN functions

References

1. Beierle, C., Leander, G.: New Instances of Quadratic APN Functions in Dimension Eight (Sep 2020). https://doi.org/10.5281/zenodo.4030734, https://doi.org/10.5281/zenodo.4030734
2. Beierle, C., Leander, G.: New instances of quadratic APN functions. IEEE Trans. Inform. Theory **68**(1), 670–678 (2022). https://doi.org/10.1109/TIT.2021.3120698, https://doi.org/10.1109/TIT.2021.3120698
3. Bending, T.D., Fon-Der-Flaass, D.: Crooked functions, bent functions, and distance regular graphs. Electr. J. Comb. **5** (1998), http://www.combinatorics.org/Volume_5/Abstracts/v5i1r34.html
4. Berger, T., Canteaut, A., Charpin, P., Laigle-Chapuy, Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inform. Theory **52**(9), 4160–4170 (2006)
5. Boura, C., Canteaut, A., Jean, J., Suder, V.: Two notions of differential equivalence on sboxes. Des. Codes Cryptogr. **87**(2-3), 185–202 (2019). https://doi.org/10.1007/S10623-018-0496-Z
6. Browning, K.A., Dillon, J., McQuistan, M.T., Wolfe, A.J.: An APN permutation in dimension six. In: Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications. vol. 518, pp. 33–42. American Mathematical Society (2010)
7. Budaghyan, L., Carlet, C., Helleseth, T., Kaleyski, N.S.: On the distance between APN functions. IEEE Trans. Inform. Theory **66**(9), 5742–5753 (2020). https://doi.org/10.1109/TIT.2020.2983684, https://doi.org/10.1109/TIT.2020.2983684
8. Canteaut, A., Couvreur, A., Perrin, L.: Recovering or testing extended-affine equivalence. IEEE Trans. Inform. Theory **68**(9), 6187–6206 (2022). https://doi.org/10.1109/TIT.2022.3166692, https://doi.org/10.1109/TIT.2022.3166692
9. Canteaut, A., Naya-Plasencia, M.: Structural weaknesses of permutations with a low differential uniformity and generalized crooked functions. In: Finite fields: theory and applications, Contemp. Math., vol. 518, pp. 55–71. Amer. Math. Soc., Providence, RI (2010). https://doi.org/10.1090/conm/518/10196
10. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**(2), 125–156 (1998)
11. Charpin, P.: The crooked property. Finite Fields Appl. **81** (2022)
12. Edel, D., Pott, A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**(1), 59–81 (2009)
13. Gorodilova, A.: On the differential equivalence of APN functions. Cryptogr. Commun. **11**(4), 793–813 (2019). https://doi.org/10.1007/S12095-018-0329-Y
14. Gorodilova, A.: A note on the properties of associated boolean functions of quadratic APN functions. Прикладная дискретная математика **47**, 16–21 (2020)
15. Heden, O.: A survey of the different types of vector space partitions. Discrete Math., Alg. and Appl. **4**(1) (2012)
16. Kaleyski, N.S.: Invariants for EA- and CCZ-equivalence of APN and AB functions. Cryptogr. Commun. **13**(6), 995–1023 (2021). https://doi.org/10.1007/S12095-021-00541-8, https://doi.org/10.1007/s12095-021-00541-8
17. Kyureghyan, G.M.M.: Crooked maps in $\mathbb{F}_{2^n}$. Finite Fields Appl. **13**(3), 713–726 (2007)
18. Nyberg, K.: Perfect nonlinear S-boxes. In: Davies, D.W. (ed.) EUROCRYPT'91. LNCS, vol. 547, pp. 378–386. Springer, Heidelberg, Germany, Brighton, UK (Apr 8–11, 1991). https://doi.org/10.1007/3-540-46416-6_32

19. Nyberg, K.: Differentially uniform mappings for cryptography. In: Helleseth, T. (ed.) EUROCRYPT'93. LNCS, vol. 765, pp. 55–64. Springer, Heidelberg, Germany, Lofthus, Norway (May 23–27, 1994). https://doi.org/10.1007/3-540-48285-7_6
20. van Dam, E., Fon-Der-Flaass, D.: Codes, graphs, and schemes from nonlinear functions. European J. Combin. **24**(1), 85–98 (2003). https://doi.org/https://doi.org/10.1016/S0195-6698(02)00116-6
21. Yu, Y., Perrin, L.: Constructing more quadratic APN functions with the QAM method. Cryptogr. Commun. **14**(6), 1359–1369 (2022). https://doi.org/10.1007/S12095-022-00598-Z, https://doi.org/10.1007/s12095-022-00598-z
22. Yu, Y., Wang, M., Li, Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. **73**(2), 587–600 (Nov 2014). https://doi.org/10.1007/s10623-014-9955-3, https://doi.org/10.1007/s10623-014-9955-3