Differential uniformity and the associated codes of cryptographic functions

Pascale Charpin, Jie Peng

Differential uniformity and the associated codes of cryptographic functions

Pascale Charpin* Jie Peng†

February 8, 2019

Abstract

The associated codes of almost perfect nonlinear (APN) functions have been widely studied. In this paper, we consider more generally the codes associated with functions that have differential uniformity at least 4. We emphasize, for such a function F, the role of codewords of weight 3 and 4, and of some cosets of its associated code C_F. We give some properties on codes associated with differential uniformity exactly 4. We obtain lower bounds and upper bounds for the numbers of codewords of weight less than 5 of the codes C_F. We show that the nonlinearity of F decreases when these numbers increase. We obtain a precise expression to compute these numbers, when F is a plateaued or a differentially two-valued function. As an application, we propose a method to construct differentially 4-uniform functions, with a large number of 2-to-1 derivatives, from APN functions.

Keywords: Vectorial function, power function, derivative, Boolean function, linear code, coset of code, plateaued function, bent functions, differential uniformity, differentially two-valued function, Walsh spectrum.

1 Introduction

Differential cryptanalysis is a statistical attack for breaking iterated block ciphers which was proposed in 1991 by Biham and Shamir [2]. The efficiency

*INRIA, 2 rue Simone Iff, Paris, FRANCE

†Mathematics and Science College of Shanghai Normal University, Shanghai, CHINA

of such attack is quantified by the so-called *differential uniformity* of the substitution box (S-box). An S-box is currently represented by a vectorial function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, where $\mathbb{F}_{2^n}$ is the finite field of order 2^n. The differential uniformity of such a function F, denoted $\delta(F)$, is equal to the largest number $\delta(a,b)$ of solutions x of the equations

$$(E_{a,b}) \ : \ F(x+a)+F(x)=b, \ a \in \mathbb{F}_{2^n}^*, \ b \in \mathbb{F}_{2^n}.$$

To have a good resistance to the differential attack, the numbers $\delta(a,b)$ must be globally low. The best value for $\delta(F)$ is 2, when every $(E_{a,b})$ has 0 or 2 solutions. In this case, F is said to be an *Almost Perfect Nonlinear* (APN) function.

Further, the associated code C_F of F was defined and its basic properties were explained in [8]. The main purpose was to describe the algebraic structure of C_F when F is an APN function or, equivalently, when C_F has minimum distance 5. It was notably proved that for odd n some APN functions, called *Almost Bent* (AB) functions, lead to *completely regular codes* (see [8, Corollary 2]).

This paper can be considered as an extension of [8], since we are interested by the full corpus of codes C_F, mainly when $\delta(F) \geq 4$. When F is not APN, the minimum distance of C_F is 3 or 4 making the codewords of weight 3 and 4 of C_F highly significant for our study. Our main purpose is to describe the set of such codewords and to establish some relations with the value of $\delta(F)$ or with special properties of F.

The paper is organized as follows. The next section gives some necessary definitions on the cryptographic properties of functions over $\mathbb{F}_{2^n}$ and basic properties of their related codes. In Section 3, we describe the links between the differential uniformity of F, the codewords of weight 3 and 4 of C_F and the cosets of C_F of minimum weight 1 and 2. In Section 4, we present specific properties of codes C_F associated to differentially 4-uniform functions. We further study the size of the set W_3 (resp. W_4) of codewords of weight 3 (resp. of weight 4). In Section 5.2, we obtain lower bounds and upper bounds for the numbers of codewords of weight less than 5 of the codes C_F. We later show that the nonlinearity of F decreases when these numbers increase. We obtain a precise expression to compute these numbers when F is a plateaued or a differentially two-valued function. Sections 6 and 7 can be seen as practical extensions. First, we are focusing on the set of 2-to-1 derivatives of any function over $\mathbb{F}_{2^n}$, providing a new method to construct differentially

4-uniform functions, which have a large number of 2-to-1 derivatives. In Section 7, we give a precise expression of the size of sets W_3 and W_4 for differentially two-valued functions and for plateaued functions.

2 Preliminaries

In this paper, some aspects of coding theory are required. A basic framework is given in Section 2.2 later. For further details, the reader can refer to [14] or to the first chapter of [17], for instance. Amongst the notations introduced in this section, some are reserved throughout this paper:
– $|E|$ is the size of any set E and $E^* = E \setminus \{0\}$;
– $N = 2^n - 1$;
– α is a primitive element of the finite field $\mathbb{F}_{2^n}$.

2.1 Notation, definitions

Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ is called a *vectorial* function over $\mathbb{F}_{2^n}$. Let F be such a function and $a \in \mathbb{F}_{2^n}^*$. Then, the function

$$D_aF : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n},\ x \mapsto F(x+a)+F(x)$$

is called *the difference function of F with respect to a*, or the *derivative* of F in direction a. Define the numbers

$$\delta(a,b) = |\{x \in \mathbb{F}_{2^n} \mid D_aF(x) = b\}|,\ b \in \mathbb{F}_{2^n}. \tag{1}$$

The *differential uniformity* of F is defined as

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

Then, F is said to be a *differentially $\delta(F)$-uniform* function. Clearly, $\delta(F)$ is an even integer. When $\delta(F) = 2$, F is said to be an *almost perfect nonlinear*, abbreviated APN, function.

The *differential spectrum* of F is the multiset consisting of integers $\delta(a,b)$ with their multiplicities. For simplicity, we will use the sequence of values

$$\omega_i = |\{(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \mid \delta(a,b) = i\}|.$$

Then it is easy to check that

$$\sum_{i=0}^{\delta(F)} \omega_i = \sum_{i=2}^{\delta(F)} i \times \omega_i = 2^n(2^n-1). \tag{3}$$

Very particular functions will appear in this paper, which could be seen as a generalization of APN functions.

Definition 1 *A function F over $\mathbb{F}_{2^n}$ is said to be differentially two-valued, if $\delta(a,b)$ takes two values only, that is $\delta(a,b) \in \{0, \delta(F)\}$ for any pair $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$.*

It is known that a differentially two-valued function F satisfies $\delta(F) = 2^s$ for some integer $s > 0$. A basic study of these functions can be found in [3, Section 5]. Little is known about the corpus of non APN such functions. We prove in this paper that some properties of differentially two-valued functions hold for quadratic functions. These results reinforce [3, Conjecture 1], claiming that such monomial functions are strongly connected with the one which are quadratic. However, note that APN functions and the inverse of differentially two-valued permutations are differentially two-valued, too. Not all differentially two-valued functions are quadratic.

The set of Boolean functions of n variables is currently denoted by B_n. Such functions, from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, will be denoted by lower case letters. Define, for any $f \in B_n$ and $a \in \mathbb{F}_{2^n}^*$,

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} \quad \text{and} \quad \varphi_a(x) = Tr(ax),$$

where Tr is the absolute trace over $\mathbb{F}_{2^n}$. The set of *Walsh coefficients* of $f \in B_n$ is

$$\mathcal{W}_f = \{\mathcal{F}(f+\varphi_a) \mid a \in \mathbb{F}_{2^n}\}.$$

The *nonlinearity* of f, say $nl(f)$, is related to the Walsh spectrum as follows:

$$nl(f) = 2^{n-1} - \frac{L(f)}{2} \quad \text{where} \quad L(f) = \max_{a \in \mathbb{F}_{2^n}} Av(\mathcal{F}(f+\varphi_a)), \tag{4}$$

where $Av(u)$ is the absolute value of any $u \in \mathbb{Z}$. The function f is said to be *bent* when n is even and $\mathcal{W}_f$ contains two values only, namely $\pm 2^{n/2}$. It

is said to be *plateaued* when either it is bent, or $\mathcal{W}_f$ contains three values, namely

$$\{0, \pm 2^{(n+s)/2}\}, \text{ where } 1 \leq s \leq n-2 \text{ with } s+n \text{ even.}$$

The value $2^{(n+s)/2}$ is the *amplitude* of f. Plateaued functions were introduced by Zhang and Zheng in [20], where the reader can find a proof of Theorem 1 below. The *sum-of-square indicator* of a Boolean function $f \in B_n$ is

$$\nu(f) = \sum_{a \in \mathbb{F}_{2^n}} \mathcal{F}^2(D_a f) = 2^{-n} \sum_{a \in \mathbb{F}_{2^n}} \mathcal{F}^4(f + \varphi_a). \tag{5}$$

Theorem 1 *[20] Any $f \in B_n$ satisfies $\nu(f) \leq 2^n L^2(f)$, where $L(f)$ is defined by (4). Equality occurs if and only if f is plateaued, that is, for some integer $1 \leq s \leq n-2$,*

$$L(f) = 2^{(n+s)/2} \quad \textit{and} \quad \nu(f) = 2^{2n+s}. \tag{6}$$

For a function F over $\mathbb{F}_{2^n}$, the nonzero linear combinations of its coordinates are called the *components* of F. They are the functions of B_n defined as follows:

$$f_\mu(x) := Tr(\mu F(x)), \ \forall \ \mu \in \mathbb{F}_{2^n}^*.$$

The nonlinearity of the vectorial function F is then

$$NL(F) = 2^{n-1} - \frac{\mathcal{L}(F)}{2} \quad \text{where} \quad \mathcal{L}(F) = \max_{\mu \in \mathbb{F}_{2^n}^*} L(f_\mu). \tag{7}$$

A *plateaued vectorial function* is a vectorial function whose components are plateaued Boolean functions. It is said that F is *plateaued with single amplitude* when all components have the same amplitude. For recent progress on plateaued functions, see [7]. See [15], and the references herein, for a generalization to any characteristic.

2.2 The related codes

In this paper, we consider *binary linear codes* which are subspaces of $\mathbb{F}_2^N$, where $N = 2^n - 1$. Such a code C is a so called $[N, k, d]$ code, *i.e.,* of length N, dimension k and *minimum weight* d. Any codeword in the *ambiant space*

$\mathbb{F}_2^N$ is a vector $c = (c_0, \ldots, c_{N-1})$, $c_i \in \mathbb{F}_2$. The (Hamming) weight of c is the number of nonzero c_i, denoted $\mathrm{wt}(c)$. The *weight enumerator* of C is the sequence $(\lambda_0, ..., \lambda_N)$, where λ_i is the number of codewords of C of weight i. Viewing $\mathbb{F}_{2^n}^*$ as the sequence

$$1, \alpha, \alpha^2, \ldots, \alpha^{N-1},$$

a codeword c can be expressed by its *locators*. These are the elements of the support of c, the α^i such that $c_i \neq 0$. Setting $c = (c_0, \ldots, c_{N-1})$ and $\omega = \mathrm{wt}(c)$, the codeword c can be expressed as follows:

$$X_c = (\alpha^{i_1}, \ \ldots, \ \alpha^{i_\omega}) \ \text{ where } \ c_i \neq 0 \ \Leftrightarrow \ i \in \{i_1, \ldots, \ i_\omega\}.$$

For simplicity, we will often say $X_c \in C$ as well as $c \in C$. Generally, we will use capital letters for a vector expressed by its locators: $X = (x_1, \ \ldots, \ x_\omega)$, $x_i \in \mathbb{F}_{2^n}$, where $\mathrm{wt}(X) = \omega$. Thus, for two such vectors X_c and $X_{c'}$, $X_c + X_{c'}$ is the vector $c + c'$ expressed by its locators and $X_c \cap X_{c'}$ is the vector whose locators are locators of both X_c and $X_{c'}$.

The dual $C^\perp$ of C is the subspace generated by the so called *parity check matrix* of C. Let $\mathcal{H}$ be such a matrix. Then $C^\perp$ is defined as follows:

$$c \in C \ \text{ if and only if } \ \mathcal{H}c^t = 0.$$

The link between linear codes and APN functions was introduced in [8].

Definition 2 *Let C be a binary linear code of length N. Denote by $(\eta_0, ..., \eta_N)$ the weight enumerator of its dual $C^\perp$, with*

$$\eta_i = |\{c \in C^\perp | wt(c) = i\}| \ \textit{and} \ \Omega = \{j : \ \eta_j \neq 0, \ 1 \leq j \leq N\}.$$

The set Ω is said to be the characteristic set of C.

Theorem 2 [8, Theorem 5] *Let F be any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$ such that $F(0) = 0$, and let C_F be the $[N = 2^n - 1, k \ , d]$ code defined by the parity check matrix*

$$\mathcal{H}_F = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{N-1} \\ F(1) & F(\alpha) & F(\alpha^2) & \ldots & F(\alpha^{N-1}) \end{pmatrix}, \tag{8}$$

where each entry is viewed as a binary vector. Then:
(i) *The code C_F is such that $3 \leq d \leq 5$;*

(ii) *F is APN if and only if $d = 5$;*
(iii) *F is almost bent (AB) if and only if the characteristic set of C_F is as follows:*

$$\Omega = \{2^{n-1}, 2^{n-1} \pm 2^{(n-1)/2}\}.$$

Let $c = (c_0, \ ..., \ c_{N-1})$ be a binary vector. By the definition of $\mathcal{H}_F$, c belongs to C_F if and only if it satisfies

$$\sum_{i=0}^{N-1} c_i \alpha^i = 0 \quad \text{and} \quad \sum_{i=0}^{N-1} c_i F(\alpha^i) = 0. \tag{9}$$

Remark 1 *AB functions exist only for odd n. Any AB function is APN. The dimension k of C_F satisfies $k \geq 2^n - 2n - 1$, with equality if and only if F has no linear component. This holds when F is APN [8, Corollary 1].*

3 Codewords of weight 3 or 4

In this paper, we mainly treat the codes C_F, with minimum distance d, such that $3 \leq d \leq 4$, *i.e.,* the functions F satisfying $\delta(F) \geq 4$. In this section, we emphasize that the differential uniformity of F is fully related with the codewords of weight 3 and 4 of C_F. We later explain the link between these codewords and the cosets of C_F of minimum weight 1 and 2. We first give definitions and notations which will be used throughout this paper.

3.1 Basic description

Definition 3 *Let F be any function over $\mathbb{F}_{2^n}$ such that $F(0) = 0$. For any $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, we define*

$$T_{a,b} = \{(x, x + a) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \mid D_a F(x) = b\}, \tag{10}$$

where by convention $(x, x + a)$ is a codeword of length N, whose weight is 1 if $x \in \{0, a\}$ and is 2 otherwise, expressed by its locators.

To be clear, if $x = \alpha^i$ for some i and $x + a = \alpha^j$, $j \neq i$, then (α^i, α^j) corresponds to the binary codeword

$$(c_0, c_1, \ldots, c_{N-1}) \text{ where } c_\ell \neq 0 \text{ if and only if } \ell \in \{i, j\}.$$

When $x \in \{0, a\}$, this codeword has only one locator (a), *i.e.,* it corresponds to a binary codeword of weight 1 in the ambiant space $\mathbb{F}_2^N$.

Note that $T_{a,b}$ is empty for any b which is not in the image set of D_aF. In particular, if F is APN, then any $T_{a,b}$ has size 0 or 1. More generally, the size of $T_{a,b}$ is

$$\kappa_{a,b} = \frac{\delta(a,b)}{2}. \tag{11}$$

Every pair $(x, y) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}^*$, with $x \neq y$, can be written as $(x, x + a)$ for $a = x + y$, and the corresponding codeword is in only one $T_{a,b}$, where $b = F(x) + F(x + a)$. When $x = 0$, we have $(a) \in T_{a,F(a)}$. Obviously, two vectors in $T_{a,b}$ do not intersect, by definition. Now, we define a mapping $\mathcal{S}$ from the set $\{T_{a,b}, (a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}\}$ to the set of subsets of C_F:

$$\mathcal{S}(T_{a,b}) = \begin{cases} \emptyset & \text{if } \kappa_{a,b} \in \{0, 1\} \\ \{X+Y \mid X, Y \in T_{a,b}, X \neq Y\} & \text{otherwise} \end{cases} \tag{12}$$

We denote by $\mathcal{S}(F)$ the union of all $\mathcal{S}(T_{a,b})$.

Lemma 1 *Assume that $\delta(F) \geq 4$. Let W_3 and W_4 be, respectively, the set of codewords of weight 3 and 4 of C_F. Then $W_3 \cup W_4 = \mathcal{S}(F)$.*

Proof. Recall that F is a function over $\mathbb{F}_{2^n}$ such that $F(0) = 0$. First, $\mathcal{S}(T_{a,b})$ is included in $W_3 \cup W_4$ for all (a, b). This is because, by definition, any codeword of $\mathcal{S}(T_{a,b})$ has locators of the form $(x, x + a, y, y + a)$, for some x and y satisfying $x \neq y \neq y + a$ and

$$F(x)+F(x+a) = b = F(y)+F(y+a).$$

According to (9), such a codeword is a codeword of C_F of weight 3 or 4. Conversely, let $X = (x, t, y, z)$ be a codeword of $W_3 \cup W_4$, where we admit that $x = 0$ when this codeword has weight 3. Set $a = x + t$ and $u = z + y$. From (9) again, we get $a = u$ and then

$$X = (x, x + a, y, y + a) \in \mathcal{S}(T_{a,b}) \text{ for } b = F(x) + F(t) = F(y) + F(z),$$

completing the proof. ◇

Lemma 2 *Assume that $\delta(F) \geq 4$. Let $X \in W_3 \cup W_4$ with*

$$X = (x, x+a, y, y+a), \quad y \neq x \neq x+a. \tag{13}$$

Then $X \in \mathcal{S}(T_{a_i,b_i})$ *for exactly three distinct* (a_i, b_i)*, that is:*

$$(a_i, b_i),\ i{=}1,2,3 \quad \textit{with}\ a_1{=}a,\ a_2{=}x{+}y,\ a_3{=}x{+}y{+}a,$$

and $b = b_1 = D_aF(x) = D_aF(y)$*,*

$$b_2{=}D_{a_2}F(x){=}D_{a_2}F(x{+}a),\ b_3{=}D_{a_3}F(x){=}D_{a_3}F(x{+}a).$$

Moreover, if F *is a permutation then* $b_1 \neq b_2 \neq b_3$*.*

Proof. Let $X \in W_3 \cup W_4$, which is in a set $\mathcal{S}(T_{a,b})$, and satisfies (13), with $b = D_aF(x) = D_aF(y)$. Now, the three pairs of locators of X are each in one and only one set $\mathcal{S}(T_{a_i,b_i})$, providing three times the same codeword.

Setting $y = x + a_2$ so that $y + a = x + a_2 + a$, we have

$$(x, y), (x{+}a, y{+}a) \in T_{a_2,b_2} \ \text{ with } D_{a_2}F(x){=}D_{a_2}F(x{+}a){=}b_2$$

and, with $a_3 = a_2 + a = y + x + a$,

$$(x, y{+}a), (x{+}a, y) \in T_{a_3,b_3} \ \text{ with } D_{a_3}F(x){=}D_{a_3}F(x{+}a){=}b_3.$$

Clearly, the a_i are distinct, since $y \neq x \neq x{+}a$, and every pair of locators of X is well placed. We have above $F(x){+}F(x{+}a_2) = b_2$ and $F(x){+}F(x{+}a) = b$. Assuming that $b = b_2$, we get $F(y) = F(x + a)$, which is impossible if F is a permutation. The cases $b = b_3$ and $b_2 = b_3$ are similar, completing the proof. ◇

3.2 The cosets of C_F

Let C be any binary linear $[N, k, d]$-code, where $N = 2^n - 1$. There are $2^{N-k} - 1$ distinct proper cosets of C. Such a coset is simply: $U = X + C$ with $X \notin C$. A codeword of minimum weight of U is called a *leader* of U. Every coset is uniquely determined by its so-called *syndrome*. For the code C_F, the syndrome of $X + C_F$, where X has locators $(x_1, \ldots, x_\ell)$, is the pair (u, v) where

$$u{=}\sum_{i=1}^{\ell} x_i \ \text{ and } \ v{=}\sum_{i=1}^{\ell} F(x_i), \tag{14}$$

according to the definition of codewords of C_F (see (9)).

Several properties of the code C_F are developed in [8, Section 3.2], when F is any APN function over $\mathbb{F}_{2^n}$. It is notably proved that when F is an AB function (see Theorem 2), the code C_F is *completely regular*, *i.e.,* for any coset of C_F its weight distribution is uniquely determined by its minimum weight. When F is not APN, the code C_F contains codewords of weight 3, or/and 4. Then the structure of C_F and the weight distributions of its cosets become more complicated, even when $\delta(F) = 4$.

In the previous section, we proved that for any not APN function F, every codeword in $\mathrm{W}_3 \cup \mathrm{W}_4$ is obtained by summing two distinct vectors of a set $T_{a,b}$. By definition, any non empty $T_{a,b}$ characterizes the coset of C_F with syndrome (a, b), by its codewords of weight 1 and 2. Such a coset, say $C_{a,b}$, has only one leader when its weight equals 1. The number of codewords of weight 2 in $C_{a,b}$ equals $\kappa_{a,b} - 1$ when $b = F(a)$ and $\kappa_{a,b}$ otherwise. Since $2\kappa_{a,b} = \delta(a, b)$, the differential uniformity of F is fully determined by the number of codewords of weight 2 in the cosets $C_{a,b}$. We summarize as follows.

Theorem 3 *Assume that $\delta(F) \geq 4$. The set $\mathrm{W}_3 \cup \mathrm{W}_4$ is fully determined by the set of cosets of C_F of minimum weight 1 or 2, which are defined by the syndromes:*

$$(a, b),\ a \in \mathbb{F}_{2^n}^*,\ b \in Im(D_aF)\ (so\ that\ \kappa_{a,b} > 0), \tag{15}$$

where $Im(D_aF)$ is the image set of D_aF. Moreover, such a coset $C_{a,b}$ has the following properties:

(i) *When $b = F(a)$, the coset $C_{a,b}$ contains $\kappa_{a,b} - 1$ codewords of weight 2 and one codeword of weight 1.*

(ii) *When $b \neq F(a)$, the coset $C_{a,b}$ contains $\kappa_{a,b}$ codewords of weight 2.*

Finally, $\delta(F) = 2 \times \max_{a,b}\{\kappa_{a,b}\}$, where (a, b) is defined by (15).

We end this section with two properties concerning low differential uniformity. They are directly deduced from the previous results. The code C_F is defined by Theorem 2 and its cosets $C_{a,b}$ by Theorem 3.

Proposition 1 *The function F is APN if and only if every coset $C_{a,b}$ of C_F, with syndrome (a, b) defined by (15), contains only one codeword with weight in $\{1, 2\}$, its leader. It means in other terms that any $T_{a,b}$ has size 0 or 1.*

Proposition 2 *The function F satisfies $\delta(F) = 4$ if and only if every coset $C_{a,b}$ of C_F, defined by (15), contains either only one codeword with weight in $\{1, 2\}$, or two codewords either both of weight 2, or one of weight 1 and the other of weight 2.*

4 The case $\delta(F) = 4$

In this section, we study specific properties of the code C_F, when $\delta(F) = 4$. The code C_F is defined by Theorem 2 and F is a function over $\mathbb{F}_{2^n}$ such that $F(0) = 0$. Also W_3 (resp. W_4) is the set of codewords of weight 3 (resp. of weight 4) of C_F.

Lemma 3 *Let X and Y be two distinct codewords of C_F, which belong to $W_3 \cup W_4$. Then $\mathrm{wt}(X + Y) \geq 3$ and $\mathrm{wt}(X \cap Y) \leq 2$. Moreover, if X and Y satisfy either $\mathrm{wt}(X \cap Y) = 2$, or $\mathrm{wt}(X \cap Y) = 1$ with $\mathrm{wt}(X) = \mathrm{wt}(Y) = 3$, then $\delta(F) \geq 6$.*

Proof. Since the vector $X + Y$ is in C_F, its weight is at least 3, from Theorem 2, implying $\mathrm{wt}(X \cap Y) \leq 2$.

Assume that $\mathrm{wt}(X \cap Y) = 2$. So, at least Y (for instance) has weight equal to 4. Let $X = (x, y, x_1, x_2)$ and $Y = (x, y, y_1, y_2)$ with $x \neq y \neq 0$. Then we have, since $X, Y \in C_F$,

$$\begin{aligned} &x+y=x_1+x_2=y_1+y_2=a \quad \text{and} \\ &F(x)+F(x+a)=F(x_1)+F(x_1+a)=F(y_1)+F(y_1+a). \end{aligned} \tag{16}$$

Hence $\delta(F) \geq 6$. Next, assume $X = (x, x_1, x_2)$ and $Y = (x, y_1, y_2)$. We get, as above, $x = x_1 + x_2 = y_1 + y_2$ with

$$F(x) = F(x_1) + F(x_1 + x) = F(y_1) + F(y_1 + x),$$

completing the proof. ◇

In the case where $\delta(F) = 4$, we can study precisely the weight of $X + Y$, when X and Y belong to $W_3 \cup W_4$. This leads to a combinatorial property of C_F.

Theorem 4 *Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$. The function F satisfies $\delta(F) = 4$ if and only if the code C_F, defined by Theorem 2, has codewords of weight 3 or 4 and, for any such two distinct codewords, the weight of their sum equals at least 5. More precisely, in the case where $\delta(F) = 4$, we have for any such $X, Y \in W_3 \cup W_4$:*

(i) *If X and Y are both of weight 3, then $\mathrm{wt}(X + Y) = 6$.*

(ii) *If $\mathrm{wt}(X) = 3$ and $\mathrm{wt}(Y) = 4$, then $\mathrm{wt}(X + Y) \in \{5, 7\}$.*

(iii) *If $\mathrm{wt}(X) = \mathrm{wt}(Y) = 4$, then $\mathrm{wt}(X + Y) \in \{6, 8\}$.*

Proof. Recall that for any codewords X and Y, one has

$$\mathrm{wt}(X+Y)=\mathrm{wt}(X)+\mathrm{wt}(Y)-2\mathrm{wt}(X\cap Y).$$

Assume that $\delta(F) = 4$. Applying Lemma 3, we know that $\mathrm{wt}(X \cap Y) \leq 1$ for any X and Y in $W_3 \cup W_4$, where $X \neq Y$. In particular, $\mathrm{wt}(X \cap Y) = 0$ when $\mathrm{wt}(X) = \mathrm{wt}(Y) = 3$. Therefore, in all cases $\mathrm{wt}(X + Y) \geq 5$. The three items are simply derived.

Now, suppose that any two distinct codewords of weight 3 or 4, say X and Y, satisfy $\mathrm{wt}(X + Y) \geq 5$. If $\delta(F) \geq 6$, then there is a pair (a, b) and $x, y, z \in \mathbb{F}_{2^n}$ such that

$$D_aF(x)=D_aF(y)=D_aF(z)=b, \quad |\{x, x+a, y, y+a, z, z+a\}|=6.$$

Thus the two codewords with locators $(x, x+a, y, y+a)$ and $(x, x+a, z, z+a)$ whose weights are 3 or 4, are such that their sum has locators $(y, y+a, z, z+a)$, and thus has weight 3 or 4, a contradiction which completes the proof. $\diamond$

To show that our results are relevant, we end this section by a first outcome; others will be given later. When $\delta(F) = 4$, every non empty $\mathcal{S}(T_{a,b})$ contains only one codeword (see (12) and Proposition 2). Thus the size of $\mathcal{S}(F)$, which is the union of the $\mathcal{S}(T_{a,b})$, is in this case

$$|\mathcal{S}(F)|=\frac{1}{3}|\{(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n} \mid \kappa_{a,b}=2\}|,$$

since every codeword is in exactly three $\mathcal{S}(T_{a,b})$ (Lemma 2).

Corollary 1 *Let F be a not APN function. We denote by λ_3 (resp. λ_4) the size of W_3 (resp. W_4). Assume that $\lambda_4 = 0$. Then $\delta(F) = 4$ and $\lambda_3 = |\mathcal{S}(F)| \leq N/3$. Also, if $\lambda_3 = N/3$ then n must be even. It is in particular the case when $F(x) = x^d$ for some d, which is not a power of 2. Consequently, it is impossible to have $\lambda_4 = 0$, for such F, when n is odd.*

Proof. Any codeword of weight 3 or 4 is obtained from a set $T_{a,b}$ of size at least 2, by means of the application $\mathcal{S}$. Since $\lambda_4 = 0$, any such $T_{a,b}$ cannot contain two codewords of weight 2. Hence $\kappa_{a,b} = 2$ and $T_{a,b} = \{(a), (x, x+a)\}$, for some x. Moreover $b = F(a)$ so that:

$$|\mathcal{S}(F)| = \frac{1}{3}|\{a \in \mathbb{F}_{2^n}^* \mid \kappa_{a,F(a)} = 2\}|.$$

Further, λ_3 equals the size of $\mathcal{S}(F)$, which is less than or equal to $N/3$, since codewords of weight 3 are disjoined. If $\lambda_3 = (2^n - 1)/3$, then n must be even.

When $F(x) = x^d$, it is well-known that the code C_F is a so-called *binary cyclic code with two zeroes*, α and α^d, where α is a primitive root of $\mathbb{F}_{2^n}$. Thus the code C_F is *invariant by shift*, that is, for any vector X given by its locators,

$$X = (x_1, x_2, \ldots, x_\ell) \in C_F \iff (\alpha x_1, \alpha x_2, \ldots, \alpha x_\ell) \in C_F. \tag{17}$$

Thus $\lambda_3 = N/3$ when n is even. When n is odd the codewords of weight 3 cannot be disjoined, a contradiction. ◇

Example 1 *Let $n = 2k$ for some k and consider the function $F : x \mapsto x^{-1}$ over $\mathbb{F}_{2^n}$. It is well-known that F satisfies $\delta(F) = 4$. Moreover, for any $a \in \mathbb{F}_{2^n}^*$, the equation*

$$\frac{1}{x} + \frac{1}{x+a} = b, \ b \neq \frac{1}{a},$$

has 0 or 2 solutions (x and $x + a$). When $b = 1/a$, the solutions are

$$x = 0, \ x = a \ \text{ and the two roots of } x^2 + ax + a^2 = 0.$$

Thus the code C_F is such that $\lambda_3 = N/3$ and $\lambda_4 = 0$. We can describe the set W_3: let x_1 be a root of $x^2 + x + 1 = 0$; then

$$W_3 = \left\{(\alpha^i, \alpha^i x_1, \alpha^i(x_1+1)), \ i = 0, \ldots, N-1\right\}.$$

Note that every codeword appears three times, for three distinct i.

Problem 1 *The main question arising from the previous example is: whether there exist or not differentially 4-uniform monomial functions with $\lambda_4 = 0$, other than the inverse function (up to equivalence)? Another question is about the existence of codes C_F such that $\lambda_4 = 0$ and $0 < \lambda_3 < N/3$.*

5 The size of W_3 and W_4 via differential spectrum

In this section, our aim is to compute the size of the sets of codewords of weight 3 and 4 of any code C_F, denoted W_3 and W_4 respectively. Recall that λ_3 and λ_4 denote the size of W_3 and W_4, respectively. In previous works, λ_3 and λ_4 were obtained essentially for some functions of type $F(x) = x^d$, with respect to the differential spectrum (see [3, 12]).

5.1 The formulas

In this subsection, we propose some expressions of λ_3 and λ_4 for any function F with respect to its differential spectrum. Recall that the binomial coefficient $\binom{u}{v} := \frac{u!}{v!(u-v)!}$ equals 0 when $u < v$. By Lemma 1, we know that the codewords of weight 3 and 4 are just all the elements of the set

$$\mathcal{S}(F) = \bigcup_{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n}} \mathcal{S}(T_{a,b})$$

(see (10) and (12) for the definitions). Every set $\mathcal{S}(T_{a,b})$ is of size $\binom{\kappa_{a,b}}{2}$, where $\kappa_{a,b}$ is the size of $T_{a,b}$. Moreover the value λ_3 is strongly related with some values of b.

(1) If $b = F(a)$, then $\kappa_{a,b} - 1$ codewords of weight 3, together with $\binom{\kappa_{a,b}-1}{2}$ codewords of weight 4, belong to $\mathcal{S}(T_{a,b})$.

(2) If $b \neq F(a)$, then $\mathcal{S}(T_{a,b})$ contains $\binom{\kappa_{a,b}}{2}$ codewords of weight 4 and no codewords of weight 3.

According to these observations, we express easily the size of W_3 and of W_4.

Theorem 5 *With notations as above, we assume that $\delta(F) \geq 4$ and $F(0) = 0$. Then we have:*

(i) *The size of* W_3 *is* $\lambda_3 = \frac{1}{3}\sum_{a\in\mathbb{F}_{2^n}^*}(\kappa_{a,F(a)}-1)$*;*

(ii) *The size of* $W_3 \cup W_4$ *is*

$$\lambda_3+\lambda_4 = \frac{1}{6}\sum_{a\in\mathbb{F}_{2^n}^*}\sum_{b\in\mathbb{F}_{2^n}}\kappa_{a,b}^2 - \frac{N(N+1)}{12} = \frac{1}{24}\sum_{i=0}^{\delta(F)} i^2\omega_i - \frac{N(N+1)}{12},$$

$$\text{where } \omega_i = |\{(a,b)\in\mathbb{F}_{2^n}^*\times\mathbb{F}_{2^n} \mid \delta(a,b)=i\}| \text{ and } N = 2^n-1.$$

Proof. By Lemma 2, each codeword $X \in W_3 \cup W_4$ appears exactly in three $\mathcal{S}(T_{a,b})$ for three distinct pairs (a,b). Hence

$$\lambda_3 = \frac{1}{3}\sum_{a\in\mathbb{F}_{2^n}^*}(\kappa_{a,F(a)}-1),$$

and

$$\begin{aligned}
\lambda_3+\lambda_4 &= |\mathcal{S}(F)| = \frac{1}{3}\sum_{a,b}|\mathcal{S}(T_{a,b})| \\
&= \frac{1}{3}\sum_{a\in\mathbb{F}_{2^n}^*}\sum_{b\in\mathbb{F}_{2^n}}\binom{\kappa_{a,b}}{2} = \frac{1}{3}\sum_{a\in\mathbb{F}_{2^n}^*}\sum_{b\in\mathbb{F}_{2^n}}\frac{\kappa_{a,b}^2-\kappa_{a,b}}{2} \\
&= \frac{1}{6}\left(\sum_{a\in\mathbb{F}_{2^n}^*}\sum_{b\in\mathbb{F}_{2^n}}\kappa_{a,b}^2 - 2^{n-1}N\right) \quad (\text{as } \sum_b \kappa_{a,b} = \frac{1}{2}\sum_b \delta(a,b) = 2^{n-1}) \\
&= \frac{1}{24}\sum_{i=0}^{\delta(F)} i^2\omega_i - \frac{N(N+1)}{12}.
\end{aligned}$$

This completes the proof. ◇

Let $F(x) = x^d$ be a power function, for some d which is not a power of 2. By applying Theorem 5 to the power functions, we obtain an extension of previous results given in [3, Corollary 1], with a different approach. The next corollary is simply derived, since for such F we have

$$2\kappa_{a,b} = \delta(a,b) = \delta(1,b/a^d), \text{ for any } a\in\mathbb{F}_{2^n}^*.$$

Corollary 2 *Let* F *be a power function over* $\mathbb{F}_{2^n}$*. Then the following holds:*

(i) *The size of* W_3 *is*

$$\lambda_3 = \frac{N(\delta(1)-2)}{6}, \text{ where } \delta(b) := \delta(1,b) \text{ for any } b \in \mathbb{F}_{2^n}.$$

(ii) *The size of* $W_3 \cup W_4$ *is*

$$\lambda_3+\lambda_4 = \frac{N}{24}\sum_{b\in\mathbb{F}_{2^n}} \delta(b)^2 - \frac{N(N+1)}{12} = \frac{N}{24}\sum_{i=0}^{\delta(F)} i^2\widetilde{\omega}_i - \frac{N(N+1)}{12},$$

where $\widetilde{\omega}_i = |\{b \in \mathbb{F}_{2^n} \mid \delta(b) = i\}|$.

The next proposition is directly obtained from Corollary 2(i) (with same notation). Since $\lambda_3 = N(\delta(1)-2)/6$, 3 must be a divisor of N or of $\delta(1)-2$. Note that 3 divides N if and only if n is even, hence 3 must divide $\delta(1)-2$ when n is odd. We summarize as follows.

Proposition 3 *Let* $F(x) = x^d$ *be defined over* $\mathbb{F}_{2^n}$ *where* d *is not a power of* 2. *Then* $\lambda_3 = 0$ *if and only if* $\delta(1) = 2$.

Assume that $\lambda_3 \neq 0$. *Then either* $\delta(1) - 2$ *or* N *is divisible by* 3. *In particular, when* n *is odd it holds*

$$\delta(1) = 3k+2 \text{ for some even } k \geq 2.$$

Therefore, if $\lambda_3 \neq 0$ *with* n *odd then* $\delta(F) \geq 8$.

Problem 2 *According to Corollary 2 and Proposition 3, it appears that for odd* n *the power functions* F *such that* $\delta(F) = 4$ *have an associated code* C_F *of minimum distance* 4. *One can see in [3, Table 1] that such a function does not exist for* $n \in \{15, 17, \ldots, 25\}$, *when* $\gcd(n, d) = 1$. *Does it hold for* $n > 25$*?*

5.2 Lower bound and upper bound

In this subsection, we discuss upper and lower bounds for λ_3 and λ_4. We set

$$\kappa(F) = \max_{a\in\mathbb{F}_{2^n}^*, b\in\mathbb{F}_{2^n}} \kappa_{a,b} \quad (\text{so that } \delta(F) = 2\kappa(F)). \tag{18}$$

Recall that differentially two-valued functions are defined in Section 2.1.

Theorem 6 *Let F be a function over $\mathbb{F}_{2^n}$ such that $\kappa(F) \geq 2$. Then it holds*

$$\lambda_3 \leq \frac{1}{3}(\kappa(F)-1)(N-M) \leq \frac{1}{3}(\kappa(F)-1)N,$$

where M is the number of $a \in \mathbb{F}_{2^n}^*$ such that $\kappa_{a,F(a)} = 1$. Both equalities hold if and only if $\kappa_{a,F(a)} = \kappa(F)$ for any $a \in \mathbb{F}_{2^n}^*$.

Proof. It follows from Theorem 5(i) that

$$\begin{aligned} \lambda_3 &= \frac{1}{3}\sum_{a\in\mathbb{F}_{2^n}^*}(\kappa_{a,F(a)}-1) \\ &\leq \frac{1}{3}(\kappa(F)-1)(N-M) \leq \frac{1}{3}(\kappa(F)-1)N. \end{aligned}$$

We first used that $\kappa_{a,F(a)} \leq \kappa(F)$, for those $a \in \mathbb{F}_{2^n}^*$ such that $\kappa_{a,F(a)} \neq 1$. Further, we put $M = 0$ to obtain the latter bound. Hence, both equalities hold if and only if $\kappa_{a,F(a)} = \kappa(F)$ for any $a \in \mathbb{F}_{2^n}^*$. ◇

We need more notations to propose the next upper bound for $\lambda_3 + \lambda_4$. Set $\{x_1, \ldots, x_N\} = \mathbb{F}_{2^n}^*$. For $1 \leq i < j \leq N$, let n_{ij} be the number of codewords of C_F of weight 4, which contains x_i and x_j as two of its locators. Set $a_{ij} = x_i + x_j$ and $b_{ij} = F(x_i) + F(x_j)$.

First, $\kappa_{a_{ij},b_{ij}} \geq 1$ as $(x_i, x_j) \in T_{a_{ij},b_{ij}}$. In particular, it holds $\kappa_{a_{ij},b_{ij}} \geq 2$ if $b_{ij} = F(a_{ij})$, since in this case $(a_{ij}) \in T_{a_{ij},b_{ij}}$ as well. Conversely, if $\kappa_{a,b} \geq 1$ for some $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $b \neq F(a)$, then $(a) \notin T_{a,b}$, and thus there exists some pair of integers $(i, j), 1 \leq i < j \leq N$, such that $(x_i, x_j) \in T_{a,b}$. This implies $a = x_i + x_j = a_{ij}$ and $b = F(x_i) + F(x_j) = b_{ij}$. Moreover, it is clear that when $\kappa_{a,F(a)} \geq 2$, there exist some $1 \leq i < j \leq N$ such that $(a, F(a)) = (a_{ij}, b_{ij})$. So, we have proved that $\kappa_{u,v} \neq 0$ if and only if

$$(u, v) \in \{(a_{ij}, b_{ij}) \mid 1 \leq i < j \leq N\} \cup \{(a, F(a)) \mid a \in \mathbb{F}_{2^n}^*\}.$$

Moreover, it holds

$$\begin{aligned} &\{(a_{ij}, b_{ij}) \mid 1 \leq i < j \leq N\} \cup \{(a, F(a)) \mid a \in \mathbb{F}_{2^n}^*\} \\ = \ &\{(a_{ij}, b_{ij}) \mid 1 \leq i < j \leq N\} \cup \{(a, F(a)) \mid a \in \mathbb{F}_{2^n}^*, \kappa_{a,F(a)} = 1\}, \end{aligned}$$

where the latter is a disjoint union. We also need to define

$$\varpi_2 = |\{(i, j) \mid 1 \leq i < j \leq N, \kappa_{a_{i,j},b_{i,j}} = 1\}|, \tag{19}$$

or equivalently,

$$\varpi_2 = \omega_2 - |\{a \in \mathbb{F}_{2^n}^* \mid \kappa_{a,F(a)} = 1\}|.$$

Theorem 7 *Let F be a function over $\mathbb{F}_{2^n}$ such that $\kappa(F) \geq 2$. Then it holds*

$$\lambda_3+\lambda_4 \leq \frac{\lambda_3}{2}+(\kappa(F)-1)(\frac{N(N-1)}{12}-\frac{\overline{\omega}_2}{6}) \leq \frac{(\kappa(F)-1)N(N+1)}{12}.$$

The first inequality is equality if and only if F is differentially two-valued $\{0, \delta(F)\}$ or three-valued $\{0, 2, \delta(F)\}$. Both equalities hold if and only if F is differentially two-valued.

Proof. On one hand, note that any codeword of weight 4 that contains x_i and x_j $(i \neq j)$ as two of its locators should appear in $\mathcal{S}(T_{a_{ij},b_{ij}})$ as $(x_i, x_j) \in T_{a_{ij},b_{ij}}$. But in each $\mathcal{S}(T_{a_{ij},b_{ij}})$, there are exactly $\kappa_{a_{ij},b_{ij}} - 1$ such codewords if $b_{ij} \neq F(a_{ij})$; and there are exactly $\kappa_{a_{ij},b_{ij}} - 2$ such codewords if $b_{ij} = F(a_{ij})$. Hence we have

$$n_{ij} = \begin{cases} \kappa_{a_{ij},b_{ij}}-1 & \text{if } b_{ij} \neq F(a_{ij}), \\ \kappa_{a_{ij},b_{ij}}-2 & \text{if } b_{ij} = F(a_{ij}). \end{cases}$$

On the other hand, the sum $n_{12}+n_{13}+\cdots+n_{N-1,N}$ is a calculation of the number of codewords of C_F of weight 4, in which every codeword of weight 4 is taken $\binom{4}{2} = 6$ times. Consequently, one obtains that

$$\begin{aligned} \lambda_4 &= \frac{1}{6}\sum_{1\leq i<j\leq N} n_{ij} \\ &= \frac{1}{6}\Bigg(\sum_{\substack{1\leq i<j\leq N,\\ b_{ij}\neq F(a_{ij})}} (\kappa_{a_{ij},b_{ij}}-1)+\sum_{\substack{1\leq i<j\leq N,\\ b_{ij}= F(a_{ij})}} (\kappa_{a_{ij},b_{ij}}-2)\Bigg) \\ &= \frac{1}{6}\sum_{1\leq i<j\leq N} (\kappa_{a_{ij},b_{ij}}-1)-\frac{1}{6}|\{(i,j) \mid i<j, b_{ij}=F(a_{ij})\}| \\ &= \frac{1}{6}\sum_{1\leq i<j\leq N} (\kappa_{a_{ij},b_{ij}}-1)-\frac{\lambda_3}{2} \\ &\leq \frac{1}{6}(\kappa(F)-1)(\frac{N(N-1)}{2}-\overline{\omega}_2)-\frac{\lambda_3}{2}, \end{aligned}$$

where in the inequality we used the fact that $\kappa_{a_{ij},b_{ij}} \leq \kappa(F)$ for any i, j such that $\kappa_{a_{ij},b_{ij}} \neq 1$. Then we arrive at

$$\lambda_3+\lambda_4 \leq \frac{\lambda_3}{2}+(\kappa(F)-1)(\frac{N(N-1)}{12}-\frac{\overline{\omega}_2}{6}),$$

with equality if and only if $\kappa_{a_{ij},b_{ij}} = \kappa(F)$ for any $1 \le i < j \le N$ such that $\kappa_{a_{ij},b_{ij}} \neq 1$, say F is differentially two-valued or three-valued $\{0, 2, \delta(F)\}$.

Furthermore, from Theorem 6, we get

$$\begin{aligned} & \frac{\lambda_3}{2} + (\kappa(F)-1)\left(\frac{N(N-1)}{12} - \frac{\overline{\omega}_2}{6}\right) \\ \le & \frac{(\kappa(F)-1)N}{6} + \frac{(\kappa(F)-1)N(N-1)}{12} \\ = & \frac{(\kappa(F)-1)N(N+1)}{12}, \end{aligned}$$

with equality if and only if $\overline{\omega}_2 = 0$ and $\kappa_{a,F(a)} = \kappa(F)$ for all $a \in \mathbb{F}_{2^n}^*$ (due to Theorem 6). Hence both equalities hold if and only if F is differentially two-valued, noting that $\overline{\omega}_2 = 0$ means that $\kappa_{a,b} = 1$ cannot happen when $b \neq F(a)$. ◇

Remark 2 *The functions which are differentially three-valued* $\{0, 2, \delta(F)\}$ *appear in the previous theorem. It is important to notice that the knowledge of* $\overline{\omega}_2$ *only allows to get the exact value of* λ_3 *and* λ_4*, according to Theorems 6 and 7 (see the next example). Note that, in particular, differentially* 4*-uniform functions are either three-valued of this form or two-valued.*

Example 2 *Let* $n = 2m$*,* $m > 2$*, and* $F(x) = x^{2^{m+1}-1}$*. From [4, Theorem 8]), we know that* F *is a so-called* locally-APN function*, i.e.,* $\delta(b) \in \{0, 2\}$ *unless* $b \in \{0, 1\}$*. Also,* F *has differential spectrum* $\{0, 2, 2^m\}$ *with* $\delta(1) = 2^m$ *and* $\delta(0) \in \{0, 2\}$*. Thus, we get*

$$\lambda_3 = (2^{m-1}-1)\frac{N}{3} \quad \textit{and} \quad \lambda_4 = \frac{N(2^{m-1}-1)(2^{m-2}-1)}{3}.$$

Since $\overline{\omega}_2 = \omega_2 = N(2^{n-1} - 2^{m-1})$*, because* $\kappa_{a,F(a)} \neq 1$ *for any* a *and* ω_2/N *is given by [4, Theorem 8]), we have*

$$\lambda_3 + \lambda_4 = \frac{N(2^{m-1}-1)2^{m-2}}{3},$$

which is equal to the bound of Theorem 7:

$$(2^{m-1}-1)\frac{2N + N(N-1) - N(2^n - 2^m)}{12} = (2^{m-1}-1)\frac{2^m N}{12}.$$

In the next theorem, we present two lower bounds for $\lambda_3+\lambda_4$. The first one is a unified constant bound for functions with same differential uniformity. The second one is more refined by introducing the parameter ω_0. Note that for any function F, we have

$$\omega_0 \geq (2^n-1)\times 2^{n-1} = N(N+1)/2 \text{ (with } \omega_0 = |\{(a,b)|\delta(a,b)=0\}|),$$

with equality if and only if F is APN. This is because the size of the image set of D_aF is at most 2^{n-1}, for any $a \in \mathbb{F}_{2^n}^*$. Equality, for any a, is obtained if and only if F is APN.

Theorem 8 *Let F be a function over $\mathbb{F}_{2^n}$ such that $\kappa(F) \geq 2$. Then we have:*

(i) $\lambda_3+\lambda_4 \geq \kappa(F)(\kappa(F)-1)/2$;

(ii)

$$\lambda_3+\lambda_4 \geq (\frac{N(N+1)/2}{N(N+1)-\omega_0}-1)\frac{N(N+1)}{12},$$

where equality holds if and only if F is differentially two-valued.

Proof. (i) There is at least one pair $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $\kappa_{a,b} = \kappa(F)$. Then

$$|\mathcal{S}(T_{a,b})| = \binom{\kappa(F)}{2} = \frac{1}{2}\kappa(F)(\kappa(F)-1),$$

so that $\lambda_3 + \lambda_4 \geq \kappa(F)(\kappa(F)-1)/2$.

(ii) First, note that the number of pairs $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$, such that $\kappa_{a,b} \neq 0$, is equal to $\omega_2 + \omega_4 + \cdots + \omega_{\delta(F)} = N(N+1) - \omega_0$. Then one has:

$$\begin{aligned}
\lambda_3+\lambda_4 &= \frac{1}{6}\sum_{a\in\mathbb{F}_{2^n}^*}\sum_{b\in\mathbb{F}_{2^n}} \kappa_{a,b}^2 - \frac{N(N+1)}{12} \\
&\geq \frac{1}{6}\times\frac{(\sum_{a,b}\kappa_{a,b})^2}{N(N+1)-\omega_0} - \frac{N(N+1)}{12} \\
&= \frac{(N(N+1))^2/24}{N(N+1)-\omega_0} - \frac{N(N+1)}{12} = (\frac{N(N+1)/2}{N(N+1)-\omega_0}-1)\frac{N(N+1)}{12},
\end{aligned}$$

where we applied the Cauchy-Schwartz inequality to the sum $\sum_{a,b} \kappa_{a,b}^2$, after eliminating all the zero's. Hence the equality holds for F if and only if $\kappa_{a,b} = \kappa(F)$ for all pairs $(a,b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$ such that $\kappa_{a,b} \neq 0$, say F is differentially two-valued. $\diamond$

According to Theorem 7, the proof of the following corollary is obvious.

Corollary 3 *Let F be a function over $\mathbb{F}_{2^n}$ such that $\kappa(F) \geq 2$ and $\lambda_3 = 0$. Then one has $\overline{\omega}_2 = \omega_2 - N$ and $\lambda_4 \leq B$ with*

$$B = (\kappa(F)-1)(\frac{N(N-1)}{12} - \frac{\overline{\omega}_2}{6}) = (\kappa(F)-1)(\frac{N(N+1)}{12} - \frac{\omega_2}{6}).$$

Equality occurs if and only if F is differentially three-valued as $\{0, 2, \delta(F)\}$.

In the following proposition, we prove that the lower bound in (ii) of Theorem 8 is larger than half of the real value for differentially 4-uniform functions.

Proposition 4 *Let F be a differentially 4-uniform function over $\mathbb{F}_{2^n}$. Then one has:*

$$(\frac{N(N+1)/2}{N(N+1)-\omega_0} - 1)\frac{N(N+1)}{12} > \frac{1}{2}(\lambda_3+\lambda_4). \tag{20}$$

Proof. Note that $\omega_0 = N(N+1)/2 + \omega_4$ by (3) and $\lambda_3 + \lambda_4 = \omega_4/3$ by Theorem 5, for differentially 4-uniform functions. Hence the inequality (20) can be rewritten as

$$(\frac{N(N+1)/2}{N(N+1)/2-\omega_4} - 1)N(N+1)/2 > \omega_4. \tag{21}$$

By simple calculations one can further rewrite (21) as follows:

$$\frac{N^2(N+1)^2/4}{N(N+1)/2-\omega_4} > N(N+1)/2+\omega_4,$$

which holds obviously as $\omega_4 \neq 0$ and

$$(N(N+1)/2-\omega_4)(N(N+1)/2+\omega_4) = N^2(N+1)^2/4-\omega_4^2.$$

$\diamond$

Remark 3 *Proposition 4 gives another upper bound, for $\lambda_3+\lambda_4$, of differentially 4-uniform functions as*

$$\lambda_3+\lambda_4 < (\frac{1}{1-\omega_0/(N^2+N)}-2)\frac{N(N+1)}{12},$$

which is better than $\lambda_3+\lambda_4 \leq \frac{N(N+1)}{12}$ given by Theorem 7, if $\omega_0 \leq \frac{2}{3}N(N+1)$.

We end this section with some results, relating the Walsh spectrum and the associated code of a vectorial function.

Theorem 9 *Let F be a function over $\mathbb{F}_{2^n}$ with component functions f_μ, $\mu \in \mathbb{F}_{2^n}^*$. Then*

$$\sum_{\mu\in\mathbb{F}_{2^n}^*} \nu(f_\mu) = (2^n-1)2^{2n+1}+3\times 2^{n+3}(\lambda_3+\lambda_4),$$

where $\nu(f_\mu)$ is defined in Section 2.1.

Proof. It has been obtained by Nyberg that, for any $a \in \mathbb{F}_{2^n}^*$,

$$\sum_{\mu\in\mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\mu) = 2^n \sum_{b\in\mathbb{F}_{2^n}} \delta_{a,b}^2$$

(see formula (4) in Page 118 of [16], which is here rewritten in our context). This is equivalent to

$$\sum_{\mu\in\mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\mu) = 2^{2n+1}+2^{n+3} \sum_{b\in\mathbb{F}_{2^n}} \binom{\kappa_{a,b}}{2}. \tag{22}$$

Indeed, $2\kappa_{a,b} = \delta_{a,b}$ and $\sum_{b\in\mathbb{F}_{2^n}} \kappa_{a,b} = 2^{n-1}$, providing

$$\sum_{b\in\mathbb{F}_{2^n}} \kappa_{a,b}^2 - 2^{n-1} = \sum_{b\in\mathbb{F}_{2^n}} \kappa_{a,b}(\kappa_{a,b}-1).$$

Then, we can deduce that

$$\begin{aligned}
\sum_{\mu\in\mathbb{F}_{2^n}^*} \nu(f_\mu) &= \sum_{\mu\in\mathbb{F}_{2^n}^*} \sum_{a\in\mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\mu) \\
&= \sum_{a\in\mathbb{F}_{2^n}^*} \sum_{\mu\in\mathbb{F}_{2^n}} \mathcal{F}^2(D_a f_\mu) \\
&= (2^n-1)2^{2n+1}+2^{n+3} \sum_{a\in\mathbb{F}_{2^n}^*} \sum_{b\in\mathbb{F}_{2^n}} \binom{\kappa_{a,b}}{2} \\
&= (2^n-1)2^{2n+1}+3\times 2^{n+3}(\lambda_3+\lambda_4),
\end{aligned}$$

where the third equality is deduced from (22). For the last equality, see Theorem 5. ◇

As a consequence of our previous results, we show that the nonlinearity of any function F over $\mathbb{F}_{2^n}$ decreases while the number of codewords of weight 3 and 4 increases. Another property will be derived by Corollary 7 in Section 7.

Corollary 4 *Let F be a function over $\mathbb{F}_{2^n}$. Then its nonlinearity satisfies*

$$NL(F) \leq 2^{n-1} - \sqrt{2^{n-1} + \frac{6(\lambda_3+\lambda_4)}{2^n-1}} \leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{2n+1}(2^n-1)}{2(2^n(2^n-1)-\omega_0)}}.$$

Proof. Recall that $NL(F)$ and $\mathcal{L}(F)$ are defined in Section 2.1 by (7). With the same notation, we have first

$$\mathcal{L}^2(F) = \max_{\substack{\mu\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} \mathcal{F}^2(f_\mu+\varphi_b) \geq \frac{\sum_{\substack{\mu\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} \mathcal{F}^4(f_\mu+\varphi_b)}{\sum_{\substack{\mu\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} \mathcal{F}^2(f_\mu+\varphi_b)},$$

while one has

$$\sum_{\substack{\mu\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} \mathcal{F}^2(f_\mu+\varphi_b) = (2^n-1)2^{2n},$$

by Parseval's relation. Moreovoer, Theorem 9 implies that

$$\sum_{\substack{\mu\in\mathbb{F}_{2^n}^*,\\ b\in\mathbb{F}_{2^n}}} \mathcal{F}^4(f_\mu+\varphi_b) = 2^n \sum_{\mu\in\mathbb{F}_{2^n}^*} \nu(f_\mu) = (2^n-1)2^{3n+1} + 3\times 2^{2n+3}(\lambda_3+\lambda_4).$$

Consequently, we arrive at

$$\mathcal{L}^2(F) \geq \frac{(2^n-1)2^{3n+1} + 3\times 2^{2n+3}(\lambda_3+\lambda_4)}{(2^n-1)2^{2n}} = 2^{n+1} + \frac{24(\lambda_3+\lambda_4)}{2^n-1},$$

and hence

$$\begin{aligned} NL(F) &\leq 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1} + \frac{24(\lambda_3+\lambda_4)}{2^n-1}} \\ &\leq 2^{n-1} - \frac{1}{2}\sqrt{\frac{2^{2n+1}(2^n-1)}{2(2^n(2^n-1)-\omega_0)}}, \end{aligned}$$

by Theorem 8(ii), completing the proof. ◇

6 The set of 2-to-1 derivatives

In this section, we are interested in the set of 2-to-1 derivatives of any function F over $\mathbb{F}_{2^n}$. It is well-known that F is APN if and only if all its derivatives are 2-to-1. Actually, it is sufficient that this last property holds for $2^{n-1}-1$ well-chosen derivatives [10]: F is APN if and only if D_aF is 2-to-1 for all non-zero a of any hyperplane of $\mathbb{F}_{2^n}$. We will show that this result can be generalized, by considering the derivatives in respect with subspaces of smaller dimensions.

Lemma 4 *Let F be a function over $\mathbb{F}_{2^n}$ and $k \geq 2$. Suppose that there is (a,b), $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$, such that*

$$T_{a,b} = \{(x_1, x_1+a), \ldots, (x_k, x_k+a)\},$$

where $x_i \neq x_j \neq x_j + a$ for all i, j. Then, we have for any (i,j), $i \neq j$,

$$\begin{aligned} &D_{x_i+x_j}F(x_i) = D_{x_i+x_j}F(x_i+a) \text{ and} \\ &D_{x_i+x_j+a}F(x_i) = D_{x_i+x_j+a}F(x_i+a). \end{aligned} \tag{23}$$

Consequently, the functions $D_\beta F$, $\beta \in S_a$ with

$$S_a := \{a, x_i+x_j, x_i+x_j+a \mid 1 \leq i < j \leq k\},$$

are not 2-to-1.

Proof. We simply apply Lemma 2. Let (x,y) be any pair (x_i, x_j), $i \neq j$. The codeword, with locators $(x, x+a, y, y+a)$, is exactly in three $\mathcal{S}(T_{a_\ell,b_\ell})$, $\ell = 1,2,3$ with $a_1 = a$, $a_2 = x+y$ and $a_3 = x+y+a$. This proves (23). $\diamond$

Remark 4 *If $k = 2$ (in Lemma 4),xs then $S_a \cup \{0\}$ is a subspace of dimension 2. If $k > 2$, then $S_a \cup \{0\}$ contains a subspace of dimension 3, for instance with basis $\{a, x_1+x_2, x_1+x_3)$.*

Now we can generalize [10, Theorem 2] as follows.

Theorem 10 *Let V be a t-dimensional subspace of $\mathbb{F}_{2^n}$ and $r = n-t$. Let F be a function over $\mathbb{F}_{2^n}$ such that D_aF is 2-to-1, for all $a \in V^*$. Then $\delta(F) \leq 2^r$.*

Proof. Note that V has 2^r cosets, including V itself. Suppose that there is $a \in \mathbb{F}_{2^n} \setminus V$ such that $\delta(a,b) \geq 2^r + 2$, for some b. Let $\ell = (2^r+2)/2$. Then we have ℓ elements of $\mathbb{F}_{2^n}$:

$$A = \{x_1, x_2, \ldots, x_\ell\} \text{ such that } D_aF(x_i) = b,\ 1 \leq i \leq \ell,$$

where $x_i \neq x_j \neq x_j + a$, for all i, j. From Lemma 4 the elements $x_i + x_j$ and $x_i + x_j + a$ are not in V. Therefore, for any pair (i,j), the elements x_i and x_j (resp. x_i and $x_j + a$) cannot be in the same coset of V. Thus, the ℓ elements of A are in ℓ different cosets of V. The same holds for the ℓ elements $x_j + a$: they are in ℓ different cosets of V, all different from the cosets $x_i + V$.

Thus, we get at all $2^r + 2$ different cosets of V, which is impossible. Hence such an a does not exist and we can conclude that $\delta(F) \leq 2^r$. ◇

Example 3 *Let n=2k and* $F(x) = x^{2^i}(x + x^{2^k})$, *where* $\gcd(i,k) = 1$. *It was proved in [18] that*

$$\delta(a,b) \in \begin{cases} \{0, 2^k\} & \text{if } a \in \mathbb{F}_{2^k}^*, \\ \{0, 2\} & \text{if } a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}. \end{cases}$$

Let W be a set of representatives of the cosets of $\mathbb{F}_{2^k}$, i.e., $\mathbb{F}_{2^n}$ is the union of the $w + \mathbb{F}_{2^k}$, $w \in W$. Clearly W is a subspace of dimension k of $\mathbb{F}_{2^n}$. Moreover, for all $a \in W^*$ the function D_aF is 2-to-1. And W is the subspace of $\mathbb{F}_{2^n}$ with the largest dimension which satisfies this property. When $a \notin W$, we have $\delta(a,b) \in \{0, 2, 2^k\}$.

We now propose an application of Theorem 10, by using together APN functions and bilinear functions. In the next example, we propose a class of functions F such that $\delta(F) \leq 4$.

Corollary 5 *Let $H(x) = L_1(x)L_2(x)$, where L_1 and L_2 are two linear functions over $\mathbb{F}_{2^n}$ satisfying* $\ker(L_1) \subseteq \ker(L_2)$. *Set* $t = \dim(\ker(L_1))$. *Then for any APN function G over $\mathbb{F}_{2^n}$, the function $F = G + H$ is such that D_aF is 2-to-1 for all $a \in \ker(L_1)^*$, so that $\delta(F) \leq 2^{n-t}$.*

Proof. We have simply to write the derivative of F for any $a \in \mathbb{F}_{2^n}^*$:

$$\begin{aligned} D_aF(x) &= D_aG(x) + L_1(x)L_2(x) + L_1(x+a)L_2(x+a) \\ &= D_aG(x) + L_1(x)L_2(a) + L_1(a)L_2(x+a). \end{aligned}$$

Thus, for any $a \in \ker(L_1)$, the equation $D_aF(x) = b$ becomes $D_aG(x) = b$, for any b. This is to say that D_aF is 2-to-1, for all $a \in \ker(L_1)^*$. Then Theorem 10 applies. ◇

Example 4 *Let $n = 2k$ and set:*
– $L_1(x) = T_2^n(x)$, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^2}$,
– $L_2(x) = Tr(x)$, the absolute trace on $\mathbb{F}_{2^n}$.
Let $F(x) = G(x) + L_1(x)L_2(x)$, where G is any APN function.

Since $Tr(x) = T_1^2(T_2^n(x))$, the kernel of L_1 is included in the kernel of L_2. We apply Corollary 5 with $t = n - 2$, the dimension of $\ker(L_1)$. *Hence $\delta(F) \leq 4$.*

Problem 3 *Two questions arise naturally, regarding functions F of Corollary 5, namely possible permutations and possible APN functions. Another problem is to find constructions, which are not derived from APN functions, as in Example 3.*

7 Particular functions

In this section, we study the values λ_3 and λ_4 for two types of vectorial functions, the differentially two-valued functions and the plateaued functions. Recall that these kinds of functions are defined in Section 2.1. The next proposition is a generalization of [3, Proposition 5], where this result was obtained for monomial functions.

Proposition 5 *Let F be a differentially two-valued function over $\mathbb{F}_{2^n}$, with differential uniformity $\delta(F) = 2^s$, where $s > 1$. Then the numbers of codewords of weight 3 and 4 of C_F satisfy*

$$\lambda_3 = \frac{N(2^{s-1}-1)}{3} \quad \textit{and} \quad \lambda_4 = (2^{n-2}-1)\lambda_3.$$

Thus $\lambda_4 \neq 0$ if and only if $\lambda_3 \neq 0$.

Proof. Note that the function F is differentially two-valued if and only the derivative D_aF is 2^s-to-1 for any $a \in \mathbb{F}_{2^n}^*$. According to Theorem 7, this holds if and only if

$$\lambda_3 + \lambda_4 = \frac{2^{n-2}N(2^{s-1}-1)}{3}.$$

Moreover, λ_3 is directly obtained from (i) of Theorem 5, since any $T_{a,F(a)}$ has size $\kappa_{a,F(a)} = 2^{s-1}$. To conclude, we compute

$$\lambda_4 = \frac{2^{n-2}N(2^{s-1}-1)}{3} - \frac{N(2^{s-1}-1)}{3} = (2^{n-2}-1)\lambda_3.$$

$\diamond$

As announced by Theorem 7, the higher bound on $\lambda_3 + \lambda_4$ is reached by differentially two-valued functions only. Moreover, λ_3 reaches its upper bound too. Notably, if $s = 2$ then $\lambda_3 = N/3$ and $\lambda_4 = N(2^{n-2} - 1)/3$, where both values must be non-zero integers, which is impossible when n and (then) $n-2$ are odd. More generally, n odd would imply s odd. Note that the next result is a generalization of [3, Corollary 3].

Corollary 6 *Let F be a differentially two-valued function over $\mathbb{F}_{2^n}$ such that $\delta(F) = 2^s$. If s is even, then n must be even too. In particular, F cannot be differentially 4-uniform when n is odd.*

Until the end of this section, F is a *plateaued function* over $\mathbb{F}_{2^n}$. Thus every component f_μ of F satisfies

$$L(f_\mu) = 2^{\frac{n+t_\mu}{2}},\ 0 \le t_\mu \le n-2, \text{where } t_\mu + n \text{ is even.} \tag{24}$$

We begin by giving a result derived from Theorem 9.

Corollary 7 *Assume that F is a plateaued function over $\mathbb{F}_{2^n}$, with components satisfying (24) above. Then*

$$\lambda_3 + \lambda_4 = \frac{2^{n-3}}{3} \sum_{\mu \in \mathbb{F}_{2^n}^*} (2^{t_\mu} - 2).$$

Proof. Since every f_μ is plateaued, we have from Theorem 1

$$\nu(f_\mu) = 2^{2n+t_\mu},\ \mu \in \mathbb{F}_{2^n}^*.$$

Hence, from Theorem 9,

$$\sum_{\mu \in \mathbb{F}_{2^n}^*} \nu(f_\mu) = \sum_{\mu \in \mathbb{F}_{2^n}^*} 2^{2n+t_\mu} = (2^n - 1)2^{2n+1} + 3 \times 2^{n+3}(\lambda_3 + \lambda_4),$$

so that

$$\lambda_3 + \lambda_4 = \frac{2^{2n}}{3 \times 2^{n+3}} \left(\sum_{\mu \in \mathbb{F}_{2^n}^*} 2^{t_\mu} - 2(2^n - 1) \right) = \frac{2^{n-3}}{3} \sum_{\mu \in \mathbb{F}_{2^n}^*} (2^{t_\mu} - 2).$$

$\diamond$

Theorem 11 *Let F be a plateaued function with components satisfying (24) above. Then*

$$\lambda_3 = \frac{1}{6} \sum_{\mu \in \mathbb{F}_{2^n}^*} (2^{t_\mu} - 2) \text{ and } \lambda_4 = (2^{n-2} - 1)\lambda_3.$$

Consequently, $\lambda_4 \neq 0$ if and only if $\lambda_3 \neq 0$. If F is plateaued with single amplitude $2^{(n+t)/2}$, then $\lambda_3 = (2^{t-1} - 1)N/3$.

Proof. For any μ, we have:

$$\sum_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}} (-1)^{Tr(\mu D_a D_b F(x))} = 2^{n+t_\mu}, \text{ for all } x \in \mathbb{F}_{2^n}.$$

This was proved by [9, Theorem 1], for plateaued Boolean functions. This result holds for any characteristic (see [15, Theorem 2]). Thus we have

$$\begin{aligned} \sum_{\mu \in \mathbb{F}_{2^n}^*} 2^{n+t_\mu} &= \sum_{\mu \in \mathbb{F}_{2^n}^*} \sum_{a,b} (-1)^{Tr(\mu D_a D_b F(x))} \\ &= \sum_{a,b} \sum_{\mu \in \mathbb{F}_{2^n}} (-1)^{Tr(\mu D_a D_b F(x))} - 2^{2n}. \end{aligned}$$

Denoting the last value on the right by A_1, we get

$$A_1 = 2^n |\{ \ (a,b) \mid D_a D_b F(x) = 0 \ \}| - 2^{2n},$$

and removing the trivial cases we obtain

$$A_2 = |\{ \ (a,b) \mid D_a D_b F(x) = 0, a \neq b \neq x \ \}|$$

as follows:

$$A_1 = 2^n(2^n + 2^{n+1} - 2) + 2^n A_2 - 2^{2n} = 2^n(2^{n+1} - 2) + 2^n A_2.$$

For $x = 0$, we obtain the number of codewords of weight 3, that is $\lambda_3 = A_2/6$. Indeed, according to (9), A_2 is then the number of codewords of C_F with locators $\{a, b, a+b\}$, $a \neq b \neq 0$, where every codeword is counted six times. Finally, we obtain

$$\lambda_3 = \frac{A_2}{6} = \frac{\sum_{\mu \in \mathbb{F}_{2^n}^*} 2^{t_\mu} - 2(2^n - 1)}{6}.$$

When $t_\mu = t$ for all μ, then $\lambda_3 = ((2^n-1)(2^t-2))/6$. Now, to get λ_4, we use Corollary 7:

$$\begin{aligned}\lambda_4 &= \frac{2^{n-3}}{3}\sum_{\mu\in\mathbb{F}_{2^n}^*}(2^{t_\mu}-2)-\lambda_3 \\ &= \sum_{\mu\in\mathbb{F}_{2^n}^*}(2^{t_\mu}-2)\left(\frac{2^{n-3}}{3}-\frac{1}{6}\right)=\frac{1}{6}\left(\sum_{\mu\in\mathbb{F}_{2^n}^*}(2^{t_\mu}-2)\right)(2^{n-2}-1),\end{aligned}$$

completing the proof. ◇

Remark 5 *Let F be a plateaued function, whose components f_μ have amplitude $2^{(n+t_\mu)/2}$, $0 \le t_\mu \le n-2$. Note that $t_\mu = 0$ if and only if f_μ is a bent function.*

If n is odd then $t_\mu > 0$. From Corollary 7, we obtain this well-known result: F is APN if and only if $t_\mu = 1$ for all μ. *When n is even, we obtain a property on the number of bent components of F.*

Proposition 6 *Let F be a plateaued function over $\mathbb{F}_{2^n}$. Let n be even, and denote by B the number of bent components of F. Then F is APN if and only if*

$$B=\sum_{\mu\in\mathbb{F}_{2^n}^*,t_\mu>0}(2^{t_\mu}-2).$$

Consequently, $\sum_{\mu\in\mathbb{F}_{2^n}^*,t_\mu>0}(2^{t_\mu-1}-1) \ge (2^n-1)/3$ with equality if and only if $t_\mu = 2$, for all non zero t_μ.

Proof. We obtain directly the value B by applying Theorem 11 with $\lambda_3 = 0$. Further, the lower bound of B was given by [1, Corollary 3], a result which is here completed. ◇

When F is plateaued, the numbers of codewords of weight 3 and 4 of C_F satisfy the same relationship (between λ_4 and λ_3) as for a differentially two-valued function. Moreover, if F is plateaued with single amplitude $2^{(n+t)/2}$ and, at the same time, differentially two-valued $\{0, 2^s\}$, we get

$$\lambda_3=\frac{(2^{t-1}-1)N}{3}=\frac{N(2^{s-1}-1)}{3}.$$

Clearly, in this case $t = s$, where s has the same parity as t. A similar result was proved for monomial plateaued functions by [3, proposition 6]. Here we can generalize to plateaued functions a property of quadratic functions that we proved in [11, Theorem 8].

Corollary 8 *Let F be a plateaued function over $\mathbb{F}_{2^n}$, which is with single amplitude $2^{(n+t)/2}$ and differentially two-valued $\{0, 2^s\}$. Then $t = s$ where $s + n$ must be even.*

Remark 6 *Quadratic functions are plateaued and not always differentially two-valued, unless they are monomial. A binary code C is said invariant by translation when any codeword of C given by its locators, say $X = (x_1, \ldots, x_k)$, satisfies*

$$(g+x_1, \ldots, g+x_k) \in C \quad \text{for all } g \in \mathbb{F}_{2^n}.$$

Let F be quadratic and consider its extended code $\overline{C_F}$. The extended code $\overline{C_F}$ of C_F is obtained by adding a position "0" and a digit $\overline{c} = \sum_{i=0}^{N-1} c_i$ on this position to any codeword $c \in C_F$. Clearly all codewords of $\overline{C_F}$ have an even weight. If F is quadratic, then $\overline{C_F}$ is invariant by translation, and one deduce easily that $\lambda_4 = (2^{n-2} - 1)\lambda_3$ (by extending the proof of [8, Lemma 3]).

Some, but still too few, monomials are known to be plateaued and not quadratic. We end this section by an example, which illustrates the following property, directly derived from the previous theorem.

Corollary 9 *Let F be a plateaued function over $\mathbb{F}_{2^n}$, which is with single amplitude $2^{(n+2)/2}$, with n even. Then $\lambda_3 = N/3$.*

Example 5 *Let $n = 2m$ with $m \geq 5$ being odd. The functions defined as*

$$F_d(x) = x^d, \ d = 2^m + 2^{(m+1)/2} + 1 \text{ and } d = 2^{m+1} + 3,$$

are known to be plateaued, bijective and with single amplitude $2^{(n+2)/2}$ [13]. Further, the differential spectrum of F_d was computed in [19] confirming that $\delta(F_d) = 8$ and all values $0, 2, 4, 6, 8$ appear in this spectrum, for both values of d.

We get $\lambda_3 = N/3$ and $\lambda_4 = (2^{n-2} - 1)N/3$. Thus, both functions have only one codeword of weight 3, which is shifted $N/3$ times. Moreover, codewords of weight 3 do not intersect and $\delta(1) = 4$, as expected (from Corollary 2). Thus, according to Theorem 4, there are pairs of codewords of weight 4 such that their sum has weight 4. This is because $\delta(F_d) > 4$.

8 Conclusion

In this paper, we initiate another approach for the study of the differential uniformity of any function F, by replacing it in coding theory. Our purpose was first to establish clearly the relations between the differential uniformity of F, the codewords of weight 3 and 4 and some cosets of the code C_F associated to F. But we still believe that this point of view needs to use together classical tools for the study of functions over $\mathbb{F}_{2^n}$ and of Boolean functions. This paper extends the work on APN functions and their associated codes presented in [8]. More recently, some studies on equivalent APN functions have shown that the properties of these associated codes are of interest (see [5], [6] and references herein). The study of algebraic and combinatorial properties of the code C_F opens up a wide sphere of knowledge.

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy, On almost perfect nonlinear functions over F_2^n, *IEEE Transactions on Information Theory*, 52(9):4160–4170, 2006.

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

[3] C. Blondeau, A. Canteaut and P. Charpin, Differential properties of power functions, *Int. J. of Information and Coding Theory*, 1(2):149–170, 2010. Special Issue dedicated to Vera Pless.

[4] C. Blondeau, A. Canteaut and P. Charpin, Differential properties of $x \mapsto x^{2^t-1}$, *IEEE Transactions on Information Theory*, 57(12):8127–8137, 2011.

[5] C. Bracken, E. Byrne, G. Mcguire and G. Nebe, On the equivalence of quadratic APN functions, *Des. Codes Cryptogr.*, 61:261–272, 2011.

[6] A. Canteaut and L. Perrin, On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting, Cryptology ePrint Archiv, 2018/713.

[7] C. Carlet, Boolean and Vectorial Plateaued Functions and APN Functions, *IEEE Transactions on Information Theory*, 61(11): 6272–6289, 2015.

[8] C. Carlet, P. Charpin, and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[9] C. Carlet and E. Prouff, On plateaued functions and their constructions, in Proc. of *Fast Software Encryption-FSE'03 (Lecture Notes in Computer Science)*, T. Johansson (Ed.), Springer-Verlag, 2887:54–73, 2003.

[10] P. Charpin and G. Kyureghyan, On sets determining the differential spectrum of mappings, *Int. J. of Information and Coding Theory*, Special Issue on the honor of Gerard Cohen, 4(2/3):170–184, 2017.

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

[12] P. Charpin, A. Tietäväinen and V. Zinoviev, On binary cyclic codes with minimum distance $d = 3$, *Problems of Information Transmission*, 33(4):287-296, 1997.

[13] T. Cusick and H. Dobbertin, Some new three-valued crosscorrelation functions for binary m-sequences, *IEEE Transactions on Information Theory*, 42(4):1238-1240, 1996.

[14] F. Macwilliams and N. Sloane, *The theory of Error Correcting Codes.* Amsterdam, The Netherlands: North-Holland, 1977.

[15] S. Mesnager, F. Ozbudak, A. Sinak and G. Cohen, On q-ary plateaued functions over F_q and their explicit characterizations functions, to appear in *European Journal of Combinatorics.*

[16] K. Nyberg, S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity, In Proc. of *Fast Software Encryption-FSE'94 (Lecture Notes in Computer Science).* Berlin, Germany: Springer-Verlag, 1008:111-130, 1995.

[17] V. Pless, R. Brualdi and W. Huffman, *Handbook of coding theory*. Elsevier Science Inc. New York, USA, 1998.

[18] A. Pott, E. Pasalic, A. Muratovic-Ribic and S. Bajric, On the maximum number of bent component of vectorial functions, *IEEE Transactions on Information Theory*, 64(1):403-411, 2018.

[19] M. Xiong, H. Yan and P. Yuan, On a conjecture of differentially 8-uniform power functions, *Des. Codes Cryptogr.*, 86(8):1601-1621, 2018.

[20] Y. Zheng and X. Zhang, Plateaued functions, In *Information and Communication Security-ICICS'99 (Lecture Notes in Computer Science)*, Springer-Verlag, 1726:284–300, 1999.