Characterizations of the differential uniformity of vectorial functions by the Walsh transform

Claude Carlet

LAGA, Department of Mathematics, University of Paris 8
(and Paris 13 and CNRS), Saint–Denis cedex 02, France.
E-mail: claude.carlet@univ-paris8.fr

Abstract. For every positive integers n, m and every even positive integer δ, we derive inequalities satisfied by the Walsh transforms of all vectorial (n, m)-functions and prove that the case of equality characterizes differential δ-uniformity. This provides a generalization to all differentially δ-uniform functions of the characterization of APN (n, n)-functions due to Chabaud and Vaudenay, by means of the fourth moment of the Walsh transform. Such generalization has been missing since the introduction of the notion of differential uniformity by Nyberg in 1994 and since Chabaud-Vaudenay's result the same year.

For each even $\delta \geq 2$, we find several such characterizations. In particular, when $\delta = 2$ and $\delta = 4$, we have that, for any (n, n)-function (resp. any $(n, n-1)$-function), the arithmetic mean of $W_F^2(u_1, v_1)W_F^2(u_2, v_2)W_F^2(u_1 + u_2, v_1 + v_2)$ when u_1, u_2 range independently over $\mathbb{F}_2^n$ and v_1, v_2 are nonzero and distinct and range independently over $\mathbb{F}_2^m$, is at least 2^{3n}, and that F is APN (resp. is differentially 4-uniform) if and only if this arithmetic mean equals 2^{3n} (which is the value we would get with a bent function if such function could exist).

These inequalities give more knowledge on the Walsh spectrum of (n, m)-functions. We deduce in particular a property of the Walsh support of highly nonlinear functions. We also consider the completely open question of knowing if the nonlinearity of APN functions is necessarily non-weak (as it is the case for known APN functions); we prove new lower bounds which cover all power APN functions (and hence a large part of known APN functions), which explain why their nonlinearities are rather good, and we discuss the question of the nonlinearity of APN quadratic functions (since almost all other known APN functions are quadratic).

Keywords: Boolean function, vectorial function, Walsh–Hadamard transform, APN function, differential uniformity, nonlinearity.

1 Introduction

The notions of APN function and more general differentially uniform functions have been introduced by Nyberg [14]. These functions play a major role for the design of substitution boxes (S-boxes) in block ciphers. The differential uniformity of a vectorial function quantifies the contribution of the function to the resistance against differential cryptanalysis, when it is used as an S-box in a block cipher. APN functions, that is, differentially 2-uniform functions, have best possible differential uniformity in characteristic two, but very few classes of APN functions are known. Most known APN functions have potential drawbacks, and a differentially 4-uniform function has then been used as S-box in the AES (and is used in many more recent block ciphers). APN functions are nicely characterized by their Walsh transform but no such characterization is known for differentially δ-uniform functions when $\delta \geq 4$. This contributes to the fact that the structure of the set of differentially δ-uniform (n,m)-functions is still less well understood than that of the subset of APN (n,n)-functions, even in the subcase of differentially 4-uniform $(n,n-1)$-functions (while these functions are optimal, as are APN (n,n)-functions, which means that their structure is probably simpler than that of general differentially 4-uniform functions). In this paper, for all (n,m)-functions and every even δ, we prove in Theorem 3.1 an inequality involving the values at $(0,0)$ of the convolutional products of orders at most $\frac{\delta}{2}+1$ of their squared Walsh transforms, and we characterize differentially δ-uniform (n,m)-functions as those for which this is an equality. For $\delta = 2$, this characterization is not new: it is the characterization mentioned above. For $\delta \geq 4$, it is a new characterization, which in the case of $\delta = 4$ is rather simple (as explicited in Corollary 5.1), and becomes more and more complex as δ increases. We observe (Proposition 3.6) that several similar characterizations can be obtained, some of which can have a simpler expression than others. For $\delta = 2$ and $m = n$, we have in particular a new characterization of APN functions (Theorem 5.2) which is the same (except for the number of output bits) as a characterization (Theorem 5.11) for the case $\delta = 4$ and $m = n-1$. This gives more insight on the Walsh transform of APN (n,n)-functions and differentially 4-uniform $(n,n-1)$-functions and it shows a similarity between them, which illustrates the fact that they are, in both cases, optimal functions from the viewpoint of the resistance to the differential attacks against those block ciphers in which they are used as substitution boxes. We deduce from our inequalities a new property of the Walsh support of highly nonlinear vectorial functions and we consider the open question of determining if the nonlinearity of APN functions could be low in some cases to be found. We prove new lower bounds (Theorem 5.8) on the nonlinearity of power APN functions and we study the nonlinearity of quadratic APN functions. This partly shows that the rather good nonlinearity of known APN functions may be related to the singularity of these functions (which are almost all either power functions or quadratic). We go into slightly more technical details on differentially 4-uniform functions, and in the last section, we explicit the characterization of Theorem 3.1 for $\delta = 6$.

2 Preliminaries

Given two positive integers n, m, any vectorial function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ (i.e. any (n,m)-function) has a unique algebraic normal form $F(x_1, \ldots, x_n) = \sum_{I \subseteq \{1,\ldots,n\}} a_I \prod_{i \in I} x_i$, where $a_I \in \mathbb{F}_2^m$, and whose global degree is called the algebraic degree of F. We say that F is quadratic if its algebraic degree is at most 2 (and F is affine if and only if its algebraic degree is at most 1). If $\mathbb{F}_2^n$ is identified with the field $\mathbb{F}_{2^n}$ (thanks to the fact that this field is an n-dimensional $\mathbb{F}_2$-vector space) and if m divides n, then F has also a unique univariate polynomial representation $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, where

$a_i \in \mathbb{F}_{2^n}$. The algebraic degree equals then the maximum Hamming weight of the binary expansion of those exponents i with nonzero coefficients a_i.

Given a third positive integer δ, function F is called *differentially δ-uniform*, see [14], if for every nonzero $a \in \mathbb{F}_2^n$ and every $z \in \mathbb{F}_2^m$, there exist at most δ solutions to the equation $D_aF(x) = z$, where $D_aF(x) = F(x)+F(x+a)$ is a so-called derivative of F. This notion is invariant under some equivalences that we present in increasing order of generality. Two functions are called *linearly equivalent* (resp. *affine equivalent*) if one is equal to the other, composed on the left and on the right by linear (resp. affine) permutations. They are called *extended affine equivalent* (EA-equivalent) if one is affine equivalent to the other, added with an affine function. They are called *CCZ-equivalent* (see [2, 9]) if their graphs $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = F(x)\}$ and $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y = G(x)\}$ are affine equivalent.

Differentially δ-uniform functions exist only if $\delta \geq 2^{n-m}$ when $n > m$ and if $\delta \geq 2$ when $n \leq m$. Differentially 2^{n-m}-uniform (n, m)-functions, which are optimal with respect to differential uniformity and are called *perfect nonlinear* (PN), happen to be the same functions as the so-called bent (vectorial) functions, whose nonlinearity equals the optimal value $2^{n-1}-2^{\frac{n}{2}-1}$ (n even). The nonlinearity of an (n, m)-function F is the minimum Hamming distance between all its component functions $v{\cdot}F$, where "$\cdot$" is some inner product in $\mathbb{F}_2^m$ and $v \neq 0$, and all affine Boolean functions over $\mathbb{F}_2^n$ (that is, all affine $(n, 1)$-functions). It is related to the Walsh transform (also called Walsh-Hadamard transform) of F:

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

related to the choices of some inner products in $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, both denoted by " $\cdot$ ", by the relation:

$$nl(F) = 2^{n-1} - \frac{1}{2} \max_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m, v\neq 0} |W_F(u, v)|. \tag{1}$$

The nonlinearity is invariant under all equivalences described above. PN functions exist if and only if n is even and $m \leq n/2$ (see [13]). For $m = n$, differentially 2-uniform functions are the optimal functions with respect to differential uniformity, and are called *almost perfect nonlinear* (APN). All known APN functions are given by expressions in the field $\mathbb{F}_{2^n}$. The inner product in this field can be taken equal to $u \cdot x = tr_1^n(ux)$, where tr_1^n is the absolute trace function $tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$. Most known APN functions are power functions, listed in Table 1.

We know from [10] that, given any (n, n)-function, the Walsh transform satisfies

$$\sum_{u\in\mathbb{F}_2^n; v\in\mathbb{F}_2^m} W_F^4(u, v) \geq 3 \cdot 2^{4n} - 2^{3n+1}, \tag{2}$$

and that it is APN if and only if Relation (2) is an equality. This allows for instance proving for n odd that any plateaued (in particular, quadratic) APN (n, n)-function is AB [3]. An (n, m)-function is called *plateaued* if, for every nonzero $v \in \mathbb{F}_2^m$, its

Table 1. Known APN power functions x^d on $\mathbb{F}_{2^n}$.

Functions	Exponents d	Conditions
Gold	$2^i + 1$	$\gcd(i, n) = 1$
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$
Welch	$2^t + 3$	$n = 2t + 1$
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$
Inverse	$2^{2t} - 1$	$n = 2t + 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$

Walsh transform $W_F(u, v)$ takes its values in $\{0, \pm\lambda_v\}$ when u ranges over $\mathbb{F}_2^n$, where λ_v (called the *amplitude* of the component function $v \cdot F$) is some integer depending only on v (λ_v is then necessarily a power of 2 whose exponent is larger than or equal to $\frac{n}{2}$). An (n, n)-function is called *almost bent* (AB) if it is plateaued with the single amplitude $\lambda_v = 2^{\frac{n+1}{2}}$, $\forall v \neq 0$ (n odd). It has then optimal nonlinearity. Surveys on APN and AB functions can be found in [1, 6]. Characterizations of plateaued functions are given in [7, 12].

Relation (2) and the inequality $\max_{u \in \mathbb{F}_2^n; v \in \mathbb{F}_2^m, v \neq 0} W_F^2(u, v) \geq \frac{\sum_{u \in \mathbb{F}_2^n; v \in \mathbb{F}_2^m} W_F^4(u,v) - 2^{4n}}{\sum_{u \in \mathbb{F}_2^n; v \in \mathbb{F}_2^m} W_F^2(u,v) - 2^{2n}}$ allow showing the Sidelnikov-Chabaud-Vaudenay (SCV) bound [10] (the name of this bound is explained in [6]), stating in the case $m = n$ that the nonlinearity of an (n, n)-function is at most $2^{n-1} - 2^{\frac{n-1}{2}}$. This bound is tight for n odd; equality is achieved by AB functions. Relation (2) does not seem to allow to deduce a lower bound on the nonlinearity of APN functions. Every AB function is APN since Inequality (2) is then an equality (indeed, the Parseval relation $\sum_{u \in \mathbb{F}_2^n} W_F^2(u, v) = 2^{2n}$, valid for every v, shows that for each $v \neq 0$, there are 2^{n-1} elements u such that $W_F^2(u, v) = 2^{n+1}$). The converse is not true in general, but it is true when all the Walsh transform values of F are divisible by 2^{n+1}, with n odd, in particular for plateaued functions, for instance for quadratic functions.

There exists an inequality similar to (2) for $m \neq n$ (we shall obtain it again as a particular case below) but the case of equality is impossible. We know that no differentially 2-uniform (n, m)-function exists for $m < n$ (except for $m = n - 1$ and $n = 2$), according to the results by Nyberg recalled above.

In the next section, we shall use the *inverse Fourier transform formula*: let φ be a function from $\mathbb{F}_2^n$ to $\mathbb{Z}$ (or $\mathbb{R}$ or $\mathbb{C}$) and $\widehat{\varphi}(a) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{a \cdot x}$ its *Fourier transform*, we have, for every $b \in \mathbb{F}_2^n$ that $\sum_{a \in \mathbb{F}_2^n} \widehat{\varphi}(a)(-1)^{a \cdot b} = 2^n \varphi(b)$.

3 A characterization of differentially δ-uniform functions

Let δ be any positive even integer. It is well-known that, for every (n, m)-function F, every nonzero $a \in \mathbb{F}_2^n$ and every $z \in \mathbb{F}_2^m$, the size $|\{x \in \mathbb{F}_2^n; D_a F(x) = z\}|$ is even, since if x belongs to this set then $x + a$ does too. Hence, a function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is differentially δ-uniform if and only if, for every $a \neq 0$ in $\mathbb{F}_2^n$ and every $z \in \mathbb{F}_2^m$, we have $|\{x \in \mathbb{F}_2^n; D_aF(x) = z\}| \in \{0, 2, 4, \ldots, \delta\}$. If z is not the image of an element of $\mathbb{F}_2^n$ by D_aF, then we have $|\{x \in \mathbb{F}_2^n; D_aF(x) = z\}| = 0$. We can then restrict the condition above to those z of the form $D_aF(b)$, $b \in \mathbb{F}_2^n$. Any (n, m)-function F is then differentially δ-uniform if and only if, for every $a \neq 0$ in $\mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$, we have $|\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}| \in \{2, 4, \ldots, \delta\}$. Since we have $\prod_{i=1}^{\delta/2}(X - 2i) = 0$ for $X = 2, 4, \ldots, \delta$ and $\prod_{i=1}^{\delta/2}(X - 2i) > 0$ for every even $X > \delta$, writing $\prod_{i=1}^{\delta/2}(X - 2i) = \sum_{j=0}^{\delta/2} A_j X^j$, we have for every (n, m)-function F and every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$ that

$$\sum_{j=0}^{\delta/2} A_j \, |\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}|^j \geq 0,$$

and F is differentially δ-uniform if and only if this inequality is an equality for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$. Hence, any (n, m)-function F satisfies:

$$\sum_{j=0}^{\delta/2} A_j \sum_{a,b \in \mathbb{F}_2^n, a \neq 0} |\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}|^j \geq 0,$$

with equality if and only if F is differentially δ-uniform. We shall now characterize this condition by means of the Walsh transform. We have:

$$|\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}| = 2^{-m} \sum_{x \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m} (-1)^{v \cdot (D_aF(x) + D_aF(b))},$$

and therefore, for $j \geq 1$:

$$\sum_{a,b \in \mathbb{F}_2^n, a \neq 0} |\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}|^j =$$

$$\sum_{a,b \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}|^j - 2^{n(j+1)} =$$

$$2^{-jm} \sum_{a,b \in \mathbb{F}_2^n} \sum_{\substack{x_1, \ldots, x_j \in \mathbb{F}_2^n \\ v_1, \ldots, v_j \in \mathbb{F}_2^m}} (-1)^{\sum_{i=1}^j v_i \cdot (D_aF(x_i) + D_aF(b))} - 2^{n(j+1)} =$$

$$2^{-jm} \sum_{\substack{x_1, \ldots, x_j \in \mathbb{F}_2^n \\ v_1, \ldots, v_j \in \mathbb{F}_2^m}} \sum_{a,b \in \mathbb{F}_2^n} (-1)^{\sum_{i=1}^j v_i \cdot (F(x_i) + F(x_i + a) + F(b) + F(b + a))} - 2^{n(j+1)}.$$

To make the connection with the Walsh transform, we use that $\sum_{u_i \in \mathbb{F}_2^n} (-1)^{u_i \cdot (x_i + y_i + a)}$ (respectively $\sum_{u_0 \in \mathbb{F}_2^n} (-1)^{u_0 \cdot (a + b + c)}$) is nonzero for $y_i = x_i + a$ only (respectively $c = a + b$) and takes then value 2^n, and we deduce:

$$2^{jm + (j+1)n} \left(\sum_{a,b \in \mathbb{F}_2^n, a \neq 0} |\{x \in \mathbb{F}_2^n; D_aF(x) = D_aF(b)\}|^j + 2^{n(j+1)} \right) =$$

$$\sum_{a,b,c\in\mathbb{F}_2^n}\ \sum_{\substack{x_1,\dots,x_j,y_1,\dots,y_j\in\mathbb{F}_2^n\\ u_0,u_1,\dots,u_j\in\mathbb{F}_2^n,v_1,\dots,v_j\in\mathbb{F}_2^m}} (-1)^{\sum_{i=1}^j[v_i\cdot(F(b)+F(c)+F(x_i)+F(y_i))+u_i\cdot(x_i+y_i+a)]+u_0\cdot(a+b+c)}.$$

Then since $\sum_{b\in\mathbb{F}_2^n}(-1)^{v\cdot F(b)+u\cdot b}=W_F(u,v)$, this latter expression equals:

$$\sum_{\substack{u_0,u_1,\dots,u_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}} W_F^2\left(u_0,\sum_{i=1}^j v_i\right)\prod_{i=1}^j W_F^2(u_i,v_i)\sum_{a\in\mathbb{F}_2^n}(-1)^{(\sum_{i=0}^j u_i)\cdot a}=$$

$$2^n\sum_{\substack{u_1,\dots,u_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}} W_F^2\left(\sum_{i=1}^j u_i,\sum_{i=1}^j v_i\right)\prod_{i=1}^j W_F^2(u_i,v_i),$$

since $\sum_{a\in\mathbb{F}_2^n}(-1)^{u\cdot a}=0$ if $u\neq 0$.

Note that $\sum_{\substack{u_1,\dots,u_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}} W_F^2\left(\sum_{i=1}^j u_i,\sum_{i=1}^j v_i\right)\prod_{i=1}^j W_F^2(u_i,v_i)$ equals $W_F^2\otimes\cdots\otimes W_F^2(0,0)$ where $\otimes$ denotes the convolutional product and where the number of terms W_F^2 equals $j+1$. We shall denote such multiple convolutional product by: $(W_F^2)^{\otimes(j+1)}$.

For $j=0$, we have $\sum_{a,b\in\mathbb{F}_2^n,a\neq 0}|\{x\in\mathbb{F}_2^n; D_aF(x)=D_aF(b)\}|^j=2^n(2^n-1)$. We deduce:

Theorem 3.1 *Let n, m and δ be positive integers, with δ even, and let F be any (n,m)-function. Let $A_0,\dots,A_{\delta/2}$ be defined by the polynomial equality:*

$$\prod_{i=1}^{\delta/2}(X-2i)=\sum_{j=0}^{\delta/2}A_jX^j.$$

Then we have:

$$2^n(2^n-1)A_0+\sum_{j=1}^{\delta/2}2^{-j(n+m)}A_j\left((W_F^2)^{\otimes(j+1)}(0,0)-2^{(2j+1)n+jm}\right)\geq 0, \qquad (3)$$

where $^{\otimes(j+1)}$ denotes the convolutional product iterated $j+1$ times, that is:

$$(W_F^2)^{\otimes(j+1)}(0,0)=\sum_{\substack{u_1,\dots,u_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}} W_F^2\left(\sum_{i=1}^j u_i,\sum_{i=1}^j v_i\right)\prod_{i=1}^j W_F^2(u_i,v_i).$$

Moreover, this inequality is an equality if and only if F is differentially δ-uniform.

Remark 3.2 *If, instead of writing $\prod_{i=1}^{\delta/2}(X-2i)=\sum_{j=0}^{\delta/2}A_jX^j$ as above, we write $\prod_{i=0}^{\delta/2}(X-2i)=\sum_{j=0}^{\delta/2}A_jX^{j+1}$, then with the same method, we have the inequality*

$\sum_{j=0}^{\delta/2} A_j \sum_{a\in\mathbb{F}_2^n, z\in\mathbb{F}_2^m, a\neq 0} |\{x\in\mathbb{F}_2^n; D_aF(x)=z\}|^{j+1}\geq 0$, which is an equality if and only if F is differentially δ-uniform. We have $\displaystyle\sum_{a\in\mathbb{F}_2^n, z\in\mathbb{F}_2^m, a\neq 0} |\{x\in\mathbb{F}_2^n; D_aF(x)=z\}|^{j} =$ $\displaystyle 2^{-jm}\sum_{\substack{x_1,\dots,x_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}}\ \sum_{a\in\mathbb{F}_2^n, z\in\mathbb{F}_2^m} (-1)^{\sum_{i=1}^j v_i\cdot(F(x_i)+F(x_i+a)+z)} - 2^{nj}$, for $j\geq 1$. We deduce

$$2^{jm+jn}\left(\sum_{a\in\mathbb{F}_2^n, z\in\mathbb{F}_2^m, a\neq 0} |\{x\in\mathbb{F}_2^n; D_aF(x)=z\}|^{j} + 2^{nj}\right) =$$

$$\sum_{\substack{u_1,\dots,u_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}} \prod_{i=1}^{j} W_F^2(u_i,v_i) \sum_{a\in\mathbb{F}_2^n} (-1)^{(\sum_{i=1}^j u_i)\cdot a} \sum_{z\in\mathbb{F}_2^n} (-1)^{(\sum_{i=1}^j v_i)\cdot z} =$$

$$2^{n+m} \sum_{\substack{u_1,\dots,u_{j-1}\in\mathbb{F}_2^n\\ v_1,\dots,v_{j-1}\in\mathbb{F}_2^m}} W_F^2\left(\sum_{i=1}^{j-1} u_i, \sum_{i=1}^{j-1} v_i\right) \prod_{i=1}^{j-1} W_F^2(u_i,v_i),$$

and this gives the same result as in Theorem 3.1.

Remark 3.3 *As recalled in Section 2, we know that an (n,m)-function F is PN, that is, $|\{x\in\mathbb{F}_2^n; D_aF(x)=D_aF(b)\}| = 2^{n-m}$ for every nonzero $a\in\mathbb{F}_2^n$ and every $b\in\mathbb{F}_2^n$, if and only if F is bent, that is, $W_F^2(u,v)=2^n$ for every u and every $v\neq 0$. This equivalence is valid independently of the existence of such functions, which happens only for n even and $m\leq n/2$. Hence, since for every even $\delta\geq 2^{n-m}$, with $n>m$ (so that 2^{n-m} is also even), every PN function is differentially δ-uniform, if we replace in (3) $W_F^2(u,v)$ by 2^n for every u and every $v\neq 0$, by 2^{2n} for $v=0$ and $u=0$ and by 0 for $v=0$ and every $u\neq 0$, we obtain an equality.*

Remark 3.4 *It is well-known that the convolutional product of the Fourier transforms of a sequence of functions equals the Fourier transform of the product of the functions. Here, $W_F^2(u,v)$ equals $2^{-(n+m)}$ times the Fourier transform of the function $(a,b)\mapsto \sum_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m} W_F^2(u,v)(-1)^{a\cdot u+b\cdot v}$. This allows transforming the terms $(W_F^2)^{\otimes(j+1)}(0,0)$ into powers in Relation (3). In fact, this can be done in an elementary way:*

$$(W_F^2)^{\otimes(j+1)}(0,0) = \sum_{\substack{u_1,\dots,u_j\in\mathbb{F}_2^n\\ v_1,\dots,v_j\in\mathbb{F}_2^m}} W_F^2\left(\sum_{i=1}^{j} u_i, \sum_{i=1}^{j} v_i\right) \prod_{i=1}^{j} W_F^2(u_i,v_i) =$$

$$2^{-(n+m)} \sum_{\substack{a,u_1,\dots,u_j,u_{j+1}\in\mathbb{F}_2^n\\ b,v_1,\dots,v_j,v_{j+1}\in\mathbb{F}_2^m}} (-1)^{a\cdot\sum_{i=1}^{j+1} u_i + b\cdot\sum_{i=1}^{j+1} v_i} \left(\prod_{i=1}^{j+1} W_F^2(u_i,v_i)\right) =$$

$$2^{-(n+m)} \sum_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m} \left(\sum_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m} W_F^2(u,v)(-1)^{a\cdot u+b\cdot v} \right)^{j+1}.$$

Note that:

$$\sum_{\substack{u\in\mathbb{F}_2^n\\ v\in\mathbb{F}_2^m}} W_F^2(u,v)(-1)^{a\cdot u+b\cdot v} = 2^{n+m} \left|\left\{(x,y)\in(\mathbb{F}_2^n)^2;\ x+y=a \text{ and } F(x)+F(y)=b\right\}\right|.$$

Then, Theorem 3.1 could have been also proved by starting from the definition of differentially δ-uniform functions.

Remark 3.5 *Since by definition, every differentially δ-uniform function is differentially δ'-uniform for every δ' larger than δ, it satisfies a series of equalities (those corresponding to $\delta, \delta+2, \delta+4, \dots$), which provide the values of $(W_F^2)^{\otimes(j+1)}(0,0)$ for every $j \geq \delta/2$, by means of the values of these same expressions for $1 \leq j < \delta/2$.*

3.1 More formulae for characterizing differentially δ-uniform functions

According to the proof introducing Theorem 3.1, the left hand side of Inequality (3) equals:

$$\sum_{k=\delta/2+1}^{2^{n-1}} \left|\left\{(a,b)\in(\mathbb{F}_2^n)^2;\ |\{x\in\mathbb{F}_2^n;\ D_aF(x)=D_aF(b)\}|=2k\right\}\right| \prod_{i=1}^{\delta/2}(2k-2i),$$

that is, the sum of the numbers: $\left|\left\{(a,b)\in(\mathbb{F}_2^n)^2;\ |\{x\in\mathbb{F}_2^n;\ D_aF(x)=D_aF(b)\}|=2k\right\}\right|$, weighted by the coefficients $B_k=\prod_{i=1}^{\delta/2}(2k-2i)$, for $k=\delta/2+1,\dots,2^{n-1}$. Any other strictly positive coefficients B'_k instead of B_k would fit as well for a characterization of differentially δ-uniform functions, but they do not all allow a characterization by means of the Walsh transform. Indeed, we do not see how expressing the quantity $\left|\left\{(a,b)\in(\mathbb{F}_2^n)^2;\ |\{x\in\mathbb{F}_2^n;\ D_aF(x)=D_aF(b)\}|=2k\right\}\right|$ by means of the Walsh transform. However, if the coefficients B'_k equal $\phi_\delta(2k)$ for some polynomial expression ϕ_δ vanishing at $2,4,\dots,\delta$ (i.e. multiple of $\prod_{i=1}^{\delta/2}(X-2i)$) and strictly positive at $\delta+2,\dots,2^n$, then we can deduce a characterization by the Walsh transform since, in the place of the left hand side of Inequality (3), we then get:

$$\sum_{(a,b)\in(\mathbb{F}_2^n)^2} \phi_\delta\left(|\{x\in\mathbb{F}_2^n;\ D_aF(x)=D_aF(b)\}|\right),$$

and such expression can be expressed by means of the Walsh transform, similarly as above, thanks to the fact that ϕ_δ is polynomial. We deduce a generalization of Theorem 3.1:

Proposition 3.6 *Let n, m and δ be positive integers, with δ even, and let F be any (n,m)-function. Let $A'_0, \ldots, A'_{\delta/2}, A'_{\delta/2+1}, \ldots$ be defined by the polynomial equality:*

$$\prod_{i=1}^{\delta/2}(X-2i)P(X) = \sum_{j\geq 0} A'_j X^j,$$

where $P(X)$ is a polynomial taking strictly positive values at $\delta+2, \ldots, 2^n$. Then we have:

$$2^n(2^n-1)A'_0 + \sum_{j\geq 1} 2^{-j(n+m)} A'_j \left((W_F^2)^{\otimes(j+1)}(0,0) - 2^{(2j+1)n+jm}\right) \geq 0,$$

where $(W_F^2)^{\otimes(j+1)}(0,0)$ is defined in Theorem 3.1, with equality if and only if F is differentially δ-uniform.

This generalization gives simpler characterizations than (3) in some cases (but the simpler characterizations we shall deduce below from it will be also obtainable by the combination of (3) for two values of δ).

4 Characterizations in the case of $\delta = 2$ (APN functions)

Let us first check that in the case of $\delta = 2$, Theorem 3.1 gives the known characterization of APN functions. For this value of δ, we have $A_0 = -2$ and $A_1 = 1$. Inequality (3) becomes:

$$-2^{n+1}(2^n-1) + 2^{-(n+m)}\left(\sum_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m} W_F^4(u,v) - 2^{3n+m}\right) \geq 0,$$

that is:

$$\sum_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m} W_F^4(u,v) \geq 3\cdot 2^{3n+m} - 2^{2n+m+1}, \tag{4}$$

or equivalently

$$\sum_{\substack{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v) \geq 3\cdot 2^{3n+m} - 2^{2n+m+1} - 2^{4n}. \tag{5}$$

It is well-known that Inequality (5) is an equality if and only if F is APN (with $m=n$ if $n>2$, since for $m=n-1$, we know that it is impossible since F would be bent). Note that Inequality (5) gives information only for $m \geq n-1$; otherwise, the term at the right hand side is negative. For $m \leq n-2$, the only inequality we know can be derived from the Parseval relation and the Cauchy-Schwartz inequality:

$$\sum_{\substack{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v) \geq \sum_{\substack{v\in\mathbb{F}_2^m\\ v\neq 0}} \frac{\left(\sum_{u\in\mathbb{F}_2^n,} W_F^2(u,v)\right)^2}{2^n} = 2^{3n}(2^m-1).$$

Remark 4.1 *An (n,n)-function is then APN if and only if the arithmetic mean of $W_F^4(u,v)$ when u ranges over $\mathbb{F}_2^n$ and v ranges over $\mathbb{F}_2^n \setminus \{0\}$ equals 2^{3n+1}. This proves the non-existence of bent (n,n)-functions. But Inequality (5) does not prove the non-existence of bent (n,m)-functions for $n/2 < m < n$ since for such function we have $\sum_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m} W_F^4(u,v) = 2^{4n} + (2^m-1)2^{3n} \geq 3\cdot 2^{3n+m} - 2^{2n+m+1}$.*

Remark 4.2 *Note that $\sum_{\substack{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v)$ is a nonlinearity parameter, quantifying the "difference" between the function and affine functions, since it is minimal for APN functions and maximal for affine functions. Indeed, since $W_F^2(u,v) \leq 2^{2n}$ for every u,v, we have $\sum_{\substack{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v) \leq 2^{2n} \sum_{\substack{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^2(u,v) = 2^{4n}(2^m-1)$ (according to the Parseval relation) and this inequality is an equality if and only if F is affine. Being connected with the variance of the random variable W_F^2, this nonlinearity parameter is related not only to the differential attack but also to the linear attack (in a looser way than the parameter called the nonlinearity, though).*

Note that Remark 3.3 applies for $m = n-1$.

Let us now apply Proposition 3.6 in the particular case where $P(X) = X - 4 + \alpha$, with $\alpha > 0$ (so that $P(X)$ takes strictly positive values at $4, 6, \ldots$ and the hypothesis of Proposition 3.6 is satisfied). We have $A'_0 = 8 - 2\alpha$, $A'_1 = -6 + \alpha$ and $A'_2 = 1$; Proposition 3.6 gives: $2^{-2(n+m)}\left((W_F^2)^{\otimes 3}(0,0) - 2^{5n+2m}\right) - 2^{-(n+m)}(6-\alpha)\left((W_F^2)^{\otimes 2}(0,0) - 2^{3n+m}\right) \geq 2^n(2^n-1)(2\alpha-8)$, that is:

Corollary 4.3 *Let F be any (n,m)-function and $\alpha > 0$. Then*

$$(W_F^2)^{\otimes 3}(0,0) - 2^{n+m}(6-\alpha)(W_F^2)^{\otimes 2}(0,0) \geq \tag{6}$$

$$2^{5n+2m} + 2^{4n+2m}(\alpha-6) + 2^{3n+2m}(2^n-1)(2\alpha-8),$$

where

$$(W_F^2)^{\otimes 3}(0,0) = \sum_{u_1,u_2\in\mathbb{F}_2^n; v_1,v_2\in\mathbb{F}_2^m} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$$

and

$$(W_F^2)^{\otimes 2}(0,0) = \sum_{u\in\mathbb{F}_2^n; v\in\mathbb{F}_2^m} W_F^4(u,v).$$

Moreover, F is APN if and only if this inequality is an equality.

Corollary 4.3 is particularly interesting for $\alpha = 6$: taking $m = n$ (since APN functions exist for $m = n$), Relation (6) becomes:

$$(W_F^2)^{\otimes 3}(0,0) \geq 2^{7n} + 2^{5n+2}(2^n-1), \tag{7}$$

with equality if and only if F is APN.

We know that $W_F(u,0)$ equals 2^n if $u=0$ and is null otherwise. Let us denote:

$$W_F'^2(u,v) = \begin{cases} W_F^2(u,v) \text{ if } v \neq 0 \\ 0 \text{ otherwise.} \end{cases}$$

We have then:

$$(W_F'^2)^{\otimes 2}(0,0) = \sum_{\substack{u\in\mathbb{F}_2^n; v\in\mathbb{F}_2^m \\ v\neq 0}} W_F^4(u,v)$$

and

$$(W_F'^2)^{\otimes 3}(0,0) = \sum_{\substack{u_1,u_2\in\mathbb{F}_2^n; v_1,v_2\in\mathbb{F}_2^m \\ v_1\neq 0, v_2\neq 0, v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2).$$

Then, (7) is equivalent to:

$$(W_F'^2)^{\otimes 3}(0,0) \geq 2^{7n} + 2^{5n+2}(2^n-1) - 3\cdot 2^{2n}(W_F'^2)^{\otimes 2}(0,0) - 2^{6n}$$

and since we know that for any APN function we have $(W_F'^2)^{\otimes 2}(0,0) = 2^{3n+1}(2^n-1)$, we deduce that for any such function: $(W_F'^2)^{\otimes 3}(0,0) = 2^{7n} - 3\cdot 2^{6n} + 2^{5n+1}$, that is:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n; v_1,v_2\in\mathbb{F}_2^m \\ v_1\neq 0, v_2\neq 0, v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) = 2^{5n}(2^n-1)(2^n-2). \quad (8)$$

Hence, the arithmetic mean of $W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$ when u_1,u_2 range independently over $\mathbb{F}_2^n$ and v_1,v_2 are nonzero and distinct and range independently over $\mathbb{F}_2^n$ equals what we would get with a bent function if such function could exist: 2^{3n}. This is a new information on APN functions, to be compared with the fact already mentioned in Remark 5.3 that the arithmetic mean taken by $W_F^4(u,v)$ when u ranges over $\mathbb{F}_2^n$ and v is nonzero and ranges over $\mathbb{F}_2^n$, equals 2^{2n+1} in the case of an APN function, that is twice what we get with a bent function.

We have here only an equality valid for APN functions, but we do not have an inequality valid for all functions and whose case of equality would be characteristic of APN functions. We shall derive such inequality in Subsection 5.1 (see Theorem 5.2). Note also that we have here $m=n$ and Remark 3.3 does not apply (we can check that replacing $W_F'^2$ by 2^n in (8) indeed does not work).

Remark 4.4 *The case of $\alpha = 6$ in Corollary 4.3 corresponds to $P(X) = X+2$. We can also take more generally $P(X) = X^{k-1} + 2X^{k-2} + \cdots + 2^{k-2}X + 2^{k-1}$ for some $k \geq 2$ which gives $(X-2)P(X) = X^k - 2^k$ and then we have for every function F:*

$$(W_F^2)^{\otimes(k+1)}(0,0) \geq 2^{(3k+1)n} + (2^n-1)2^{(2k+1)n+k},$$

with equality if and only if F is APN.

5 Characterizations in the case of $\delta = 4$ (differentially 4-uniform functions) and more knowledge in the case $\delta = 2$

In the case of $\delta = 4$ in Theorem 3.1, we have $A_0 = 8$, $A_1 = -6$ and $A_2 = 1$, which gives:

Corollary 5.1 *Let F be any (n, m)-function. Then*

$$(W_F^2)^{\otimes 3}(0,0) - 3 \cdot 2^{n+m+1}(W_F^2)^{\otimes 2}(0,0) \geq 2^{5n+2m} - 7 \cdot 2^{4n+2m+1} + 2^{3n+2m+3}, \quad (9)$$

where $(W_F^2)^{\otimes 3}(0,0)$ and $(W_F^2)^{\otimes 2}(0,0)$ are defined in Corollary 4.3. Moreover, F is differentially 4-uniform if and only if this inequality is an equality.

Of course, Inequality (9) is Inequality (6) when $\alpha = 0$, but equality in (6) characterizes APN functions only for $\alpha > 0$.

Using the notation $W_F'^2(u,v) = \begin{cases} W_F^2(u,v) \text{ if } v \neq 0 \\ 0 \text{ otherwise.} \end{cases}$ already introduced in Section 4, Corollary 5.1 writes:

$$(W_F'^2)^{\otimes 3}(0,0) - 3 \cdot (2^{n+m+1} - 2^{2n})(W_F'^2)^{\otimes 2}(0,0) \geq \quad (10)$$
$$2^{5n+2m} + 3 \cdot 2^{5n+m+1} - 7 \cdot 2^{4n+2m+1} + 2^{3n+2m+3} - 2^{6n},$$

with equality if and only if F is differentially 4-uniform.

Note that Remark 3.3 applies for $m \in \{n-1, n-2\}$. By replacing $W_F'^2(u,v)$ by 2^n in the left hand side term of (10) for $v \neq 0$, we obtain in each case an expression equal to the right hand side term.

In Section 6, we investigate a little further the inequalities (9) and (10). This gives more insight, but is also a little more technical.

5.1 The case $m = n$

In that case, Corollary 5.1 gives:

$$(W_F^2)^{\otimes 3}(0,0) - 3 \cdot 2^{2n+1}(W_F^2)^{\otimes 2}(0,0) \geq 2^{7n} - 7 \cdot 2^{6n+1} + 2^{5n+3}, \quad (11)$$

and Relation (10) becomes:

$$(W_F'^2)^{\otimes 3}(0,0) - 3 \cdot 2^{2n}(W_F'^2)^{\otimes 2}(0,0) \geq 2^{7n} - 9 \cdot 2^{6n} + 2^{5n+3}, \quad (12)$$

with in each case equality if and only if f is differentially 4-uniform.

Using Relation (2) and the related relation $(W_F'^2)^{\otimes 2}(0,0) \geq 2^{3n+1}(2^n - 1)$, we deduce from (11) and (12):

Theorem 5.2 *For every (n, n)-function, we have:*

$$(W_F^2)^{\otimes 3}(0,0) \geq 2^{7n} + 2^{6n+2} - 2^{5n+2}$$

Equivalently, we have $(W_F'^2)^{\otimes 3}(0,0) \geq 2^{7n} - 3 \cdot 2^{6n} + 2^{5n+1}$*, that is:*

$$\sum_{\substack{u_1,u_2 \in \mathbb{F}_2^n; v_1,v_2 \in \mathbb{F}_2^m \\ v_1 \neq 0, v_2 \neq 0, v_1 \neq v_2}} W_F^2(u_1,v_1) W_F^2(u_2,v_2) W_F^2(u_1+u_2,v_1+v_2) \geq 2^{5n}(2^n-1)(2^n-2) \quad (13)$$

(whose case of equality is (8)), with, in each case, equality if and only if F *is APN.*

Remark 5.3 *Theorem 5.2 illustrates the observation of Remark 3.3: the arithmetic mean of* $W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$ *when* u_1,u_2 *range independently over* $\mathbb{F}_2^n$ *and* v_1,v_2 *are nonzero and distinct and range independently over* $\mathbb{F}_2^n$ *equals, in the case of an APN function, what we would get with a bent function if such function could exist:* 2^{3n}*.*

Remark 5.4 *Theorem 5.2 says what is the minimal value of* $(W_F'^2)^{\otimes 3}(0,0)$ *but it does not say what is the maximal value.*
Clearly we have that $\sum_{\substack{u_1,u_2 \in \mathbb{F}_2^n; v_1,v_2 \in \mathbb{F}_2^m \\ v_1 \neq 0, v_2 \neq 0, v_1 \neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$ *is lower than or equal to* $2^{2n} \sum_{\substack{u_1,u_2 \in \mathbb{F}_2^n; v_1,v_2 \in \mathbb{F}_2^m \\ v_1 \neq 0, v_2 \neq 0, v_1 \neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2) = 2^{2n}[2^{4n}(2^n - 1)(2^n-2)] = 2^{6n}(2^n-1)(2^n-2)$*, according to the Parseval relation. This maximum is achieved, with affine functions. Indeed, without loss of generality, we can take* F *linear. For each* u,v *we have then* $W_F(u,v) = 2^n$ *if the two linear functions* $v \cdot F(x)$ *and* $u \cdot x$ *are equal and* $W_F(u,v) = 0$ *otherwise. Moreover, if* $W_F(u_1,v_1) = 2^n$ *and* $W_F(u_2,v_2) = 2^n$ *then* $W_F(u_1+u_2,v_1+v_2) = 2^n$*. This implies, using again the Parseval relation, that* $(W_F'^2)^{\otimes 3}(0,0) = 2^{6n}(2^n-1)(2^n-2)$*. It is easily seen that only affine functions achieve such value. This shows that* $(W_F'^2)^{\otimes 3}(0,0)$ *is a numerical parameter also quantifying the "nonlinearity" of* F*, but here also, it is more related to the differential attacks than to the linear attacks.*

Consequence on highly nonlinear (n,n)-functions All known APN functions have a rather good nonlinearity (probably at least $2^{n-1} - 2^{\frac{3n}{5}-1} - 2^{\frac{2n}{5}-1}$, but this has to be confirmed since the nonlinearity of the Dobbertin function is unknown except for small values of n). AB functions have optimal nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ and for n even, many APN functions like Gold and Kasami functions or the inverse function have nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$ (see [6]). Theorem 5.2 gives information on the structure of the support of the Walsh transform of any (n,n)-function whose nonlinearity is high:

Corollary 5.5 *Let* F *be any* (n,n)*-function and let* $\lambda \geq 0$ *be such that* $nl(F) = 2^{n-1} - \frac{1}{2}\sqrt{2^{n+1}+\lambda}$ *(with* $\lambda = 0$ *if and only if* F *is AB, according to the case of equality of the SCV bound). Then we have:*

$$\left| \left\{ (u_1,u_2,v_1,v_2) \in (\mathbb{F}_2^n)^4;\ \begin{cases} v_1 \neq 0, v_2 \neq 0, v_1 \neq v_2, W_F(u_1,v_1) \neq 0, \\ W_F(u_2,v_2) \neq 0, W_F(u_1+u_2,v_1+v_2) \neq 0 \end{cases} \right\} \right| \geq \frac{2^{5n}(2^n-1)(2^n-2)}{(2^{n+1}+\lambda)^3}.$$

Proof. By definition of λ we have $\max_{u,v\in\mathbb{F}_2^n,v\neq 0} W_F^2(u,v) = 2^{n+1}+\lambda$. Theorem 5.2 and the inequality $W_F^2(u,v)\leq 2^{n+1}+\lambda$, $\forall u,v\in\mathbb{F}_2^n, v\neq 0$ prove the result. □

This gives more insight on the structure of the so-called Walsh support $\{(u,v)\in(\mathbb{F}_2^n)^2; W_F(u,v)\neq 0\}$ of highly nonlinear (n,n)-functions.

Generalization of Theorem 5.2 Note that we have:

$$\sum_{u_1,u_2,v_1,v_2\in\mathbb{F}_2^n} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) =$$

$$\sum_{u_1,u_2,v_1,v_2\in\mathbb{F}_2^n}\ \sum_{(x_1,y_1,x_2,y_2,x_3,y_3)\in(\mathbb{F}_2^n)^6} (-1)^{(F(x_1)+F(y_1))\cdot v_1+(x_1+y_1)\cdot u_1+(F(x_2)+F(y_2))\cdot v_2+(x_2+y_2)\cdot u_2}$$

$$(-1)^{(F(x_3)+F(y_3))\cdot(v_1+v_2)+(x_3+y_3)\cdot(u_1+u_2)} =$$

$$\sum_{(x_1,y_1,x_2,y_2,x_3,y_3)\in(\mathbb{F}_2^n)^6}\ \sum_{v_1,v_2\in\mathbb{F}_2^n} (-1)^{(F(x_1)+F(y_1)+F(x_3)+F(y_3))\cdot v_1+(F(x_2)+F(y_2)+F(x_3)+F(y_3))\cdot v_2}$$

$$\sum_{u_1,u_2\in\mathbb{F}_2^n} (-1)^{(x_1+y_1+x_3+y_3)\cdot u_1+(x_2+y_2+x_3+y_3)\cdot u_2} =$$

$$2^{4n}\left|\left\{\begin{array}{l}(x_1,y_1,x_2,\\ y_2,x_3,y_3)\in(\mathbb{F}_2^n)^6\end{array};\begin{array}{l}x_1+y_1=x_2+y_2=x_3+y_3,\\ F(x_1)+F(y_1)=F(x_2)+F(y_2)=F(x_3)+F(y_3)\end{array}\right\}\right| =$$

$$2^{4n}\sum_{a,b\in\mathbb{F}_2^n}|(D_aF)^{-1}(b)|^3,$$

while $\sum_{u,v\in\mathbb{F}_2^n} W_F^4(u,v) = 2^{2n}\sum_{a,b\in\mathbb{F}_2^n}|(D_aF)^{-1}(b)|^2$. This gives a direct proof of Theorem 5.2. It gives also more insight on why it characterizes APN functions: $\sum_{a,b\in\mathbb{F}_2^n}|(D_aF)^{-1}(b)|^3$ is minimized when $|(D_aF)^{-1}(b)|\in\{0,2\}$ for all $a,b\in\mathbb{F}_2^n$ with $a\neq 0$ (since $|(D_aF)^{-1}(b)|$ is always even and is the same for all functions when $a=0$ – it equals 2^n for $a=b=0$ and 0 for $a=0,b\neq 0$).
For the same reason, for every $k\geq 2$, we have $\sum_{a,b\in\mathbb{F}_2^n}|(D_aF)^{-1}(b)|^k\geq 2^{kn}+2^k(2^n-1)2^{n-1}=2^{kn}+2^{2n+k-1}-2^{n+k-1}$ and F is APN if and only if this inequality is an equality. We have:

$$\sum_{a,b\in\mathbb{F}_2^n}|(D_aF)^{-1}(b)|^k =$$

$$2^{-2(k-1)n}\sum_{\substack{u_1,\dots,u_{k-1},\\ v_1,\dots,v_{k-1}\in\mathbb{F}_2^n}}\left(\prod_{i=1}^{k-1}W_F^2(u_i,v_i)\right)W_F^2(u_1+\cdots+u_{k-1},v_1+\cdots+v_{k-1}).$$

Hence, we have:

Proposition 5.6 *Let F be any (n,n)-function and k any integer such that $k\geq 2$. We have:*

$$\sum_{\substack{u_1,\dots,u_{k-1},\\ v_1,\dots,v_{k-1}\in\mathbb{F}_2^n}}\left(\prod_{i=1}^{k-1}W_F^2(u_i,v_i)\right)W_F^2(u_1+\cdots+u_{k-1},v_1+\cdots+v_{k-1})\geq$$

$$2^{2(k-1)n}\left(2^{kn}+2^{2n+k-1}-2^{n+k-1}\right)$$

and F is APN if and only if this inequality is an equality.

In the case of $k=3$, this gives again Theorem 5.2.
We can have another similar but different characterization: for every (a,b) such that $|(D_aF)^{-1}(b)|\neq 0$, we have $|(D_aF)^{-1}(b)|\geq 2$; we deduce then:

$$\sum_{\substack{a,b\in\mathbb{F}_2^n\\ a\neq 0}}|(D_aF)^{-1}(b)|^{k+1}\geq 2\sum_{\substack{a,b\in\mathbb{F}_2^n\\ a\neq 0}}|(D_aF)^{-1}(b)|^{k},$$

with equality if and only if F is APN. Hence, we have also:

Proposition 5.7 *Let F be any (n,n)-function and k any integer such that $k\geq 2$. We have:*

$$\sum_{\substack{u_1,\dots,u_k,\\ v_1,\dots,v_k\in\mathbb{F}_2^n}}\left(\prod_{i=1}^{k}W_F^2(u_i,v_i)\right)W_F^2(u_1+\cdots+u_k,v_1+\cdots+v_k)-2^{(3k+1)n}\geq$$

$$2^{2n+1}\left(\sum_{\substack{u_1,\dots,u_{k-1},\\ v_1,\dots,v_{k-1}\in\mathbb{F}_2^n}}\left(\prod_{i=1}^{k-1}W_F^2(u_i,v_i)\right)W_F^2(u_1+\cdots+u_{k-1},v_1+\cdots+v_{k-1})-2^{(3k-2)n}\right),$$

with equality if and only if F is APN.

In particular, for $k=2$, we have:

$$\sum_{\substack{u_1,u_2,\\ v_1,v_2\in\mathbb{F}_2^n}}W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)-2^{7n}\geq$$

$$2^{2n+1}\left(\sum_{u,v\in\mathbb{F}_2^n}W_F^4(u,v)-2^{4n}\right),$$

with equality if and only if F is APN. Hence, Proposition 5.7, which for $k=2$ does not give exactly Theorem 5.2, is slightly different from Proposition 5.6.

5.2 On the nonlinearity of APN functions

As recalled above, all known APN functions have a rather good nonlinearity. But no proof exists that the nonlinearity of APN functions cannot be weak. The only result, proved in [6], is that, for $n>2$, any APN function has nonzero nonlinearity. The proof of this result uses APNness in the form of its definition, that is, the fact that each equation $D_aF(x)=z$, $a\neq 0$, has at most 2 solutions. It seems that using, instead, the characterization of APN functions by the fourth moment of the Walsh transform does not allow to derive a better lower bound on the nonlinearity of APN functions. The same seems to happen with the characterization from Theorem 5.2. It is then still a completely open question to know whether APN functions can have low nonlinearity.

It is interesting to investigate reasons why the known APN functions have non-weak nonlinearity. Most known APN functions are either power functions $F(x) = x^d$ over $\mathbb{F}_{2^n}$ (n odd or n even) or quadratic functions. In the former case, as proved by Dobbertin and reported in [6], we have $gcd(d, 2^n - 1) = 1$ if n is odd (and F is then a permutation and all the component functions $tr_1^n(vF)$, $v \neq 0$, are linearly equivalent, since all the elements $v \in \mathbb{F}_{2^n}^*$ are cubes and are then d-th powers) and $gcd(d, 2^n - 1) = 3$ if n is even (and two component functions $tr_1^n(vF)$ and $tr_1^n(v'F)$ are linearly equivalent when v' equals v times a nonzero cube).

Theorem 5.8 *Let F be any APN power function. Then, if n is odd, we have $nl(F) \geq 2^{n-1} - 2^{\frac{3n-3}{4}}$ and if n is even, we have $nl(F) \geq 2^{n-1} - 2^{\frac{3n-2}{4}}$.*

Proof. If n is odd then, for every v, the sum $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, v)$ is independent of the choice of $v \neq 0$ and, according to the characterization of APN functions by the fourth moment of Walsh transform, equals then 2^{3n+1}. Hence, we have $W_F^4(u, v) \leq 2^{3n+1}$ for every u and the result follows from (1). If n is even, then, since $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, v)$ does not change when v is multiplied by a nonzero cube, it takes, when v ranges over $\mathbb{F}_{2^n}^*$, $\frac{2^n-1}{3}$ times the value $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, 1)$, $\frac{2^n-1}{3}$ times the value $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, \alpha)$ and $\frac{2^n-1}{3}$ times the value $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, \alpha^2)$, where α is a primitive element of $\mathbb{F}_{2^n}$. Hence we have $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, 1) + \sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, \alpha) + \sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, \alpha^2) = 3 \cdot 2^{3n+1}$. We have, by the Cauchy-Schwartz inequality, that $\sum_{u \in \mathbb{F}_2^n} W_F^4(u, v) \geq \frac{\left(\sum_{u \in \mathbb{F}_2^n} W_F^2(u,v)\right)^2}{2^n} = 2^{3n}$, for every $v \neq 0$. Hence, we have by complementation that each of the sums $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, 1), \sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, \alpha)$ and $\sum_{u \in \mathbb{F}_{2^n}} W_F^4(u, \alpha^2)$ is bounded above by $3 \cdot 2^{3n+1} - 2 \cdot 2^{3n} = 2^{3n+2}$. We have then $W_F^4(u, v) \leq 2^{3n+2}$ for every u, v such that $v \neq 0$ and Relation (1) completes the proof. □

Remark 5.9 *There are other possible approaches but it seems that they are less efficient. For instance, up to linear equivalence, we can assume that every coordinate function f_i of F has nonlinearity $nl(F)$. This is clearly true if n is odd and if n is even, all component functions $tr_1^n(vx^d)$, $v \neq 0$, of F belonging to the three linear equivalence classes of $tr_1^n(x^d)$, $tr_1^n(\alpha x^d)$ and $tr_1^n(\alpha^2 x^d)$, where α is a primitive element of $\mathbb{F}_{2^n}$, one of these three functions has nonlinearity $nl(F)$; it is then easily seen that, up to a change of basis, it is possible to have all coordinate functions of F in the corresponding equivalence class. Then, adding to F a proper affine function, we may assume that every f_i has Hamming weight $nl(F)$ and $F(\mathbb{F}_{2^n}) \setminus \{0\}$ being included in the union of the supports of the f_i's, its size is then at most $n \cdot nl(F)$. For every $a \neq 0$, the size of $D_aF(\mathbb{F}_{2^n})$ is then at most $(n \cdot nl(F) + 1)^2$, and since F is APN, the size of $D_aF(\mathbb{F}_{2^n})$ equals 2^{n-1}. We have then $nl(F) \geq \frac{2^{\frac{n}{2}} - \sqrt{2}}{n\sqrt{2}}$. But this lower bound is much worse than that of Theorem 5.8 (it is true however for all functions* *such that there exist linearly independent $v_1, \dots, v_n$ such that $nl(v_i \cdot F) = nl(F)$ for every i).*

In the case where F is quadratic, if n is odd and F is APN, then F is AB and its nonlinearity is optimal. For n even, the question is more difficult. Since we know that $nl(F) \neq 0$ and according to the knowledge on quadratic functions (see e.g. [5]), we have $nl(F) \geq 2^{n-1} - 2^{n-3} = 3 \cdot 2^{n-3}$. This bound is not strong.

Remark 5.10 *The next issue is to determine whether quadratic APN (n,n)-functions can have nonlinearity $2^{n-1} - 2^{n-3}$. Suppose that such function F exists. Then one of its component functions is EA-equivalent to $x_{n-1}x_n$ and, without loss of generality, we may assume that the last coordinate function f_n of F equals $x_{n-1}x_n$. We have then $F(x) = (F'(x), x_{n-1}x_n)$ where F' is an $(n, n-1)$-function. The restriction of a differentially 2-uniform function being differentially 2-uniform, the restrictions of F to the hyperplanes of equations $x_n = 0$ and $x_n = 1$ are differentially 2-uniform and have last coordinate function linear. We deduce that the restrictions of F' to these hyperplanes are differentially 2-uniform and since these restrictions are quadratic $(n-1, n-1)$-functions with $n-1$ odd, these restrictions are AB. This means that for every $u \in \mathbb{F}_2^n$, every nonzero $v \in \mathbb{F}_2^{n-1}$ and every $\epsilon \in \mathbb{F}_2$, we have $\sum_{x\in\in\mathbb{F}_2^n; x_n=\epsilon} (-1)^{v\cdot F(x)+u\cdot x} \in \{0, \pm 2^{\frac{n}{2}}\}$, which implies $\sum_{x\in\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)+u\cdot x} \in \{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}\}$. Hence, the matrix of the symplectic form associated to the quadratic Boolean function $v \cdot F$ has rank at least $n-2$ (see e.g. [11]). Since the matrix associated to f_n has rank 2, that of function $v \cdot F + f_n$ has rank at least $n-4$. Hence $\sum_{x\in\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)+f_n(x)+u\cdot x} \in \{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n+2}{2}}, \pm 2^{\frac{n+4}{2}}\}$, while $\sum_{x\in\in\mathbb{F}_2^n} (-1)^{f_n(x)+u\cdot x} \in \{0, \pm 2^{n-1}\}$.*
We deduce $\sum_{u,v\in\in\mathbb{F}_2^n; v\neq 0} W_F^4(u,v) = \lambda_0 2^{3n} + \lambda_1 2^{3n+2} + \lambda_2 2^{3n+4} + 2^{4n-2}$, where λ_i is the number of v's in $\mathbb{F}_2^n$ such that $W_F(u,v) \in \{0, \pm 2^{\frac{n}{2}+i}\}$, since for each such v we have $\sum_{u\in\in\mathbb{F}_2^n} W_F^4(u,v) = 2^{n+2i} \sum_{u\in\in\mathbb{F}_2^n} W_F^2(u,v) = 2^{3n+2i}$. And since $\lambda_0 + \lambda_1 + \lambda_2 = 2^n - 2$, F is APN if and only if $\lambda_1 + 5\lambda_2 = 2^{n-2}$. We do not see a reason why such function F could not exist for n large enough (but we leave the difficult search of such functions for future work). This would mean that APN functions with very low nonlinearity could exist (if such functions were found, they would be of course new up to CCZ-equivalence).

5.3 The case $m = n - 1$

According to Corollary 5.1 and to Relation (10), we have:

Theorem 5.11 *Let F be any $(n, n-1)$-function. Then, we have:*

$$(W_F^2)^{\otimes 3}(0,0) - 3 \cdot 2^{2n} (W_F^2)^{\otimes 2}(0,0) \geq 2^{7n-2} - 7 \cdot 2^{6n-1} + 2^{5n+1},$$

where $(W_F^2)^{\otimes 3}(0,0)$ and $(W_F^2)^{\otimes 2}(0,0)$ are defined in Corollary 4.3, and

$$(W_F'^2)^{\otimes 3}(0,0) \geq 2^{7n-2} - 3 \cdot 2^{6n-1} + 2^{5n+1} = 2^{5n}(2^{n-1} - 1)(2^{n-1} - 2), \qquad (14)$$

where $W'^2_F(u,v)$ and $(W'^2_F)^{\otimes 3}(0,0)$ are defined after Corollary 4.3, that is:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)\geq 2^{5n}(2^{n-1}-1)(2^{n-1}-2),$$

and F is differentially 4-uniform if and only if one of these inequalities is an equality.

The expression on the left hand side is the same in Theorems 5.2 and 5.11. This is particularly interesting to see that the same (or a very similar) characterization is valid for APN (n,n)-functions and differentially 4-uniform $(n,n-1)$-functions.

Remark 5.12 *We have the same observation as at the end of Subsection 5.1 (generalization of Theorem 5.2): we have $\sum_{u_1,u_2,v_1,v_2\in\mathbb{F}_2^n} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) = 2^{4n-2}\sum_{a\in\mathbb{F}_2^n,b\in\mathbb{F}_2^{n-1}}|(D_aF)^{-1}(b)|^3$, and this value can be minimized only when we have $|(D_aF)^{-1}(b)|$ as small as possible, that is when F is differentially 4-uniform (unless F can be bent, that is, when $n=2$). However Theorem 5.11 is more precise than this observation. We could also generalize Theorem 5.11 similarly as in Subsection 5.1.*

6 Further observations on differential uniformity

In this section, we investigate more on the properties viewed in Section 5. Our results give more insight but are also a little more technical.
Inequality (10) is equivalent to:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n)(W_F^2(u_2,v_2)-2^n)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$$

$$-3\cdot(2^{n+m+1}-2^{2n})\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v)\geq$$

$$2^{5n+2m}+3\cdot 2^{5n+m+1}-7\cdot 2^{4n+2m+1}+2^{3n+2m+3}-2^{6n}-$$

$$3\cdot 2^n\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)+3\cdot 2^{3n}(2^m-2)\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^2(u,v)$$

$$-2^{5n}(2^m-1)(2^m-2)=$$

$$2^{5n+2m}+3\cdot 2^{5n+m+1}-7\cdot 2^{4n+2m+1}+2^{3n+2m+3}-2^{6n}+2\cdot 2^{5n}(2^m-1)(2^m-2)$$

$$-3\cdot 2^n\left(\left(\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^2(u,v)\right)^2-\sum_{\substack{v\in\mathbb{F}_2^m\\ v\neq 0}}\left(\sum_{u\in\mathbb{F}_2^n} W_F^2(u,v)\right)^2\right)=$$

$$3\cdot 2^{5n+2m}-7\cdot 2^{4n+2m+1}+2^{3n+2m+3}-2^{6n}+4\cdot 2^{5n}-3\cdot 2^n\left(\left(2^{2n}(2^m-1)\right)^2-2^{4n}(2^m-1)\right)=$$

$$-7\cdot 2^{4n+2m+1}+2^{3n+2m+3}-2^{6n}+9\cdot 2^{5n+m}-2\cdot 2^{5n}.$$

We deduce:

Corollary 6.1 *Let F be any (n,m)-function. Then*

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n)(W_F^2(u_2,v_2)-2^n)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$$

$$-3\cdot(2^{n+m+1}-2^{2n})\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v)\geq$$

$$-7\cdot 2^{4n+2m+1}+2^{3n+2m+3}-2^{6n}+9\cdot 2^{5n+m}-2^{5n+1},$$

and F is differentially 4-uniform if and only if this inequality is an equality.

Then for every λ, we have

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n-\lambda)(W_F^2(u_2,v_2)-2^n+\lambda)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$$

$$-3\cdot(2^{n+m+1}-2^{2n})\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v)\geq$$

$$-7\cdot 2^{4n+2m+1}+2^{3n+2m+3}-2^{6n}+9\cdot 2^{5n+m}-2^{5n+1}.$$

Indeed, $\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}}(W_F^2(u_1,v_1)-2^n)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$ is equal to $\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}}(W_F^2(u_2,v_2)-2^n)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$ and we have $\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^m\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}}(W_F^2(u_1+u_2,v_1+v_2)-2^n)=0$.
F is differentially 4-uniform if and only if this inequality is an equality.

6.1 In the case $m=n$

Corollary 6.1 gives:

$$\sum_{\substack{u_1,u_2,v_1,v_2\in\mathbb{F}_2^n\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n)(W_F^2(u_2,v_2)-2^n)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$$

$$-3\cdot 2^{2n}\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v)\geq -6\cdot 2^{5n}(2^n-1),$$

and the observation which follows it gives, for every λ:

$$\sum_{\substack{u_1,u_2,v_1,v_2\in\mathbb{F}_2^n\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n-\lambda)(W_F^2(u_2,v_2)-2^n+\lambda)(W_F^2(u_1+u_2,v_1+v_2)-2^n)$$

$$-3\cdot 2^{2n}\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^m\\ v\neq 0}} W_F^4(u,v)\geq -6\cdot 2^{5n}(2^n-1),$$

with, in both cases, equality if and only if F is differentially 4-uniform, and using Relation (2):

$$\sum_{\substack{u_1,u_2,v_1,v_2\in\mathbb{F}_2^n\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n-\lambda)(W_F^2(u_2,v_2)-2^n+\lambda)(W_F^2(u_1+u_2,v_1+v_2)-2^n)\geq 0,$$

with equality if and only if F is APN.

6.2 In the case $m=n-1$

Corollary 6.1 gives:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n)(W_F^2(u_2,v_2)-2^n)(W_F^2(u_1+u_2,v_1+v_2)-2^n)\geq 0,$$

and the observation which follows it gives:

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} (W_F^2(u_1,v_1)-2^n-\lambda)(W_F^2(u_2,v_2)-2^n+\lambda)(W_F^2(u_1+u_2,v_1+v_2)-2^n)\geq 0,$$

with, in both cases, equality if and only if F is differentially 4-uniform.

Remark 6.2 *Applying the Cauchy-Schwarz inequality to the case of equality in (14), and denoting by E_F the set:*

$\{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}\backslash\{0\};v_1\neq v_2;\ W_F(u_1,v_1)W_F(u_2,v_2)W_F(u_1+u_2,v_1+v_2)\neq 0\}$,

we have:

$$\left(\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F(u_1,v_1)W_F(u_2,v_2)W_F(u_1+u_2,v_1+v_2)\right)^2\leq$$

$$2^{5n}(2^{n-1}-1)(2^{n-1}-2)|E_F|.$$

And since:

$$\sum_{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}} W_F(u_1,v_1)W_F(u_2,v_2)W_F(u_1+u_2,v_1+v_2)=$$

$$\sum_{u_1,u_2,x,y,z\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}} (-1)^{v_1\cdot(F(x)+F(z))+v_2\cdot(F(y)+F(z))+u_1\cdot(x+z)+u_2\cdot(y+z)}=2^{5n-2},$$

and

$$\sum_{u_1,u_2\in\mathbb{F}_2^n;v_1\in\mathbb{F}_2^{n-1}} W_F(u_1,v_1)W_F(u_2,v_1)W_F(u_1+u_2,0) =$$

$$2^n \sum_{u_1\in\mathbb{F}_2^n;v_1\in\mathbb{F}_2^{n-1}} W_F^2(u_1,v_1) = 2^{4n-1},$$

and

$$\sum_{u_1,u_2\in\mathbb{F}_2^n} W_F(u_1,0)W_F(u_2,0)W_F(u_1+u_2,0) = 2^{3n},$$

we deduce:

$$|E_F| \geq \frac{(2^{5n-2} - 3\cdot 2^{4n-1} + 2\cdot 2^{3n})^2}{2^{5n}(2^{n-1}-1)(2^{n-1}-2))} = 2^n(2^{n-1}-1)(2^{n-1}-2).$$

Remark 6.3 *Schur's inequality (see e.g. [15, page 15]) for positive numbers:*

$$\sum_{j=1}^{M}\sum_{k=1}^{N} c_{j,k}x_jy_k \leq \sqrt{RC}\left(\sum_{j=1}^{M} x_j^2\right)^{1/2}\left(\sum_{k=1}^{N} y_k^2\right)^{1/2},$$

where $R = \max_j \sum_{k=1}^{N} c_{j,k}$ and $C = \max_k \sum_{j=1}^{M} c_{j,k}$, gives, with $N = M = 2^{2n-1}$, with the two sequences x_j and y_k both equal to $W_F^2(u,v)$ if $v \neq 0$ and to 0 if $v = 0$ and with the coefficient $c_{j,k}$ equal to $W_F^2(u_1+u_2,v_1+v_2)$ if $v_1 \neq 0, v_2 \neq 0, v_1+v_2 \neq 0$ and to 0 otherwise, that

$$\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) \leq$$

$$(2^{n-1}-2)2^{2n} \sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^{n-1}\\ v\neq 0}} W_F^4(u,v).$$

Rel. (14) gives then $\displaystyle\sum_{\substack{u\in\mathbb{F}_2^n;v\in\mathbb{F}_2^{n-1}\\ v\neq 0}} W_F^4(u,v) \geq \frac{2^{5n}(2^{n-1}-1)(2^{n-1}-2)}{(2^{n-1}-2)2^{2n}} = 2^{3n}(2^{n-1}-1),$ *for every $(n,n-1)$-function. This is Inequality (5) with $m = n-1$. In a way, Inequality (5) can then be viewed as weaker than Inequality (14) in the case $m = n-1$. The difference between the left hand side and the right hand side of (14) may give more precise information on F with (14) than with (5).*

Note that Loomis-Whitney's inequality (see [15, page 17]): $\sum_{i,j,k=1}^{N} a_{i,j}^{1/2}b_{j,k}^{1/2}c_{k,i}^{1/2} \leq \left(\sum_{i,j=1}^{N} a_{i,j}\right)^{1/2}\left(\sum_{j,k=1}^{N} b_{j,k}\right)^{1/2}\left(\sum_{k,i=1}^{N} c_{k,i}\right)^{1/2}$, valid for every non-negative numbers, gives the same information. The Arithmetic-Mean-Geometric-Mean (AMGM) inequality [15] gives little information.

Note that, in the case $m = n$, the same claculations can be made but they give weaker results than Relation (2).

Remark 6.4 *A case of differentially 4-uniform $(n, n-1)$-function is $F = L \circ G$, where G is any APN (n, n)-function and L any affine surjective $(n, n-1)$- function*[1]*; without loss of generality, we can assume that L is linear. The kernel of L has dimension 1; it equals then $\{0, e\}$ for some $e \neq 0$. Function L being surjective, its adjoint operator $L^* : \mathbb{F}_2^{n-1} \mapsto \mathbb{F}_2^n$ (defined by $x \cdot L(y) = L^*(x) \cdot y$) is injective and is then a bijection from $\mathbb{F}_2^{n-1}$ to $Im(L^*) = \{0, e\}^\perp$, and for every $b = L^*(v) \in Im(L^*)$, we have $W_F(a, v) = \sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot L(G(x))+a\cdot x} = \sum_{x\in\mathbb{F}_2^n}(-1)^{L^*(v)\cdot G(x)+a\cdot x} = W_G(a, b)$. We have then:*

$$\begin{aligned}&\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;v_1,v_2\in\mathbb{F}_2^{n-1}\\ v_1\neq 0,v_2\neq 0,v_1\neq v_2}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2) =\\ &\sum_{\substack{u_1,u_2\in\mathbb{F}_2^n;b_1,b_2\in\{0,e\}^\perp\\ b_1\neq 0,b_2\neq 0,b_1\neq b_2}} W_G^2(u_1,b_1)W_G^2(u_2,b_2)W_G^2(u_1+u_2,b_1+b_2) =\\ &2^{5n}(2^{n-1}-1)(2^{n-1}-2).\end{aligned} \tag{15}$$

Hence, for every APN (n, n)-function G and every linear hyperplane of $\mathbb{F}_2^n$, the arithmetic mean of $W_G^2(u_1, v_1)W_G^2(u_2, v_2)W_G^2(u_1 + u_2, v_1 + v_2)$ when u_1, u_2 range independently over $\mathbb{F}_2^n$ and v_1, v_2 are nonzero and distinct and range independently over this hyperplane equals 2^{3n} (i.e. what we would get with a bent function if such function could exist).
Equivalently to (15), we have:

$$\sum_{u_1,u_2\in\mathbb{F}_2^n;b_1,b_2\in\{0,e\}^\perp} W_G^2(u_1,b_1)W_G^2(u_2,b_2)W_G^2(u_1+u_2,b_1+b_2) =$$

$$-3\cdot 2^{2n}\sum_{u\in\mathbb{F}_2^n;b\in\{0,e\}^\perp} W_G^4(u,v) = 2^{7n-2} - 7\cdot 2^{6n-1} + 2^{5n+1}.$$

Note that

$$\sum_{u_1,u_2\in\mathbb{F}_2^n;b_1,b_2\in\{0,e\}^\perp} W_G^2(u_1,b_1)W_G^2(u_2,b_2)W_G^2(u_1+u_2,b_1+b_2)$$

equals 2^{4n-2} times:

$$\left|\left\{\begin{array}{l}(x_1,y_1,x_2,y_2,\\ \quad x_3,y_3)\in(\mathbb{F}_2^n)^6\end{array};\ \begin{array}{l}x_1+y_1=x_2+y_2=x_3+y_3,\\ G(x_1)+G(y_1)\equiv G(x_2)+G(y_2)\equiv G(x_3)+G(y_3)\,[\mathrm{mod}\ e]\end{array}\right\}\right|$$

and

$$\sum_{u\in\mathbb{F}_2^n;b\in\{0,e\}^\perp} W_G^4(u,v)$$

equals

$$2^{2n-1}\left|\left\{x_1,y_1,x_2,y_2\in\mathbb{F}_2^n;\ \begin{array}{l}x_1+y_1=x_2+y_2,\\ G(x_1)+G(y_1)\equiv G(x_2)+G(y_2)\,[\mathrm{mod}\ e]\end{array}\right\}\right|.$$

[1] There exist other examples of differentially 4-uniform $(n, n-1)$-functions; see [8].

7 Characterizations in the case of $\delta = 6$

For $\delta = 6$, we have in Theorem 3.1: $A_0 = -48$, $A_1 = 44$, $A_2 = -12$ and $A_3 = 1$. We deduce:

Corollary 7.1 *Let F be any (n, m)-function. Then*

$$(W_F^2)^{\otimes 4}(0,0) - 12 \cdot 2^{n+m}(W_F^2)^{\otimes 3}(0,0) + 44 \cdot 2^{2(n+m)}(W_F^2)^{\otimes 2}(0,0) \geq \\ 2^{7n+3m} - 12 \cdot 2^{6n+3m} + 92 \cdot 2^{5n+3m} - 48 \cdot 2^{4n+3m},$$

where

$$(W_F^2)^{\otimes 4}(0,0) = \sum_{\substack{u_1,u_2,u_3 \in \mathbb{F}_2^n \\ v_1,v_2,v_3 \in \mathbb{F}_2^m}} W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_3,v_3)W_F^2\left(u_1+u_2+u_3, v_1+v_2+v_3\right)$$

and $(W_F^2)^{\otimes 3}(0,0)$ and $(W_F^2)^{\otimes 2}(0,0)$ are defined in Corollary 4.3. Moreover, F is differentially 6-uniform if and only if this inequality is an equality.

Case $m = n - 2$ Note that Remark 3.3 applies. Corollary 7.1 gives:

$$\sum_{\substack{u_1,u_2,u_3 \in \mathbb{F}_2^n \\ v_1,v_2,v_3 \in \mathbb{F}_2^{n-2}}} W_F^2\left(u_1+u_2+u_3, v_1+v_2+v_3\right) W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_3,v_3) \\ -12 \cdot 2^{2n-2} \sum_{\substack{u_1,u_2 \in \mathbb{F}_2^n \\ v_1,v_2 \in \mathbb{F}_2^{n-2}}} W_F^2\left(u_1+u_2, v_1+v_2\right) W_F^2(u_1,v_1)W_F^2(u_2,v_2) + \\ 44 \cdot 2^{4n-4} \sum_{\substack{u \in \mathbb{F}_2^n \\ v \in \mathbb{F}_2^{n-2}}} W_F^4\left(u,v\right) \geq 2^{10n-6} - 12 \cdot 2^{9n-6} + 92 \cdot 2^{8n-6} - 48 \cdot 2^{7n-6},$$

with equality if and only if F is differentially 6-uniform.

Note that the existence of differentially 6-uniform $(n, n-2)$-functions for $n \geq 6$ is an open question (a few differentially 6-uniform $(5, 3)$-functions are known, as mentioned in [8]).

Acknowledgements. We thank Sihem Mesnager, for her useful observations and her careful reading, and Lilya Budaghyan for her kind informations.

References

1. L. Budaghyan, "Construction and Analysis of Cryptographic Functions", Springer Verlag, 2015.
2. L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

3. A. Canteaut, P. Charpin, and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, vol. 46, no. 1, pp. 4-8, 2000.
4. C. Carlet. *Codes de Reed-Muller, codes de Kerdock et de Preparata.* PhD thesis. Publication of LITP, Institut Blaise Pascal, Université Paris 6, 90.59, 1990.
5. C. Carlet. Boolean Functions for Cryptography and Error Correcting Codes. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257-397 (2010). Preliminary version available at www.math.univ-paris13.fr/~carlet/english.html
6. C. Carlet. Vectorial Boolean Functions for Cryptography. Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398-469 (2010). Preliminary version available at www.math.univ-paris13.fr/~carlet/english.html
7. C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* Vol. 61 no. 11, pp. 6272-6289, 2015.
8. C. Carlet and Y. Al Salami. A New Construction of Differentially 4-uniform $(n, n-1)$-Functions. *Advances in Mathematics of Communications*, Vol. 9, no. 4, pp. 541 - 565, 2015.
9. C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156 (1998).
10. F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.
11. F. J. MacWilliams and N. J. Sloane. *The theory of error-correcting codes*, Amsterdam, North Holland. 1977.
12. S. Mesnager: Characterizations of Plateaued and Bent Functions in Characteristic p. Proceedings of SETA 2014, pp. 72-82, 2014.
13. K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT' 91, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.
14. K. Nyberg. Differentially uniform mappings for cryptography. *Proceedings of EUROCRYPT' 93, Lecture Notes in Computer Science* 765, pp. 55-64, 1994.
15. JM Steele. The Cauchy-Schwarz master class: an introduction to the art of mathematical inequalities. Cambridge University Press, 2004.