On the properties of the Boolean functions associated to the differential spectrum of general APN functions and their consequences

Claude Carlet,

Universities of Bergen, Norway, and Paris 8, France.

E-mail: `claude.carlet@gmail.com`

Abstract

We initiate a study, when F is a general APN function, of the Boolean function γ_F related to the differential spectrum of F (which is known to be bent if and only if F is almost bent). We first list many open questions about it. We study its algebraic normal form and its bivariate representation. We characterize its linear structures and specify nonexistence cases; we show, for n even, their relation with bent components $v \cdot F$, $v \neq 0_n$, of F. We pose three related open problems. We characterize further in terms of γ_F the fact that a component function of F is bent and study if the number of bent components can be optimal. We consider in particular two classes, one of which is that of APN power functions. We study more deeply the relation between the Walsh transform of γ_F and the Walsh transform of F. By applying the Titsworth relation to the Walsh transform W_{γ_F}, we deduce a very simple new relation satisfied by W_F^2. From this latter relation, we deduce, for a sub-class of APN functions, a lower bound on the nonlinearity, that is significantly stronger than $nl(F) > 0$ (the only general known bound). This sub-class of APN functions includes all known APN functions. The question (which is another open problem that we state) arises whether this sub-class equals that of all APN functions, but our bound provides at least a beginning of explanation why all known APN functions have non-weak nonlinearity. We finally show how the nonlinearities of γ_F and F are related by a simple formula; this leads to a last open problem.

1 Introduction

Almost perfect nonlinear functions [21] are those functions $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$ (called (n, n)-functions) such that

$$\delta_F := \max\left(|\{x \in \mathbb{F}_2^n; F(x) + F(x+a) = b\}|; a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^n, a \neq 0_n\right)$$

is equal to 2. They have been much studied since the 1990's.
Characterizations of APN functions (and of more general differentially δ-uniform functions) are known by the Walsh transform (see [15, 9]) and by other means as well (see the surveys [3] and [11, Chapter 11]), but after thirty years, we must admit that little is known on general APN functions.
It has been proved in [13] that, given $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^n$, the Boolean function $\gamma_F(a, b)$ over $\mathbb{F}_2^n \times \mathbb{F}_2^n$ taking value 1 if and only if $a \neq 0$ and the set $\{x \in \mathbb{F}_2^n; F(x) + F(x + a) = b\}$ is non-empty, is bent (i.e. lies at the optimal Hamming distance $2^{2n-1} - 2^{n-1}$ from the vector space $\mathcal{A}$ of affine Boolean functions) if and only if F is almost bent (that is, for every nonzero $v \in \mathbb{F}_2^n$, the so-called component function $v \cdot F$, where "$\cdot$" is an inner product in $\mathbb{F}_2^n$, lies at the Hamming distance $2^{n-1} - 2^{\frac{n-1}{2}}$ from $\mathcal{A}$, n must then be odd). Recall that almost bent functions are APN and that the converse is not true in general. Very little is known on γ_F when F is APN without being almost bent. Since almost bent functions are very peculiar functions in odd dimension n (and are shown in [7] not to be good choices as substitution boxes in block ciphers - see also [10] - even if they are bijective, while APN permutations would be very good choices if some could be found for $n = 8$), it seems useful to determine more precisely the characteristics of the γ_F functions associated to general APN functions.
Function γ_F has some known properties that we shall recall below, but it is clearly not a general $2n$-variable Boolean function having such properties, and it seems then necessary to learn more about it, thanks to a systematic search for new properties and a study of the consequences of the known relation between the Walsh transforms of F and γ_F. We shall deduce a new relation on the Walsh transform of APN functions, which seems similar to the characterizations obtained in [9], but is in fact quite different and will have an interesting consequence.
A puzzling observation on APN functions is that no one is known with a bad nonlinearity (that is, with a component function lying close to affine functions), which leads to asking whether APN functions with low nonlinearity can exist. The only known lower bound on the nonlinearity of APN functions is that it is strictly positive [11]. Using the new relation found on the Walsh transform of general APN functions, we derive a lower bound on the nonlinearity of a large class of APN functions that includes all known APN functions. This does not answer the question on the nonlinearity of general APN functions mentioned above, but it gives at least an explanation why all known APN functions have a not so bad nonlinearity (such explanation has been missing since the early nineties for non-power functions; a lower bound is known from [9] for power functions: $nl(F) \geq 2^{n-1} - 2^{\frac{3n-3}{4}}$ for n odd and $nl(F) \geq 2^{n-1} - 2^{\frac{3n-2}{4}}$ for n even). The new lower bound tells us what kind of APN functions need to be avoided when searching for APN functions with bad nonlinearity (whose discovery would probably have little practical interest but would be quite illuminating, theoretically).

The paper is organized as follows. After preliminaries in Section 2, we make in Section 3 some observations, some of which are new, about the Boolean function $\gamma_F(a,b)$, for general APN functions, and we mention many open questions. We briefly study in Section 4 the ANF and the bivariate representation of γ_F, and in Section 5, we tackle the question of the (non)existence of its linear structures. We solve (negatively) the problem when n is odd and, for n even, when the linear structure is 1-valued or of the form (α,β) with $\alpha \neq 0_n$. We characterize in terms of bent components $v \cdot F$ of F the 0-valued linear structures of the form $(0_n,\beta)$, for n even, and we leave open the problem of their existence; we address negatively some particular cases. We observe that a component function of an APN function is bent if and only if, for every $a \in \mathbb{F}_2^n$, the Boolean function $b \mapsto \gamma_F(a,b) + v \cdot b$ is balanced, we deduce that APN power functions cannot have an optimal number of bent components. In Section 6, we recall the relation between the Walsh transforms of γ_F and F and we study the relations on each, which can be deduced from the classical relations on the other. By applying the Titsworth relation to the Walsh transform of γ_F, we derive a new relation satisfied by the Walsh transform of F, which is astonishingly simple. We deduce a lower bound on the nonlinearity of the subclass of those APN functions F such that the minimum Hamming distance between the component functions $v \cdot F$, v nonzero, and affine Boolean functions is achieved more than once. We show that all known APN functions belong to this subclass and leave open the questions of determining whether all APN functions do too and of finding a better bound which would completely explain why all known APN functions have rather good nonlinearity. We eventually show a relation expressing the nonlinearity of γ_F as a degree 2 strictly increasing function of the nonlinearity of F. This relation shows again the equivalence between "F is almost bent" and "γ_F is bent", but it also extends the relation to APN functions that are not necessarily almost bent. We state a last open problem which includes as a sub-problem an open question posed in [5].

2 Preliminaries

For a given positive integer n, we shall denote by 0_n (resp. 1_n) the zero vector (resp. the all-1 vector) of length n and by e_i the i-th vector of Hamming weight 1, that is, of the canonical basis of the vector space $\mathbb{F}_2^n$. We denote by $w_H(x)$ the Hamming weight of an element x of $\mathbb{F}_2^n$, that is, the size of its support $\{i \in \{1,\ldots,n\};\, x_i = 1\}$.

The vector space $\mathbb{F}_2^n$ will sometimes be endowed with the structure of the field $\mathbb{F}_{2^n}$ (this field being an n-dimensional vector space over $\mathbb{F}_2$, each of its elements can be identified with the binary vector of length n of its coordinates relative to a fixed basis). We shall simply denote by 0 the null element in this field (whose vector of coordinates is 0_n).

We shall denote by $\mathcal{B}_n$ the 2^n-dimensional $\mathbb{F}_2$-vector space of n-variable Boolean functions (from $\mathbb{F}_2^n$ to $\mathbb{F}_2$). For a given n-variable pseudo-Boolean function φ, that is, a function from $\mathbb{F}_2^n$ to $\mathbb{R}$, the *Fourier-Hadamard transform* of φ is the $\mathbb{R}$-linear bijective mapping (see e.g. [11, Section 2.3]) which maps φ

to the function $\widehat{\varphi}$ defined on $\mathbb{F}_2^n$ by:

$$\widehat{\varphi}(u) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)\,(-1)^{u\cdot x};\ u \in \mathbb{F}_2^n, \tag{1}$$

where "$\cdot$" is some chosen inner product in $\mathbb{F}_2^n$ (for instance, the usual inner product $u \cdot x = \sum_{i=1}^n u_i x_i$, or, if $\mathbb{F}_2^n$ is endowed with the structure of $\mathbb{F}_{2^n}$, the inner product $u\cdot x = tr_n(ux)$, where $tr_n(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the so-called absolute trace function). The pseudo-Boolean function is identically null if and only if its Fourier-Hadamard transform is identically null (see e.g. [11, Subsection 2.3.3]).

Given an n-variable Boolean function f, we can apply the Fourier-Hadamard transform to f itself viewed as a pseudo-Boolean function, which gives $\widehat{f}(u) = \sum_{x\in supp(f)}(-1)^{u\cdot x}$, where $supp(f) = \{x \in \mathbb{F}_2^n; f(x) = 1\}$, or to the so-called sign function $\varphi = (-1)^f$, which gives the *Walsh transform* of f: $W_f(u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+u\cdot x}$. The two transforms are closely related by the formula:

$$W_f(u) = 2^n\delta_0(u) - 2\widehat{f}(u), \tag{2}$$

where δ_0 is the Dirac (or Kronecker) symbol. Note that f is then *balanced* (that is, has Hamming weight 2^{n-1}) if and only if $W_f(0_n) = 0$. The Walsh transform satisfies the so-called *inverse Walsh transform relation*:

$$\sum_{u\in\mathbb{F}_2^n} W_f(u)(-1)^{u\cdot v} = 2^n(-1)^{f(v)}, \forall v \in \mathbb{F}_2^n, \tag{3}$$

the *Parseval relation*:

$$\sum_{u\in\mathbb{F}_2^n} W_f^2(u) = 2^{2n}, \tag{4}$$

the *Titsworth relation*:

$$\sum_{u\in\mathbb{F}_2^n} W_f(u)W_f(u+v) = 0, \forall v \neq 0_n, \tag{5}$$

and the *Wiener-Khintchine formula* which expresses that the Fourier-Hadamard transform of W_f^2 equals 2^n times the autocorrelation function of f:

$$\sum_{u\in\mathbb{F}_2^n} W_f^2(u)(-1)^{u\cdot a} = 2^n \sum_{x\in\mathbb{F}_2^n}(-1)^{D_a f(x)}, \tag{6}$$

where $D_a f(x) = f(x) + f(x+a)$ is called a derivative of f.

In this paper, we shall be interested in the $2n$-variable Boolean functions γ_F related to (n,n)-functions F. Let us then specify what are the Fourier-Hadamard and Walsh transforms for such a $2n$-variable Boolean function, say γ: the input can be viewed as a pair (a,b) of elements of $\mathbb{F}_2^n$ or of $\mathbb{F}_{2^n}$, and we have $\widehat{\gamma}(u,v) = \sum_{(a,b)\in supp(\gamma)}(-1)^{u\cdot a+v\cdot b}$, and $W_\gamma(u,v) = \sum_{a,b\in\mathbb{F}_2^n}(-1)^{\gamma(a,b)+u\cdot a+v\cdot b}$.

For a given (n,m)-function F, that is, a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, the value $W_F(u,v)$ of the Walsh transform of F at $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^m$ equals by definition that of the Walsh transform of the Boolean function $v\cdot F$ at u.

The *nonlinearity* of a Boolean function f equals its minimum Hamming distance to affine Boolean functions $u\cdot x+\epsilon$, $u\in\mathbb{F}_2^n$, $\epsilon\in\mathbb{F}_2$. It equals then:

$$nl(f)=2^{n-1}-\frac{1}{2}\max_{u\in\mathbb{F}_2^n}|W_f(u)|. \tag{7}$$

It is bounded above by $2^{n-1}-2^{\frac{n}{2}-1}$, according to the covering radius bound which is a direct consequence of the Parseval relation (see e.g. [11, Section 2.3]) and f is called *bent* if it achieves this value with equality. Bent functions exist for n even only, and they are characterized by the fact that $W_f(u)\in\{\pm 2^{\frac{n}{2}}\}$ for every u. The nonlinearity of an (n,m)-function F equals the minimum nonlinearity of its component functions $v\cdot F$, $v\in\mathbb{F}_2^m\setminus\{0_m\}$. It equals then

$$nl(F)=2^{n-1}-\frac{1}{2}\max_{\substack{u\in\mathbb{F}_2^n\\ v\in\mathbb{F}_2^m,v\neq 0_m}}|W_F(u,v)|. \tag{8}$$

It is of course bounded above by $2^{n-1}-2^{\frac{n}{2}-1}$ as well and F is called *bent* if it achieves this value with equality. As shown in [20], bent functions exist if and only if $m\leq\frac{n}{2}$ and n is even. For $m=n$, $nl(F)$ is bounded above by $2^{n-1}-2^{\frac{n-1}{2}}$, according to the Sidelnikov-Chabaud-Vaudenay (SCV) bound (see [15], or see [11, Theorem 6]) and F is called *almost bent* (AB) if it achieves this value with equality (n must be then odd). Equivalently, F is AB if $W_F(u,v)\in\{0,\pm 2^{\frac{n+1}{2}}\}$, for every $u\in\mathbb{F}_2^n$ and every nonzero $v\in\mathbb{F}_2^n$.

Any (n,m)-function can be uniquely represented by its algebraic normal form (ANF):

$$F(x)=\sum_{I\subseteq\{1,\ldots,n\}}a_I\left(\prod_{i\in I}x_i\right)=\sum_{I\subseteq\{1,\ldots,n\}}a_I\,x^I, \tag{9}$$

where a_I belongs to $\mathbb{F}_2^m$. The global degree of the ANF is called the algebraic degree of F and denoted by $d_{alg}(F)$. It equals the maximum algebraic degree of the component functions of F. Affine functions are those functions of algebraic degree at most 1. We call *quadratic* those functions of algebraic degree at most 2. A quadratic n-variable Boolean function is bent if and only if it has Hamming weight $2^{n-1}\pm 2^{\frac{n}{2}-1}$. The algebraic degree of an n-variable Boolean function f equals n if and only if its Hamming weight is odd and, in the case the weight is smaller than n, it equals $n-1$ if and only if $\sum_{x\in\mathbb{F}_2^n}xf(x)\neq 0$. The algebraic degree of an (n,m)-function F equals n if and only if $\sum_{x\in\mathbb{F}_2^n}F(x)\neq 0_m$. For all these results, we refer to the survey [11]. If $\mathbb{F}_2^n$ is endowed with the structure of $\mathbb{F}_{2^n}$, then any (n,n)-function (and then, every (n,m)-functions where m divides n, in particular, any Boolean functions) can be uniquely represented by its univariate representation:

$$F(x)=\sum_{i=0}^{2^n-1}u_i\,x^i\in\mathbb{F}_{2^n}[x]/(x^{2^n}+x). \tag{10}$$

The algebraic degree of F equals then the largest Hamming weight of the binary expansion of those exponents i whose coefficients u_i are nonzero. The functions whose univariate expression is a monomial are called *power functions*.

An (n,m)-function F is called differentially δ-uniform, for a given positive integer δ, if for every $a \in \mathbb{F}_2^n \setminus \{0_n\}$ and every $b \in \mathbb{F}_2^m$, the equation $F(x) + F(x+a) = b$ has at most δ solutions. We denote the minimum of these integers δ by δ_F and call it the differential uniformity of F. For every (n,m)-function F, we have $\delta_F \geq \max(2, 2^{n-m})$. It is shown in [20] that for $m < n$, equality can happen for bent functions only, and then if and only if n is even and $m \leq \frac{n}{2}$.

Note that we can have $\delta_F = 2$ only when $n \geq m$. An (n,n)-function F is called *almost perfect nonlinear* (APN) if it is differentially 2-uniform, that is, if for every $a \in \mathbb{F}_2^n \setminus \{0_n\}$ and every $b \in \mathbb{F}_2^n$, the equation $F(x) + F(x+a) = b$ has 0 or 2 solutions (i.e. the derivative $D_aF(x) = F(x) + F(x+a)$ is 2-to-1). Equivalently, $|\{D_aF(x), x \in \mathbb{F}_2^n\}| = 2^{n-1}$. Still equivalently, for distinct elements x, y, z, t of $\mathbb{F}_2^n$, the equality $x + y + z + t = 0_n$ implies $F(x) + F(y) + F(z) + F(t) \neq 0_n$, that is, the restriction of F to any 2-dimensional flat (*i.e.* affine plane) of $\mathbb{F}_2^n$ is non-affine. There are several characterizations of APN functions (see [11, Chapter 11]): by the numbers of solutions of systems of equations, by the function γ_F defined above, and as proved in [15] by the fourth moment of the Walsh transform: $\sum_{\substack{u,v \in \mathbb{F}_2^n \\ v \neq 0_n}} W_F^4(u,v) = 2^{4n+1} - 2^{3n+1}$ and other relations involving the Walsh transform [9].

A subclass of APN functions is that of AB functions, that we defined already (they are the (n,n)-functions, n odd, whose nonlinearity equals $2^{n-1} - 2^{\frac{n-1}{2}}$, and this is equivalent to saying that their Walsh transform takes values $\{0, \pm 2^{\frac{n+1}{2}}\}$).

3 Generalities on γ_F

Recall from [13] the definition of the Boolean function γ_F associated to any (n,n)-function F:

$$\forall a, b \in \mathbb{F}_2^n, \gamma_F(a,b) = \left\{ \begin{array}{l} 1 \text{ if } a \neq 0_n \text{ and } \exists x \in \mathbb{F}_2^n; F(x) + F(x+a) = b, \\ 0 \text{ otherwise.} \end{array} \right. .$$

In other words, the support of the function $b \in \mathbb{F}_2^n \mapsto \gamma_F(a,b)$ equals the empty set for $a = 0_n$ and the image set of D_aF for $a \neq 0_n$ (we shall denote it by $Im(D_aF)$). Still equivalently, denoting by $\mathcal{G}_F$ the graph $\{(x, F(x)), x \in \mathbb{F}_2^n\}$ of F, the support of γ_F equals $(\mathcal{G}_F + \mathcal{G}_F) \setminus \{(0_n, 0_n)\}$. Function F is APN if and only if γ_F has Hamming weight $2^{2n-1} - 2^{n-1}$, and we have more precisely for F APN that the Boolean function $b \mapsto \gamma_F(a,b)$ is balanced if $a \neq 0_n$ and is null if $a = 0_n$. The definition of γ_F from F makes it rather difficult to study.

A property of γ_F is that, for every nonzero $a \in \mathbb{F}_2^n$, $\sum_{b \in \mathbb{F}_2^n} b\, \gamma_F(a,b)$ equals the same value in $\mathbb{F}_2^n$, equal to $\sum_{x \in \mathbb{F}_2^n} F(x)$, for every $a \neq 0_n$. Indeed, let E_a be any linear hyperplane not containing a, we have $\sum_{b \in \mathbb{F}_2^n} b\, \gamma_F(a,b) = \sum_{x \in E_a} D_aF(x) = \sum_{x \in E_a} F(x) + \sum_{x \in E_a} F(x+a) = \sum_{x \in \mathbb{F}_2^n} F(x)$.
If F is a permutation then, since F^{-1} is also APN and $\gamma_{F^{-1}}(a,b) = \gamma_F(b,a)$,

because $F^{-1}(x)+F^{-1}(x+a)=b$ is equivalent to $F(F^{-1}(x))+F(F^{-1}(x)+b)=a$, we deduce that the sum $\sum_{a\in\mathbb{F}_2^n}\gamma_F(a,b)$ calculated in $\mathbb{Z}$ (i.e. the Hamming weight of the restriction of γ_F obtained by fixing b) equals 2^{n-1} and $\sum_{a\in\mathbb{F}_2^n} a\,\gamma_F(a,b)$ equals the same value in $\mathbb{F}_2^n$ for every $b\neq 0_n$, this value being equal to $\sum_{x\in\mathbb{F}_2^n} F^{-1}(x)$. But if F is not a permutation, then it is difficult to see the specificities of $\sum_{a\in\mathbb{F}_2^n} a\,\gamma_F(a,b)$, and even those of the Hamming weight $\sum_{a\in\mathbb{F}_2^n}\gamma_F(a,b)$ of the restriction of γ_F obtained by fixing b, as can already be seen for n even with the simplest APN functions over $\mathbb{F}_{2^n}$, that are the Gold APN functions $F(x)=x^{2^j+1}$, where $\gcd(j,n)=1$: for $b\neq 0_n$, we have $\{a\in\mathbb{F}_{2^n};\gamma_F(a,b)=1\}=\{a\in\mathbb{F}_{2^n}\setminus\{0_n\};\exists x\in\mathbb{F}_{2^n};\, a^{2^j+1}(x^{2^j}+x+1)=b\}=\{a\in\mathbb{F}_{2^n};\exists x\in\mathbb{F}_{2^n}\setminus(\mathbb{F}_4\setminus\mathbb{F}_2);\, a^{2^j+1}=\frac{b}{x^{2^j}+x+1}\}=\{a\in\mathbb{F}_{2^n};\exists y\in\mathbb{F}_{2^n}\setminus\{0\};\, tr_n(y)=0, a^{2^j+1}=\frac{b}{y}\}$, and we know (as proved by Dobbertin for every APN power function in even dimension, and reported for instance in [11, Proposition 165]) that a^{2^j+1} ranges over the set of cubes of $\mathbb{F}_{2^n}$ when a ranges over $\mathbb{F}_{2^n}$ and $a\mapsto a^{2^j+1}$ is 3-to-1 over $\mathbb{F}_{2^n}^*$. This leads to determining those cubes which equal $\frac{b}{y}$ with $tr_n(y)=0$.

Remark. By using the Poisson summation formula (see e.g. [11, Corollary 3]), it is possible to relate the Hamming weight of any restriction of γ_F obtained by fixing a, respectively b, to the Fourier-Hadamard transform of γ_F (or to its Walsh transform), that is related as shown in [13] (see also Section 6 in the present paper) to the Walsh transform of F. We shall not give the details of the calculation, but we could check that this gives with no surprise that the Hamming weight of the restriction of γ_F obtained by fixing $a\neq 0_n$ equals 2^{n-1}. It also gives that the Hamming weight of the restriction of γ_F obtained by fixing $b\neq 0_n$ equals $2^{-(n+1)}\sum_{v\in\mathbb{F}_2^n} W_F^2(0_n,v)(-1)^{b\cdot v}$ (this could also be shown by using the Wiener-Khintchine formula, see e.g. [11, Relation 2.53]). We find again 2^{n-1} in the case of a permutation since we have then $W_F(0_n,v)=0$ for every $v\neq 0_n$. For non-permutations, $\sum_{v\in\mathbb{F}_2^n} W_F^2(0_n,v)(-1)^{b\cdot v}$ clearly depends on b.$\square$

Another property of γ_F is that, for every $a,a',b\in\mathbb{F}_2^n$ where a and a' are nonzero and distinct, if $\gamma_F(a,b)=1$ then there exists b' such that $\gamma_F(a',b')=\gamma_F(a+a',b+b')=1$. Indeed, there exists $x\in\mathbb{F}_2^n$ such that $b=D_aF(x)$ and taking $b'=D_{a'}F(x)$, we have $b+b'=D_{a+a'}F(x+a)$.

Since APN functions are rare, it seems obvious that γ_F cannot be any $2n$-variable Boolean function having the properties described above, but little is known on γ_F for general APN functions F, which would make it easier to distinguish when a general $2n$-variable Boolean function having such properties can be a γ_F function. After the investigation we shall make in the present paper, the Walsh transform will appear as the most efficient way of selecting functions likely to be γ_F functions (see Section 6).

Quadratic APN functions have a well-known additional property, which makes them slightly easier to find than general APN functions: the equation $D_aF(x)=b$ being linear, APNness reduces for them to the condition that, for every $a \neq 0_n$, the homogeneous linear equation $\varphi_F(a,x) := D_aF(x) + D_aF(0_n) = F(x) + F(x+a) + F(0_n) + F(a) = 0_n$ has exactly two solutions[1], which are 0_n and a. Note that φ_F is bilinear (more precisely, symplectic). Quadratic APN functions are probably rare among all APN functions, but they are rather numerous among known APN functions. The γ_F functions of quadratic APN functions have also well-known additional properties: for every $a \neq 0_n$, the support $Im(D_aF)$ of the function $b \mapsto \gamma_F(a,b)$ is an affine hyperplane, and since for every a, a', the function $D_aD_{a'}F(x)$ takes constant value and this value equals $D_aD_{a'}F(0_n) = \varphi_F(a,a')$, then for every $a, a' \neq 0_n$, $Im(D_aF)$ is stable under translation by $\varphi_F(a,a')$, since $D_aF(x) + D_aD_{a'}F(x) = D_aF(x+a')$ belongs to $Im(D_aF)$.

The general expression of the algebraic normal form or the univariate representation of γ_F has never been studied (the latter has been given only for the main examples of known almost bent functions, see [4]). We briefly address them in Section 4.

No real study of the algebraic degree of γ_F when F is a general APN function has been made (and for some known APN functions, it is not even easy to determine the algebraic degree of their γ_F function).

When F is almost bent, then we know that since γ_F is bent, it has algebraic degree at most n (see e.g. [11, Theorem 13] for the fact that any $2n$-variable bent function has algebraic degree at most n), but what is the lowest possible algebraic degree is unknown (and what are all the particularities of this bent function is also not clear).

The possible values of the algebraic degree of γ_F function for general APN function F are even more of a mystery. They can be as large as $2n-4$ (at least for n odd) since when F is the multiplicative inverse function $F(x) = x^{2^n-2}$, which is APN for n odd, we have (see [13]) $\gamma_F(a,b) = tr_n\left(\frac{1}{ab}\right) + 1 + \delta_0(a) + \delta_0(b) + \delta_0(a)\delta_0(b) + \delta_0(ab+1)$ and the algebraic degree of this function is $2n-4$, since the algebraic degree of $tr_n\left(\frac{1}{ab}\right)$ and of $\delta_0(a)\delta_0(b) + \delta_0(ab+1) = (a^{2^n-1}+1)(b^{2^n-1}+1) + (ab+1)^{2^n-1} + 1 = \sum_{i=0}^{2^n-2}(ab)^i + a^{2^n-1} + b^{2^n-1}$ equals $2n-2$ and these two functions have the same terms of algebraic degree $2n-2$, no term of algebraic degree $2n-3$ and different terms of algebraic degree $2n-4$. Can the algebraic degree be larger than $2n-4$? This is not clear (but we know it cannot equal $2n$ since γ_F has an even Hamming weight). It equals $2n-1$ if and only if F has algebraic degree n, since we have seen that $\sum_{b\in\mathbb{F}_2^n} b\,\gamma_F(a,b)$ equals the same value $\sum_{x\in\mathbb{F}_2^n} F(x)$ for every $a \neq 0_n$ and is zero for $a = 0_n$, and this implies $\sum_{a,b\in\mathbb{F}_2^n}(a,b)\,\gamma_F(a,b) = (0_n, \sum_{x\in\mathbb{F}_2^n} F(x))$. We know (see Section 2) that the nullity of these two sums is equivalent to the facts that, respectively, γ_F has degree less than $2n-1$ and F has degree less than n. Determine whether there exist APN (n,n)-functions of algebraic degree n is an open problem (proofs of non-existence are given in [5] within some general classes of functions).

Remark. According to the observations above, we have also that the algebraic degree of an APN function F equals n if and only if at least one (equivalently,

[1] This generalizes to plateaued APN functions, see [8, 11].

any) of the functions $f_a(b) = \gamma_F(a, b)$, $a \neq 0_n$, has algebraic degree $n - 1$. $\diamond$

What can be the lowest possible algebraic degree of γ_F functions is also unknown. We know it cannot be 0 or 1 because of the Hamming weight of γ_F. Note that McEliece's theorem [17] does not give more information: it tells us that the Hamming weights of $2n$-variable Boolean functions of algebraic degree at most r are divisible by $2^{\lceil \frac{2n}{r} \rceil - 1}$. Since the Hamming weight of γ_F is not divisible by 2^n, we have $\lceil \frac{2n}{r} \rceil - 1 < n$ and this only gives $d_{alg}(\gamma_F) > 1$. Considering the Hamming weight of restrictions does not seem to give information either: for instance, given $a \neq 0_n$, the restriction of γ_F to the $(n + 1)$-dimensional subspace $\{0_n, a\} \times \mathbb{F}_2^n$ has Hamming weight 2^{n-1}, which only tells that the algebraic degree is at least 2.

Note however that if γ_F is quadratic, then it is bent, and F is then almost bent (and n is odd), according to the result of [13] recalled in the introduction. The existence of APN functions F such that γ_F is quadratic reduces then to the existence of almost bent functions having this property, and the minimum algebraic degree of γ_F when F is an APN (n, n)-function with n even is at least 3. No (almost bent) function is known with a quadratic γ_F function for $n \geq 5$ (even for the quadratic Gold APN functions $F(x) = x^{2^j+1}$, $\gcd(j, n) = 1$, we have $\gamma_F(a, b) = 1 + tr_n(1 + ba^{2^n-2^j-2})$ as observed in [13] and the algebraic degree of γ_F is then $n - 2$). We leave open the question of the determination of the possible values of the algebraic degrees of the γ_F functions of APN (n, n)-functions, respectively, of almost bent (n, n)-functions, and in particular of their minimum values.

Nothing seems to be known either on the linear structures of γ_F, that is, those nonzero pairs $(\alpha, \beta) \in (\mathbb{F}_2^n)^2$ such that $D_{(\alpha,\beta)}\gamma_F(a, b) = \gamma_F(a, b) + \gamma_F(a + \alpha, b + \beta)$ is constant (even if we restrict ourselves to 0-valued linear structures, that is, those such that $D_{(\alpha,\beta)}\gamma_F(a, b)$ is the zero function - the others being called 1-valued). The study of linear structures is often one of the simplest studies to be done on Boolean functions. However, for γ_F functions, the question seems wide open, while knowing the linear structures on the γ_F functions of general APN functions F would tell much on F. We obtain partial results in Section 5 and deduce corollaries in Subsection 5.3.

What is known from [19] is that, for every APN (n, n)-function F with n even, there exists $v \neq 0_n$ such that the component function $v \cdot F$ has no (nonzero) linear structure, that is, admits no $a \neq 0_n$ such that the Boolean function $v \cdot (D_aF)$ is constant. This is equivalent to saying that, for every nonzero $a \in \mathbb{F}_2^n$, the set $\{b \in \mathbb{F}_2^n;\ \gamma_F(a, b) = 1\}$ is neither included in $\{0, v\}^\perp$ nor disjoint from this hyperplane. In other words, $\{b \in \mathbb{F}_2^n;\ \gamma_F(a, b) = 1\}$ is neither equal to $\{0, v\}^\perp$ nor equal to its complement. This is good to know but it is rather thin as a piece of information on γ_F.

We shall see in Subsection 6.3 that the nonlinearity of γ_F is closely related to that of F itself; many questions remain open about them. We shall provide a lower bound in Subsection 6.2 thanks to results obtained in Subsections 6 and 6.1.

It is difficult to make conjectures about the questions evoked above, since all known APN functions, except a sporadic one due to Edel and Pott [16], are either power functions or quadratic functions, and seem then peculiar.

4 On the algebraic normal form and univariate representation of γ_F

Let F be known by its ANF:

$$F(x) = \sum_{I \subseteq \{1,\ldots,n\}} u_I \prod_{i \in I} x_i; \quad u_I, x \in \mathbb{F}_2^n.$$

Let us denote by $f_1, \ldots, f_n$ the coordinate functions of F. Denoting $u_I = (u_{I,1}, \ldots, u_{I,n})$, we have that, for every $i = 1, \ldots, n$, the ANF of f_i is

$$f_i(x) = \sum_{I \subseteq \{1,\ldots,n\}} u_{I,i} \prod_{i \in I} x_i.$$

For every $a \in \mathbb{F}_2^n$, we have:

$$D_a F(x) = \sum_{I \subseteq \{1,\ldots,n\}} u_I \left(\sum_{J \subsetneq I} \prod_{i \in I \setminus J} a_i \prod_{i \in J} x_i \right),$$

$$D_a f_i(x) = \sum_{I \subseteq \{1,\ldots,n\}} u_{I,i} \left(\sum_{J \subsetneq I} \prod_{i \in I \setminus J} a_i \prod_{i \in J} x_i \right).$$

For every $a, b \in \mathbb{F}_2^n$, we have $\gamma_F(a,b) = 1$ if and only if $a \neq 0_n$ and $\exists x \in \mathbb{F}_2^n$; $b = D_a F(x)$. Since the contrary of "$\exists x \in \mathbb{F}_2^n$; $b = D_a F(x)$" is "$\forall x \in \mathbb{F}_2^n$; $\exists i \in \{1, \ldots, n\}$; $b_i + D_a f_i(x) + 1 = 0$" and a product is null if and only if one of its terms is null, we have then:

$$\gamma_F(a,b) =$$

$$(\delta_0(a) + 1) \left[1 + \prod_{x \in \mathbb{F}_2^n} \left(\prod_{i=1}^{n} [b_i + D_a f_i(x) + 1] + 1 \right) \right] =$$

$$(\delta_0(a)+1) \left[1 + \prod_{x \in \mathbb{F}_2^n} \left(\prod_{i=1}^{n} \left[b_i + \sum_{I \subseteq \{1,\ldots,n\}} u_{I,i} \left(\sum_{J \subsetneq I} \prod_{i \in I \setminus J} a_i \prod_{i \in J} x_i \right) + 1 \right] + 1 \right) \right].$$

This expression is rather complex, but the situation simplifies if we consider the univariate representation of F (leading to the bivariate expression of $\gamma_F(a,b)$) instead of its ANF. Let:

$$F(x) = \sum_{i=0}^{2^n-1} u_i x^i; \; u_i, x \in \mathbb{F}_{2^n}.$$

For every $a \in \mathbb{F}_{2^n}$, we have:

$$D_aF(x) = \sum_{i=0}^{2^n-1} u_i \sum_{j \preceq i; j \neq i} a^{i-j} x^j,$$

where $j \preceq i$ means that the binary expansion of j is covered by that of i. Indeed, for $i = \sum_{k \in K} 2^k$, we have $(x+a)^i = \prod_{k \in K} (x^{2^k} + a^{2^k}) = \sum_{K' \subseteq K} a^{\sum_{k \in K \setminus K'} 2^l} x^{\sum_{k \in K'} 2^l}$.
We have $\delta_0(a) = a^{2^n-1} + 1$ and for every $a, b \in \mathbb{F}_{2^n}$, $\gamma_F(a,b) = 1$ if $a \neq 0$ and $\exists x \in \mathbb{F}_{2^n}; b = D_aF(x)$. The contrary of "$\exists x \in \mathbb{F}_{2^n}; b = D_aF(x)$" is then "$\prod_{x \in \mathbb{F}_{2^n}} (b + D_aF(x))^{2^n-1} = 1$". We have then, for every $a, b \in \mathbb{F}_{2^n}$:

$$\gamma_F(a,b) =$$

$$a^{2^n-1} \left[1 + \prod_{x \in \mathbb{F}_{2^n}} (b + D_aF(x))^{2^n-1} \right] =$$

$$a^{2^n-1} \left[1 + \prod_{x \in \mathbb{F}_{2^n}} \left(b + \sum_{i=0}^{2^n-1} u_i \sum_{j \preceq i; j \neq i} a^{i-j} x^j \right)^{2^n-1} \right]. \tag{11}$$

Note that this expression of a and b has in general degree larger than 2^n in each variable a and b. The bivariate representation of $\gamma_F(a,b)$ is obtained after reducing Relation (11) modulo $a^{2^n} + a$ and $b^{2^n} + b$, that is, concretely, after:
- reducing modulo $2^n - 1$ each exponent of a (resp. b) which is not a multiple of $2^n - 1$,
- replacing by $2^n - 1$ each nonzero exponent of a (resp. b) which is a multiple of $2^n - 1$,
and this seems difficult to perform on the general expression.

5 On the linear structures of γ_F and their relation with bent components of F

We shall see in Subsection 5.3 that the study of 0-valued linear structures of the form $(0_n, \beta)$ of APN functions have consequences on the number of their bent components. Let us first show that these are the only ones which could possibly exist. In the next proposition W_{γ_F} denotes the Walsh transform of γ_F.

Proposition 1. *Let n be any positive integer, F any APN (n,n)-function, α and β any elements of $\mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$. Function γ_F admits (α, β) for ϵ-valued linear structure if and only if:*

$$\forall u, v \in \mathbb{F}_2^n, \ (\alpha \cdot u + \beta \cdot v = \epsilon + 1) \Rightarrow W_{\gamma_F}(u,v) = 0.$$

Function γ_F admits then no 1-valued linear structure and no (0-valued) linear structure (α, β) such that $\alpha \neq 0_n$.

For every $\beta \in \mathbb{F}_2^n$, $(0_n, \beta)$ is a 0-valued linear structure of γ_F if and only if all the component functions $v \cdot F$ such that $v \notin \{0_n, \beta\}^\perp$ are bent.
No APN (n,n)-function with n odd has linear structures.

Proof. It is known (see e.g. [11, Proposition 29]) that any n-variable Boolean function f admits $e \in \mathbb{F}_2^n$ for 0-valued (resp. 1-valued) linear structure if and only if the support $\{u \in \mathbb{F}_2^n;\, W_f(u) \neq 0\}$ of W_f is included in $\{0_n, e\}^\perp = \{x \in \mathbb{F}_2^n;\, e \cdot x = 0\}$ (resp. in its complement). This proves the first part of the proposition, after replacing n by $2n$, f by γ_F and e by (α, β).
It is known (see [13], or Section 6 below) that, for every $u, v \in \mathbb{F}_2^n$, $W_{\gamma_F}(u,v)$ equals 2^n if $v = 0_n$, and $2^n - W_F^2(u,v)$ otherwise. Since $W_{\gamma_F}(u,v)$ is then nonzero for every u if $v = 0_n$, this shows that, if (α, β) is a linear structure of γ_F, then the affine hyperplane $\{(u,v) \in (\mathbb{F}_2^n)^2;\, \alpha \cdot u + \beta \cdot v = \epsilon + 1\}$ has empty intersection with the vector space $\mathbb{F}_2^n \times \{0_n\}$, that is, the equation $\alpha \cdot u = \epsilon + 1$ has no solution, or equivalently, $\epsilon = 0$ and $\alpha = 0_n$. The rest of the proposition is straightforward. □

Open problem 1: Address the (non)existence of the linear structures of γ_F functions for general APN functions. Proposition 1 allows to restrict the study to 0-valued linear structures of the form $(0_n, \beta)$ for n even.

Remark. Thanks to Proposition 1, determining whether, for a given APN (n,n)-function F (n even), function γ_F has linear structures, is a sub-problem of determining what is the maximum dimension of the affine spaces of bent components of F. Indeed, if F admits a linear structure $(0_n, \beta)$, then the complement, say H, of $\{0_n, \beta\}^\perp$ is an affine hyperplane of $\mathbb{F}_2^n$ such that all the components $v \cdot F$, $v \in H$, of F are bent, and conversely, if we have such an affine hyperplane, then we have a linear structure. And it is easily seen (using that any APN function has nonzero nonlinearity, see [11, Proposition 161]) that, for any APN function F, the dimension of an affine subspace A of $\mathbb{F}_2^n$ equals the dimension of the affine subspace $\{v \cdot F;\, v \in A\}$ of $\mathcal{B}_n$. The functions $v \cdot F$, $v \in H$, above provide then an affine space of maximum dimension of bent components. This leads naturally to the following open question: what is, for a given even n, the largest dimension of the affine spaces of bent functions? All these questions seem difficult (probably more difficult, but also more interesting from the viewpoint of bent functions, than determining the number of bent components of vectorial functions, see Subsection 5.3). ⋄

Open problem 2: Determine, for every even positive integer n, the maximum dimension of affine spaces of bent components of APN (n,n)-functions.

Open problem 3: Determine, for every even positive integer n, the maximum dimension of affine spaces of bent n-variable Boolean functions.

Remark. An m-dimensional affine space of n-variable bent functions (n even) is a set of bent functions over $\mathbb{F}_2^n$ of the form $f + \sum_{i \in I} g_i$ where I ranges over

the subsets of $\{1, \dots m\}$ and where the g_i's are linearly independent Boolean functions. Let us denote by G the (n, m)-function whose coordinate functions are the g_i's. The functions write then $f + y \cdot G$ where y ranges over $\mathbb{F}_2^m$ and "$\cdot$" is the usual inner product. Note that the function $h : (x, y) \mapsto f(x) + y \cdot G(x)$ is a Maiorana-McFarland function (see [11]).
The function $x \mapsto f(x)+y \cdot G(x)$ is bent for every $y \in \mathbb{F}_2^m$ if and only if, for every nonzero $a \in \mathbb{F}_2^n$ and every y, the function $D_a f(x) + y \cdot D_a G(x)$ is balanced, that is, $\sum_{x \in \mathbb{F}_2^n} (-1)^{D_a f(x)+y \cdot G(x)} = 0$, and using that a pseudo-Boolean function is identically null if and only if its Fourier-Hadamard transform is identically null, this is equivalent to:

$$\forall a \in \mathbb{F}_2^n, a \neq 0, \forall b \in \mathbb{F}_2^m, \sum_{\substack{x \in \mathbb{F}_2^n \\ y \in \mathbb{F}_2^m}} (-1)^{D_a f(x)+y \cdot D_a G(x)+b \cdot y} =$$

$$2^m \sum_{x \in (D_a G)^{-1}(b)} (-1)^{D_a f(x)} = 0.$$

A necessary condition for all functions $f(x) + y \cdot G(x)$ to be bent is then that, for every nonzero $a \in \mathbb{F}_2^n$ and every b in $\mathbb{F}_2^m$, the size of the set $(D_a G)^{-1}(b)$ is divisible by 4. Indeed, if for some $a \neq 0$ and some b we have $|(D_a G)^{-1}(b)| \equiv 2 \pmod 4$, the sum $\sum_{x \in (D_a G)^{-1}(b)} (-1)^{D_a f(x)}$ is the double of an odd integer, since both the function $D_a f$ and the set $(D_a G)^{-1}(b)$ are invariant under translation by a (in particular, if G is an APN (n, n)-function, then it is impossible that the n-dimensional affine space of n-variable functions $f(x) + y \cdot G(x)$ is made of bent functions, only).
Once the necessary condition is satisfied, a necessary and sufficient condition is that, for every $a \neq 0$, function $D_a f$ is balanced on each pre-image by $D_a G$. $\diamond$

In the rest of this section, we shall, according to Proposition 1, assume n even and focus on 0-valued linear structures of the form $(0_n, \beta)$. Function γ_F admits $(0_n, \beta)$ for 0-valued linear structure if and only if, for every (a, b) such that $\gamma_F(a, b) = 1$, we have $\gamma_F(a, b + \beta) = 1$ (indeed, the condition is necessary, and it is sufficient since this implies that $\gamma_F(a, b) = 1$ is equivalent to $\gamma_F(a, b + \beta) = 1$ and therefore, $\gamma_F(a, b) = 0$ is equivalent to $\gamma_F(a, b + \beta) = 0$, and then $D_{(0_n, \beta)} \gamma_F(a, b)$ equals 0). Function γ_F admits then $(0_n, \beta)$ for 0-valued linear structure if and only if, for every nonzero a and every x in $\mathbb{F}_2^n$, there exists $y \in \mathbb{F}_2^n$ such that $D_a F(x) + D_a F(y) = \beta$. Thanks to the change of variable $b = x + y$, we have that γ_F admits $(0_n, \beta)$ for 0-valued linear structure if and only if, for every nonzero a and every x in $\mathbb{F}_2^n$, there exists $b \in \mathbb{F}_2^n$ such that $D_a D_b F(x) = \beta$.

Remark. Denoting $\Delta = \{(x, x);\, x \in \mathbb{F}_2^n\}$, we have that F being APN, the function $\phi : (a, x, y) \in (\mathbb{F}_2^n \setminus \{0_n\}) \times ((\mathbb{F}_2^n)^2 \setminus \Delta) \mapsto D_a F(x) + D_a F(y)$, involved in this characterization, is such that, when fixing any two elements among a, x and y, the corresponding restriction of ϕ is 2-to-1. Indeed, if we fix $a \neq 0_n$ and x (or y), then this corresponds exactly to the definition of APNness, and if we fix x and y such that $x \neq y$ and consider two distinct elements a, a' in $\mathbb{F}_2^n \setminus \{0_n\}$, then we have that $D_aF(x) + D_aF(y) = D_{a'}F(x) + D_{a'}F(y)$ if and only if $D_aF(x)+D_aF(y)+D_{a'}F(x)+D_{a'}F(y) = D_{a+a'}F(x+a)+D_{a+a'}F(y+a) = 0$ and F being APN and $x+y$ nonzero, this is equivalent to saying that $x+y = a+a'$. $\diamond$

It seems difficult to study the 0-valued linear structures of the form $(0_n, \beta)$ of γ_F, in general. We have seen that handling γ_F in bivariate representation is simpler than with the ANF. Let us then consider the expression in (11). The pair $(0, \beta)$ is a linear structure of γ_F if and only if the bivariate expression of $\gamma_F(a, b)$ is invariant under translation of b by β, that is, according to (11), if for every $a \neq 0$:

$$\prod_{x\in\mathbb{F}_{2^n}} \left(b + \sum_{i=0}^{2^n-1} u_i \sum_{j\preceq i; j\neq i} a^{i-j}x^j \right)^{2^n-1} \equiv$$

$$\prod_{x\in\mathbb{F}_{2^n}} \left(b + \beta + \sum_{i=0}^{2^n-1} u_i \sum_{j\preceq i; j\neq i} a^{i-j}x^j \right)^{2^n-1} \quad [\text{mod } a^{2^n} + a, b^{2^n} + b].$$

It seems hard to go further with this method, when dealing with general APN functions; this would need to handle the reduction modulo $a^{2^n} + a$ and $b^{2^n} + b$, which is necessary before we can apply the uniqueness of the univariate representation of an (n, n)-function.

5.1 The case of APN power functions

APN power functions are easier to study. For $F(x) = x^d$ and $a \neq 0$, we have $\gamma_F(a, b) = \gamma_F(1, \frac{b}{a^d})$, since $D_aF(ax) = a^d D_1F(x)$. Then, $(0, \beta)$ is a 0-valued linear structure of γ_F if and only if, for every $a \neq 0$, $\frac{\beta}{a^d}$ is a 0-valued linear structure of the n-variable function $\gamma_F(1, b)$. We know, according to the Dobbertin result already recalled and recorded in [11, Proposition 165], that when a ranges over $\mathbb{F}_{2^n}^*$ (n even), a^d ranges over the multiplicative group C of all cubes of $\mathbb{F}_{2^n}^*$. The existence of a (nonzero) 0-valued linear structure of the form $(0, \beta)$ for function γ_F would imply the invariance of the support of $\gamma_F(1, b)$ under the translation by any element of a coset $b\,C$ of C, and then under translation by any element of $b < C >$ where $< C >$ is the $\mathbb{F}_2$-vector space spanned by C. It is easily seen that, n being even, $x^3 + (x+1)^3$ ranges over the set E of elements of trace 0 and then $C + C$ equals $C\,E$, since $(ax)^3 + (ax+a)^3 = a^3(x^3 + (x+1)^3)$, and therefore $|C + C| > |E| = 2^{n-1}$ since there are cubes of traces 0 and 1, and therefore $< C >= \mathbb{F}_2^n$ (since its dimension is strictly larger than $n-1$ and equals then n), a contradiction since γ_F is not constant. According to Proposition 1, we have then:

Proposition 2. *For any n and for any APN power (n, n)-function F, the γ_F function has no (nonzero) linear structure.*

Remark. Despite the result of Proposition 2, for every $a \neq 0_n$, the Boolean function $b \mapsto \gamma_F(a,b)$ may have linear structures. For instance in the case of Gold APN functions over $\mathbb{F}_{2^n}$: $F(x) = x^{2^j+1}$, $\gcd(j,n) = 1$, we have that β is a linear structure of $b \mapsto \gamma_F(a,b)$ if and only if, for every $a \in \mathbb{F}_{2^n}$ there exists $y \in \mathbb{F}_{2^n}$ such that $a^{2^j}x + ax^{2^j} + a^{2^j+1} + a^{2^j}y + ay^{2^j} + a^{2^j+1} = a^{2^j+1}\left(\frac{x+y}{a} + \left(\frac{x+y}{a}\right)^{2^j}\right) = \beta$ and this happens for every β such that $tr_n\left(\frac{\beta}{a^{2^j+1}}\right) = 0$, but there is no $\beta \neq 0$ which satisfies this condition for every $a \neq 0$. ◇

5.2 Another class admitting no linear structure

Another case where the study of linear structures of γ_F is simplified (in fact, is straightforward) is when F is plateaued with a single amplitude, that is, when there exists some integer λ such that, for every $u, v \in \mathbb{F}_2^n$, $v \neq 0_n$, we have $W_F(u,v) \in \{0, \pm\lambda\}$. Indeed, since, according to Proposition 1, some component functions of F should be bent, all should then be bent, that is, F should be bent, and we know from [20] that no bent (n,n)-function exists.

According to [8], F is plateaued with a single amplitude if and only if the size of the set $\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = w\}$ does not depend on $x \in \mathbb{F}_2^n$ nor on $w \in \mathbb{F}_2^m$ when $w \neq 0_n$. Let us extend the non-existence result to those functions such that, for some $x \in \mathbb{F}_2^n$, the size of the set $\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = w\}$ does not depend on $w \in \mathbb{F}_2^m$ when $w \neq 0_n$.

Proposition 3. *Let n be any positive integer and F any APN (n,n)-function such that, for some $x \in \mathbb{F}_2^n$, the size of the set $\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = w\}$ does not depend on $w \in \mathbb{F}_2^m$ when $w \neq 0_n$. Then F admits non linear structure.*

Proof. According to Proposition 1, we can restrict ourselves to a 0-valued linear structure of the form $(0_n, \beta)$. Suppose that $(0_n, \beta)$ is such a linear structure of γ_F. Then, for every nonzero a, there exists $b \in \mathbb{F}_2^n$ such that $D_aD_bF(x) = \beta$, and we have then $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = \beta\}| \geq 2^n - 1$, but then we have $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, a \neq 0_n, b \neq 0_n, a \neq b\}| \geq \sum_{w \in \mathbb{F}_2^n \setminus \{0_n\}} |\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = w\}| = (2^n - 1)\ |\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = \beta\}| \geq (2^n-1)^2$, a contradiction since $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, a \neq 0_n, b \neq 0_n, a \neq b\}| = (2^n-1)(2^n-2)$. □

Remark. The class of those APN functions such that, for some x, the size $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(x) = w\}|$ does not depend on $w \in \mathbb{F}_2^m$ when $w \neq 0_n$, is larger than the class of plateaued APN functions with a single amplitude. Let us give examples of such functions which are not plateaued with a single amplitude. Let us take for instance $x = 0_n$ and restrict ourselves to those (n,n)-functions F such that $F(0_n) = 0_n$. We have that $|\{(a,b) \in (\mathbb{F}_2^n)^2\,;\, D_aD_bF(0_n) = w\}| = 2^{-n} \sum\limits_{a,b,v \in \mathbb{F}_2^n} (-1)^{v \cdot (F(a)+F(b)+F(a+b)+w)}$, equal to $2^{-4n} \sum_{a,b,v,u,u',u'' \in \mathbb{F}_2^n} W_F(u,v) W_F(u',v) W_F(u'',v) (-1)^{(u+u'') \cdot a + (u'+u'') \cdot b + v \cdot w} =$

$2^{-2n}\sum_{v,u\in\mathbb{F}_2^n} W_F^3(u,v)(-1)^{v\cdot w}$ and $|\{(a,b)\in(\mathbb{F}_2^n)^2\,;\,D_aD_bF(x)=w\}|$, does not depend on $w\neq 0_n$ if and only if $\sum_{u\in\mathbb{F}_2^n} W_F^3(u,v)$ does not depend on $v\neq 0_n$. This is for instance the case of power permutations.
Note that the proof of Proposition 3 above does not work for general plateaued functions (satisfying $\forall u,v\in\mathbb{F}_2^n, W_F(u,v)\in\{0,\pm\lambda_v\}$ for some integers λ_v depending only on v): it is shown in [8] that F is plateaued if and only if the size of the set $\{(a,b)\in(\mathbb{F}_2^n)^2\,;\,D_aD_bF(x)=w\}$ does not depend on $x\in\mathbb{F}_2^n$; but changing x for another value does not change $\{(a,b)\in(\mathbb{F}_2^n)^2\,;\,D_aD_bF(x)=w\}$ into a disjoint set, contrary to changing w for another value (when F is quadratic, it does not even change the set at all). Hence, we cannot have x playing the role played by w in the proof above. ◇

5.3 On the bent component functions of APN functions

We have seen that the component function $v\cdot F$ of an APN function F is bent if and only if $W_{\gamma_F}(u,v)$ equals 0 for every $u\in\mathbb{F}_2^n$. Now, since $W_{\gamma_F}(u,v)$ can be viewed as the value at u of the Fourier-Hadamard transform of the function $a\mapsto\sum_{b\in\mathbb{F}_2^n}(-1)^{\gamma_F(a,b)+v\cdot b}$, and since (as already used), a pseudo-Boolean function is identically null if and only if its Fourier-Hadamard transform is identically null, we have the following property, which could be proved also by using the Wiener-Khintchine formula:

Proposition 4. *Let F be any APN (n,n)-function. Then for every nonzero $v\in\mathbb{F}_2^n$, the component function $v\cdot F$ is bent if and only if, for every $a\in\mathbb{F}_2^n$, the Boolean function $b\mapsto\gamma_F(a,b)+v\cdot b$ is balanced.*

Remark. In this proposition, v is assumed nonzero. If we take $v=0_n$ and if F is APN, then the Boolean function $b\mapsto\gamma_F(a,b)+v\cdot b$ is balanced for every $a\neq 0_n$ but not for $a=0_n$. We could have stated the proposition with a nonzero instead of v nonzero since, if $v\neq 0_n$, $b\mapsto\gamma_F(a,b)+v\cdot b$ is automatically balanced for $a=0_n$. ◇

Remark. Replacing $(-1)^{\gamma_F(a,b)}$ (respectively, $(-1)^{v\cdot b}$) by $1-2\gamma_F(a,b)$ (respectively, by $1-2v\cdot b$) in the sum $\sum_{b\in\mathbb{F}_2^n}(-1)^{\gamma_F(a,b)+v\cdot b}$ and using that $b\mapsto v\cdot b$ is balanced for $v\neq 0_n$ (respectively, $b\mapsto\gamma_F(a,b)$ is balanced for $a\neq 0_n$), we have that, for every nonzero v, the component function $v\cdot F$ is bent if and only if, for every nonzero $a\in\mathbb{F}_2^n$, the Boolean function $b\mapsto v\cdot b$ is balanced on the set $\{b\in\mathbb{F}_2^n;\gamma_F(a,b)=1\}$ or its complement (respectively, the Boolean function $b\mapsto\gamma_F(a,b)$ is balanced on the hyperplane of equation $v\cdot b=1$ or its complement). ◇

Remark. Poposition 4 combined with Proposition 1 shows that $(0_n,\beta)$ is a linear structure of γ_F if and only if, for every $v\notin\{0_n,\beta\}^\perp$ and every $a\in\mathbb{F}_2^n$, the Boolean function $b\mapsto\gamma_F(a,b)+v\cdot b$ is balanced. ◇

It is shown in [22] that the number of bent components of any (n,n)-function is at most $2^n-2^{\frac{n}{2}}$ and that if an (n,n)-function F has $2^n-2^{\frac{n}{2}}$ bent components, then the set of values of v such that $v\cdot F$ is not bent is an $\frac{n}{2}$-dimensional vector space. In [18] (see also some precisions in the more recent reference [1]) is shown that the set of those (n,n)-functions having $2^n-2^{\frac{n}{2}}$ bent components does not contain any APN plateaued function (that is, as we saw already, any APN function F satisfying $\forall u,v\in\mathbb{F}_2^n, W_F(u,v)\in\{0,\pm\lambda_v\}$ for some integers λ_v depending only on v), and then in particular any quadratic APN function. We have:

Corollary 1. *For every even n and every APN (n,n)-function F, function F has $2^n-2^{\frac{n}{2}}$ bent components if and only if there exists an $\frac{n}{2}$-dimensional vector subspace V of $\mathbb{F}_2^n$ such that any pair $(0_n,\beta)$ with $\beta\in V$ is a 0-valued linear structure of γ_F.*

Proof. Let F have $2^n-2^{\frac{n}{2}}$ bent components, and according to [22], E be the $\frac{n}{2}$-dimensional vector space such that $v\cdot F$ is bent for $v\notin E$. Let us denote, for every $a\in\mathbb{F}_2^n$, by f_a the n-variable function $b\mapsto\gamma_F(a,b)$. According to Proposition 4, for every $a\in\mathbb{F}_2^n$, we have $W_{f_a}(v)=0$ for every $v\notin E$. According to the inverse Walsh transform relation (3), we have $\sum_{v\in\mathbb{F}_2^n}W_{f_a}(v)(-1)^{v\cdot b}=\sum_{v\in E}W_{f_a}(v)(-1)^{v\cdot b}=2^n(-1)^{f_a(b)},\forall b\in\mathbb{F}_2^n$, and this implies that, for every $\beta\in E^\perp:=\{x\in\mathbb{F}_2^n;\ v\cdot x=0,\ \forall v\in E\}$ and every $b\in\mathbb{F}_2^n$, we have $f_a(b+\beta)=f_a(b)$. We have then, for every $a,b\in\mathbb{F}_2^n$ and every $\beta\in E^\perp$, that $\gamma_F(a,b+\beta)=\gamma_F(a,b)$ and $(0_n,\beta)$ is a 0-valued linear structure of γ_F. This completes the proof in the direct sense since $E^\perp$ has dimension $\frac{n}{2}$. The converse is similar, using that $f_a(b+\beta)=f_a(b)$ for every $b\in\mathbb{F}_2^n$ and every $\beta\in E^\perp$ is equivalent to $W_{f_a}(v)=0$ for every $v\notin E$. □

Proposition 2 and Corollary 1 show then:

Corollary 2. *For every even n, any APN power (n,n)-function has strictly less than $2^n-2^{\frac{n}{2}}$ bent components.*

The following problem is posed in [22, Question 8]: are there any APN functions having $2^n-2^{\frac{n}{2}}$ bent components? We leave it open.

6 On the Walsh transform of γ_F and its nonlinearity

As already observed in [13], for every APN (n,n)-function F, we have that $\gamma_F(a,b)$, viewed as a pseudo-Boolean function, equals $\frac{|(D_aF)^{-1}(b)|}{2}-2^{n-1}\delta_0(a,b)$, and then, by the linearity of the Fourier-Hadamard transform: $\widehat{\gamma_F}(u,v)=\frac{1}{2}\sum_{a,x\in\mathbb{F}_2^n}(-1)^{u\cdot a+v\cdot D_aF(x)}-2^{n-1}=\frac{1}{2}W_F^2(u,v)-2^{n-1}$, which implies that γ_F is bent if and only if F is AB. According to Relation (2) applied with $2n$ in the place of n and (u,v) in the place of u, we have then $W_{\gamma_F}(0_n,0_n)=2^{2n}-W_F^2(0_n,0_n)+$

$2^n = 2^n$, and for $u \neq 0_n$ and $v \neq 0_n$: $W_{\gamma_F}(u, 0_n) = -W_F^2(u, 0_n) + 2^n = 2^n$ and $W_{\gamma_F}(u,v) = -W_F^2(u,v) + 2^n$, and then, for every u, v:

$$W_{\gamma_F}(u,v) = \begin{cases} 2^n \text{ if } v = 0_n, \\ 2^n - W_F^2(u,v) \text{ if } v \neq 0_n. \end{cases} \tag{12}$$

This kind of relation between the Walsh transform of a $2n$-variable Boolean function and the Walsh transform of an (n,n)-function is remarkable. The fact that the Walsh transform of this $2n$-variable Boolean function has all its values bounded above by 2^n (like bent functions) and that $2^n - W_{\gamma_F}(u,v)$ is moreover always a square is probably the most distinctive we know for functions γ_F (with of course also the fact that each restriction $b \mapsto \gamma_F(a,b)$ is balanced for $a \neq 0_n$). It would be interesting to make a computer investigation of those $2n$-variable Boolean functions, say γ, having the two properties:
- the n-variable function $b \mapsto \gamma(a,b)$ is balanced for every $a \neq 0_n$ and null for $a = 0_n$,
- all the values taken by $2^n - W_\gamma$, where W_γ is the Walsh transform of γ, are squares (equal to 0 when $v = 0_n$).
The computation of W_γ has complexity $2n\,2^{2n}$ which seems better than for checking the APNness of an (n,n)-function. Once such functions γ are found, we can use for each of them the resulting values of $|W_F(u,v)|$ and determine the possible signs so that F exists. This may be the hard part (see e.g. [23] for a related difficult problem) but we would have a corpus of investigation where finding new APN functions.
We study in the next subsections additional information on F, respectively on γ_F, provided by Relation (12).

Remark. When F is a power function $F(x) = x^d$, $x \in \mathbb{F}_{2^n}$, it is well known that, for $u \neq 0$, we have $W_F(u,v) = W_F(1, \frac{v}{u^d})$ (since $\sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(vx^d+ux)} = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{tr_n(\frac{v}{u^d}x^d+x)}$). We have then $W_{\gamma_F}(u,v) = W_{\gamma_F}(1, \frac{v}{u^d})$. Of course, this can also be checked directly. □

6.1 A new relation on the Walsh transform of APN functions deduced from (12)

In this subsection, we shall review the known relations satisfied by one of the functions W_F and W_{γ_F}, and see if this gives new information on the other.
- The inverse Walsh transform relation (3) applied to the component function $v \cdot F$ gives $\sum_{u\in\mathbb{F}_2^n} W_F(u,v)(-1)^{u\cdot w} = 2^n(-1)^{v\cdot F(w)}$, which does not seem to allow deducing any property on γ_F. The inverse Walsh transform relation applied to γ_F writes: $\displaystyle\sum_{u,v\in\mathbb{F}_2^n}(-1)^{u\cdot a+v\cdot b}W_{\gamma_F}(u,v) = 2^n \sum_{u,v\in\mathbb{F}_2^n}(-1)^{u\cdot a+v\cdot b} -$

$\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n}} (-1)^{u\cdot a+v\cdot b} W_F^2(u,v) = 2^{2n}(-1)^{\gamma_F(a,b)}$, that is:

$$\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n}} (-1)^{u\cdot a+v\cdot b} W_F^2(u,v) = 2^{3n}\delta_0(a,b) - 2^{2n}(-1)^{\gamma_F(a,b)}. \tag{13}$$

or equivalently, using that $(-1)^{\gamma_F(a,b)} = 1 - 2\,\gamma_F(a,b)$:

$$\sum_{u,v\in\mathbb{F}_2^n} (-1)^{u\cdot a+v\cdot b} W_F^2(u,v) = 2^{3n}\delta_0(a,b) + 2^{2n+1}\gamma_F(a,b).$$

This relation, which can also be deduced from Relation (6) applied to $f = v\cdot F$, does not give new information.
- The Parseval relation (4) applied to the component function $v\cdot F$ writes: $\forall v \in \mathbb{F}_2^n$, $\sum_{u\in\mathbb{F}_2^n} W_F^2(u,v) = 2^{2n}$, and implies:

$$\forall v \in \mathbb{F}_2^n, v \neq 0_n,\ \sum_{u\in\mathbb{F}_2^n} W_{\gamma_F}(u,v) = 0.$$

This relation can also be deduced by applying the Poisson summation formula (see e.g. [11, Corollary 3]) to γ_F and using that the Boolean function $b \mapsto \gamma_F(a,b)$ is balanced for each $a \neq 0_n$; it then gives no new information either.
The Parseval relation on γ_F provides (again) the value of the fourth moment of the Walsh transform of an APN function, see [15]: $\sum_{u,v\in\mathbb{F}_2^n} W_F^4(u,v) = 3\cdot 2^{4n} - 2^{3n+1}$.
- The Titsworth relation (5) applied to $v\cdot F$ does not seem to give anything exploitable on γ_F. When applied to γ_F, it writes:

$$\forall (u_0,v_0) \neq (0_n,0_n),\ \sum_{u,v\in\mathbb{F}_2^n} W_{\gamma_F}(u,v)W_{\gamma_F}(u+u_0,v+v_0) = 0, \tag{14}$$

that is:

- If $v_0 = 0_n$ (and $u_0 \neq 0_n$), then (by separating the case $v = 0_n$ from the case $v \neq 0_n$):

  $$2^{3n} + \sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n}} (2^n - W_F^2(u,v))(2^n - W_F^2(u+u_0,v)) = 0,$$

  that is, by using the Parseval relation on the Boolean function $v\cdot F$:

  $$\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n}} W_F^2(u,v)W_F^2(u+u_0,v) = -2^{3n} - 2^{3n}(2^n-1) + 2^{3n+1}(2^n-1) = 2^{4n} - 2^{3n+1}.$$

- If $v_0 \neq 0_n$ (and $u_0 \in \mathbb{F}_2^n$), then (by separating the cases $v = 0_n$, $v = v_0$ and $v \neq 0_n, v_0$):

  $$2^{n+1}\left(\sum_{u\in\mathbb{F}_2^n} (2^n - W_F^2(u,v_0))\right) +$$

$$\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n, v\neq v_0}} (2^n - W_F^2(u,v))(2^n - W_F^2(u+u_0, v+v_0)) =$$

$$\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n, v\neq v_0}} (2^n - W_F^2(u,v))(2^n - W_F^2(u+u_0, v+v_0)) = 0,$$

(by using again the Parseval relation on the Boolean function $v \cdot F$), that is, :

$$\begin{aligned}\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n, v\neq v_0}} W_F^2(u,v))W_F^2(u+u_0, v+v_0) &= -2^{3n}(2^n-2) + 2^{3n+1}(2^n-2)\\ &= 2^{4n} - 2^{3n+1}.\end{aligned}$$

The characterization of APNness by the fourth moment of the Walsh transform $\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n}} W_F^4(u,v) = 2^{4n+1} - 2^{3n+1}$, allows us to cover all cases in the following statement:

Theorem 1. *Any APN (n,n)-function F satisfies, for every (u_0, v_0), that:*

$$\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n, v\neq v_0}} W_F^2(u,v)W_F^2(u+u_0, v+v_0) = 2^{4n} - 2^{3n+1} + 2^{4n}\,\delta_0(u_0, v_0).$$

Of course, the converse is also true (i.e. this relation implies APNness) since in the particular case $u_0 = v_0 = 0_n$, we obtain the value of the fourth moment of W_F, which is characteristic of APNness. The relation of Theorem 1 looks like those obtained in [9], but in fact, it is quite different, for $(u_0, v_0) \neq (0_n, 0_n)$. Indeed, these latter relations involve the values at $(0_n, 0_n)$ of the convolutional products (of diverse orders) of the square of W_F with itself, and cannot then equal the expression of Theorem 1, which involves the value at a nonzero input of the convolutional product of order 2 of the square of W_F. The information provided by Theorem 1 is then complementary of those obtained in [9], and we shall see in the next subsection that it is in fact more exploitable.

6.2 A lower bound on the nonlinearity of a large class of APN functions including all known ones

In Theorem 1, if $|W_F(u,v)|$ takes its maximum at least twice, then denoting by $(u_0, v_0) \neq (0_n, 0_n)$ the difference between two values of (u,v) where this maximum is taken, we have since $\max_{v\neq 0_n, u} W_F^4(u,v)$ appears then at least twice in $\sum_{\substack{u,v\in\mathbb{F}_2^n\\ v\neq 0_n, v\neq v_0}} W_F^2(u,v)W_F^2(u+u_0, v+v_0)$:

Corollary 3. *Let n be any positive integer and F any APN (n,n)-function such that $\{|W_F(u,v)|; u,v \in \mathbb{F}_2^n, v \neq 0_n\}$ takes its maximum for at least two different inputs (u,v) (i.e. the minimum Hamming distance between the component* *functions of F and affine Boolean functions is achieved more than once), then we have :*

$$nl(F) \geq 2^{n-1} - \frac{1}{2}\sqrt[4]{2^{4n-1} - 2^{3n}}.$$

Indeed, we have according to Theorem 1 that $2\max_{v\neq 0_n,u} W_F^4(u,v) \leq 2^{4n} - 2^{3n+1}$ and Corollary 3 is then deduced from Relation (8).
Note that all known APN functions satisfy the condition of Corollary 3. Indeed, all APN power functions do[2] because, for n odd, all component functions $tr_n(vx^d)$ are affine equivalent to each others, and for n even, any two component functions $tr_n(vx^d)$ and $tr_n(v'x^d)$ are affine equivalent when $\frac{v}{v'}$ is a cube. All quadratic functions also satisfy the condition (more generally, all plateaued functions do) and the sporadic Edel-Pott function having the same Walsh spectrum as the Gold functions, it does too.

Open problem 4: Determine whether all APN functions satisfy the condition of Corollary 3. If not, then characterize, and if possible determine, all the (n,m)-functions that do not satisfy the condition of this corollary.

Remark. Even for general (n,m)-functions, it is not that easy to build functions that do not satisfy the condition of Corollary 3 (among which we could search for APN functions with low nonlinearity). The study is simplified when considering those (n,m)-functions obtained by modifying the values of an affine function $L(x)+a$ (where L is linear over $\mathbb{F}_2^n$) over a set E of size less than 2^{n-2} (which is favorable to a search of functions with low nonlinearity), but even then, the condition is not straightforward. For such function F, denoting for every $x \in E$ by $\phi(x)$ the vector added to $L(x)+a$ to obtain $F(x)$, by L^* the adjoint operator of L, defined by $v\cdot L(x) = L^*(v)\cdot x$, and by δ_b the indicator function of the singleton $\{b\}$ (that is, the Dirac symbol at b), we have $W_F(u,v) = 2^n(-1)^{v\cdot a}\delta_{L^*(v)}(u) - (-1)^{v\cdot a}\sum_{x\in E}(-1)^{(L^*(v)+u)\cdot x} + (-1)^{v\cdot a}\sum_{x\in E}(-1)^{(L^*(v)+u)\cdot x+v\cdot\phi(x)}$.
Since $|E| < 2^{n-2}$, the value of $\max\limits_{u\in\mathbb{F}_2^n, v\in\mathbb{F}_2^m\setminus\{0_m\}} |W_F(u,v)|$ is achieved for $u = L^*(v)$ and equals $2^n - |E| + \max_{v\in\mathbb{F}_2^m\setminus\{0_m\}}\sum_{x\in E}(-1)^{v\cdot\phi(x)}$, which is reached only for one value of $(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^m\setminus\{0_m\}$ under the necessary and sufficient condition that the maximum $\max_{v\in\mathbb{F}_2^m\setminus\{0_m\}}\sum_{x\in E}(-1)^{v\cdot\phi(x)}$ is achieved by one value of v only (this condition is always satisfied if $m=1$, that is, for a Boolean function, but it is not straightforward for $m>1$, and in any case, the relation $|Im(F)| \geq \left\lceil \frac{2^{2n}}{3\cdot 2^n - 2}\right\rceil$ shown in [14, 12] on the image set size of every APN function and applied to $F+L+a$ shows that, since $|E| < 2^{n-2}$, function F cannot be APN. A larger class could be investigated: that of all the functions defined the same way but with $|E|$ larger than $\frac{2^{2n}}{3\cdot 2^n-2}$; characterizing that such a function does not satisfy the condition of Corollary 3 seems very complex, since $\frac{2^{2n}}{3\cdot 2^n-2}$ is large.
◇

[2] But the bound of Corollary 3 is weaker than the bound from [9], which writes that $nl(F) \geq 2^{n-1} - 2^{\frac{3n-3}{4}}$ for n odd and $nl(F) \geq 2^{n-1} - 2^{\frac{3n-2}{4}}$ for n even.

Note that the bound of Corollary 3 can be further improved if there exists $(u_0, v_0) \neq (0_n, 0_n)$ for which there exist more than two values of (u, v) such that both $|W_F(u, v)|$ and $|W_F(u + u_0, v + v_0)|$ achieve the maximum of $\{|W_F(u, v)|; u, v \in \mathbb{F}_2^n, v \neq 0_n\}$: according to Theorem 1, if the number of these values (u, v) equals t, then we have $nl(F) \geq 2^{n-1} - \frac{1}{2}\sqrt[4]{\frac{2^{4n}-2^{3n+1}}{t}}$.

Anyway, the bound of Corollary 3 and its possible improvement have the form $nl(F) \geq \lambda 2^{n-1}$ (where of course $\lambda < 1$) and a nonlinearity more or less equal to $\lambda \cdot 2^{n-1}$ is asymptotically bad.

6.3 On the relation between the nonlinearities of γ_F and of F

The nonlinearity of γ_F equals, thanks to Relation (7) (applied with $2n$ in the place of n) and to Relation (12) and to the fact that $W_F(u, 0_n) = 0$ for $u \neq 0_n$:

$$\begin{aligned} nl(\gamma_F) &= 2^{2n-1} - \frac{1}{2}\max\left(2^n, \max_{(u,v)\in\mathbb{F}_2^n\times(\mathbb{F}_2^n\setminus\{0_n\})} |2^n - W_F^2(u, v)|\right) \\ &= 2^{2n-1} - \frac{1}{2}\max\left(2^n, \max_{(u,v)\in\mathbb{F}_2^n\times\mathbb{F}_2^n\setminus\{(0_n,0_n)\}} |2^n - W_F^2(u, v)|\right). \end{aligned}$$

For being able to deduce the expression of $nl(\gamma_F)$ by means of $nl(F)$, we need to look separately at the distances from γ_F to all linear $2n$-variable Boolean functions and to all of their complements:
- the former equals $2^{2n-1} - \frac{1}{2}\max\left(2^n, \max_{(u,v)\in\mathbb{F}_2^n\times(\mathbb{F}_2^n\setminus\{0_n\})}(2^n - W_F^2(u, v))\right) = 2^{2n-1} - 2^{n-1}$ and is achieved by the zero linear function (among others),
- the latter equals $2^{2n-1} - \frac{1}{2}\max_{(u,v)\in\mathbb{F}_2^n\times(\mathbb{F}_2^n\setminus\{0_n\})}(W_F^2(u, v) - 2^n)$.
We have $\max_{(u,v)\in\mathbb{F}_2^n\times(\mathbb{F}_2^n\setminus\{0_n\})} W_F^2(u, v) \geq 2^{n+1}$, according to the SCV bound. The nonlinearity of γ_F equals then the minimum Hamming distance between γ_F and the complements of linear forms (and if F is not AB, then the best affine approximations of γ_F are only with such complements).

Proposition 5. *Let n be any positive integer and F any APN (n, n)-function being not almost bent. The best approximations of γ_F by $2n$-variable affine Boolean functions are the functions $\ell(a, b) = u \cdot a + v \cdot b + 1$, $v \neq 0_n$, such that the Hamming distance between the component function $v \cdot F$ and the n-variable affine Boolean function $u \cdot x + \epsilon$, is minimum for some $\epsilon \in \mathbb{F}_2$.*

The fact that attacking, by the linear attack, a block cipher using an APN function F as a substitution box is related to attacking, by the fast correlation attack, a stream cipher in the filter model (see e.g. [11, Subsection 3.1.3]) using γ_F as nonlinear function, is interesting. Moreover, since the nonlinearity of F equals $2^{n-1} - \frac{1}{2}\max_{(u,v)\in\mathbb{F}_2^n\times(\mathbb{F}_2^n\setminus\{0_n\})} |W_F(u, v)|$, we have:

$$nl(\gamma_F) = 2^{2n-1} - \frac{1}{2}\left((2^n - 2nl(F))^2 - 2^n\right).$$

Hence:

Proposition 6. *For every APN (n, n)-function, we have:*

$$nl(\gamma_F) = 2^{n+1} nl(F) - 2(nl(F))^2 + 2^{n-1}. \tag{15}$$

Note that the function $x \mapsto 2^{n+1}x - 2x^2 + 2^{n-1}$ is strictly increasing from the interval $]0, 2^{n-1} - 2^{\frac{n-1}{2}}]$ (within which the nonlinearity of an (n, n)-function is located, according to the lower bound $nl(F) > 0$ and to the SCV upper bound) onto the interval $]2^{n-1}, 2^{2n-1} - 2^{n-1}]$ (within which the nonlinearity of the $2n$-variable Boolean function γ_F is located, according to (15) and to the covering radius bound). The value of $nl(\gamma_F)$ is then a strictly increasing function of $nl(F)$ which matches it maximum $2^{2n-1} - 2^{n-1}$ at $2^{n-1} - 2^{\frac{n-1}{2}}$ and Proposition 6 can be viewed as a generalization and a clarification of the fact that γ_F is bent if and only if F is almost bent. The puzzling question is that, while we know the maximum of each of the two nonlinearities for n odd, we ignore the minimum.
Note that, according to Proposition 6, the possible values of $nl(\gamma_F)$ are not all the integers of the interval $]2^{n-1}, 2^{2n-1} - 2^{n-1}]$. For instance, for $n = 5$, if $nl(F)$ could take any value between 1 and 12, the nonlinearity of γ_F could take only the values 78, 136, 190, 240, 286, 328, 366, 400, 430, 456, 478, 496. In fact, the possible values of $nl(F)$ are all known[3], see [2], and they are not all the integers between 1 and 12; indeed, there are only two possible values: the nonlinearity 10 of the Dobbertin and inverse functions and the nonlinearity 12 of almost bent functions; the nonlinearity of γ_F can then only take the values 456 and 496.

Open problem 5: Determine, for every n, which values are possible for $nl(F)$ when F is a general APN (n, n)-function, and therefore, determine which values are possible for $nl(\gamma_F)$. There are several sub-problems: determine whether $nl(F)$ can be an odd integer, which is equivalent to determining whether $nl(\gamma_F)$ can be congruent with 2 modulo 4; a positive reply would imply a positive reply to the open problem whether the algebraic degree of F can be equal to n, already mentioned. Note that for general functions F, the fact that the algebraic degree equals n does not necessarily imply that the nonlinearity is odd (take for instance a linear function and modify one of its coordinate functions so that its Hamming weight becomes odd, the algebraic degree equals then n while the nonlinearity is zero); it is not clear whether we have the same situation when restricting ourselves to APN functions (this provides then one more open problem).

Conclusion

In this paper, we have initiated a study of the $2n$-variable Boolean function γ_F (indicating where the equation $F(x) + F(x + a) = b$ has solutions $x \in \mathbb{F}_2^n$ for $a, b \in \mathbb{F}_2^n$, $a \neq 0_n$) when F is a general APN (n, n)-function. We have described how the representations of γ_F can be obtained from those of F, and shown the difficulty of studying γ_F, for instance through its linear structures. We have related the existence of linear structures to that of affine spaces of bent Boolean

[3] Number 5 is the largest value of n for which they are.

functions. We have also shown how γ_F can be used for studying F. We have in particular more deeply studied the relationship between the nonlinearities of F and γ_F and derived a lower bound which gives a beginning of explanation why the nonlinearity of all known APN functions is rather good. More needs to be done in this direction. We have posed five open problems (and a few sub-problems) (1) on the linear structures of γ_F functions, (2) on the largest dimension of affine spaces of bent components of APN functions, (3) on the largest dimension of affine spaces of bent Boolean functions, (4) whether all APN functions have Walsh transforms taking their maximum absolute value for at least two different nonzero inputs (whose positive answer would provide a lower bound on the nonlinearity of all APN functions), and (5) on the possible values of $nl(F)$ and $nl(\gamma_F)$ when F is APN. Further work is needed on these difficult problems and on other questions on γ_F functions that we also listed, which have not been tackled since the introduction of APN functions thirty years ago.

Acknowledgement

We thank Sihem Mesnager for her useful information and her kind help.

References

[1] N. Anbar, T. Kalaycı, W. Meidl and L. Mérai. On functions with the maximal number of bent components. Arxiv.com

[2] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography* 49 , Issue 1-3, pp. 273-288, 2008. Revised and extended version of a paper with the same title in the Proceedings of the Workshop on Coding and Cryptography WCC 2007, pp. 39-48, 2007.

[3] L. Budaghyan. *Construction and Analysis of Cryptographic Functions.* 168 pages. Springer 2014, ISBN 978-3-319-12990-7

[4] L. Budaghyan, C. Carlet and T. Helleseth. On bent functions associated to AB functions. *Proceedings of the IEEE Information Theory Workshop ITW 2011.*

[5] L. Budaghyan, C. Carlet, T. Helleseth, N. Li and B. Sun. On upper bounds for algebraic degrees of APN functions. *IEEE Transactions on Information Theory* 64 (6), pp. 4399-4411, 2018.

[6] C. Boura, A. Canteaut, J. Jean and V. Suder. Two notions of differential equivalence on Sboxes. *Designs, Codes and Cryptography* 87 (2-3), pp.185-202, 2019.

[7] A. Canteaut and M. Videau. Degree of composition of highly nonlinear functions and applications to higher order differential cryptanalysis. *Pro-*

ceedings of EUROCRYPT 2002, Lecture Notes in Computer Science 2332, pp. 518-533, 2002.

[8] C. Carlet. Boolean and vectorial plateaued functions, and APN functions. *IEEE Transactions on Information Theory* 61 (11), pp. 6272-6289, 2015.

[9] C. Carlet. Characterizations of the differential uniformity of vectorial functions by the Walsh transform, *IEEE Transactions on Information Theory* 64 (9), pp. 6443-6453, 2018. (preliminary version available in *IACR Cryptology ePrint Archive* http://eprint.iacr.org/ 2017/516, 2017).

[10] C. Carlet. Graph indicators of vectorial functions and bounds on the algebraic degree of composite functions. *IEEE Transactions on Information Theory* 66 (12), pp. 7702-7716, 2020.

[11] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Monograph in *Cambridge University Press*, 2020.

[12] C. Carlet. On the image set size of differentially uniform functions and related bounds on their nonlinearity and their distance to affine functions. *IACR Cryptology ePrint Archive* (http://eprint.iacr.org/) 2020/1529, 2020.

[13] 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.

[14] C. Carlet, A. Heuser and S. Picek. Trade-Offs for S-Boxes: Cryptographic Properties and Side-Channel Resilience. *Proceedings of ACNS 2017, Lecture Notes in Computer Science* 10355, pp. 393-414, 2017.

[15] F. Chabaud and S. Vaudenay. Links between Differential and Linear Cryptanalysis. *Proceedings of EUROCRYPT 1994, Lecture Notes in Computer Science* 950, pp. 356-365, 1995.

[16] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications* 3 (1), pp. 59-81, 2009.

[17] R. J. McEliece. Weight congruence for p-ary cyclic codes. *Discrete Mathematics*, 3, pp. 177-192, 1972.

[18] S. Mesnager, F. Zhang, C. Tang and Y. Zhou. Further study on the maximum number of bent components of vectorial functions. *Designs, Codes and Cryptography* 87 (11), pp. 2597-2610, 2019. Also: arXiv:1801.06542.

[19] A. Musukwa and M. Sala. On the linear structures of balanced functions and quadratic APN functions. *Cryptography and Communications* 12 (5), pp. 859-880, 2020.

[20] K. Nyberg. Perfect non-linear S-boxes. *Proceedings of EUROCRYPT 1991, Lecture Notes in Computer Science* 547, pp. 378-386, 1992.

[21] K. Nyberg. On the construction of highly nonlinear permutations. *Proceedings of EUROCRYPT 1992, Lecture Notes in Computer Science* 658, pp. 92-98, 1993.

[22] A. Pott, E. Pasalic, A. Muratović-Ribić and S. Bajrić. On the Maximum Number of Bent Components of Vectorial Functions. *IEEE Transactions on Information Theory* 64(1), pp. 403-411, 2018.

[23] V. Suder. Antiderivative functions over $\mathbb{F}_2^n$. *Designs, Codes and Cryptography* 82 (1- 2), pp. 435-447, 2017.