On some cryptographic properties of Boolean functions*

A. Musukwa[0000−0001−8792−6954], M. Sala[0000−0002−7266−5146], and M. Zaninelli[0000−0002−4425−7751]

University of Trento, Via Sommarive, 14, 38123 Povo, Trento, Italy
{augustinemusukwa, maxsalacodes, zaninelli.marco21}@gmail.com

Abstract. In this paper some cryptographic properties of Boolean functions, including weight and nonlinearity, are studied. We present some quantities derived from the behaviour of second-order derivatives, which allow us to determine whether a function is APN.

Keywords: Splitting functions · Nonlinearity · APN functions

1 Preliminaries

In this section we report some definitions and results which are well-known and relevant to our work. For details, the reader is referred to [2,6,8,9,10].

We denote the field of two elements, 0 and 1, by $\mathbb{F}$. We will denote any vector in $\mathbb{F}^n$ by v. We use ordinary addition $+$ instead of XOR $\oplus$. For any set A, $|A|$ denotes its size.

A *Boolean function (B.f.)* is any function f from $\mathbb{F}^n$ to $\mathbb{F}$ and a *vectorial Boolean function (v.B.f.)* is any function F from $\mathbb{F}^n$ to $\mathbb{F}^m$, $n, m \in \mathbb{N}$. However, we only consider v.B.f.'s from $\mathbb{F}^n$ to $\mathbb{F}^n$. We represent the B.f.'s in algebraic normal form (ANF for short) which is the n-variable polynomial representation over $\mathbb{F}$ given by

$$f(x_1, ..., x_n) = \sum_{I \subseteq \mathcal{P}} a_I \left(\prod_{i \in I} x_i \right)$$

where $\mathcal{P} = \{1, ..., n\}$ and $a_I \in \mathbb{F}$. We will write $X = \{x_1, ..., x_n\}$. The *algebraic degree* or simply *degree* of f (denoted by $\deg(f)$) is $\max_{I \subseteq \mathcal{P}}\{|I| \mid a_I \neq 0\}$. The set of all B.f.'s is denoted by B_n.

For a B.f. f, we say that f is *linear* if $\deg(f) \leq 1$ and $f(0) = 0$, *affine* if $\deg(f) \leq 1$, *quadratic* if $\deg(f) = 2$ and *cubic* if $\deg(f) = 3$. The set of all affine functions is denoted by A_n. Given a v.B.f. $F = (f_1, ..., f_n)$, the functions $f_1, ..., f_n$ are called *coordinate functions* and the functions $\lambda \cdot F$, with $\lambda \in \mathbb{F}^n$ and "$\cdot$" denoting dot product, are called *component functions*. If $\lambda \neq 0$, then $\lambda \cdot F$ is a *nontrivial component*. The degree of a v.B.f. F is given by $\deg(F) = \max_{\lambda \in \mathbb{F}^n \setminus \{0\}}\{\deg(\lambda \cdot F)\}$. We say that F is *quadratic* if $\deg(F) = 2$ and *cubic* if

* University of Trento

$\deg(F) = 3$. If all nontrivial components of a cubic v.B.f. F are cubic, we call F a *pure cubic*.

For $m < n$, if f is in B_n and depends only on m variables, then we denote by $f_{\restriction \mathbb{F}^m}$ its restriction to these m variables. Clearly $f_{\restriction \mathbb{F}^m} \in B_m$. The *Hamming weight* of f is given by $\mathrm{w}(f) = |\{x \in \mathbb{F}^n \mid f(x) = 1\}|$. We say that f is *balanced* if $\mathrm{w}(f) = 2^{n-1}$. The *distance* between f and g is $d(f, g) = \mathrm{w}(f + g)$ and the *nonlinearity* of f is $\mathcal{N}(f) = \min_{\alpha \in A_n} d(f, \alpha)$.

We define the *Walsh transform* of f, the function $\mathcal{W}_f$ from $\mathbb{F}^n$ to $\mathbb{Z}$, as

$$\mathcal{W}_f(a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+l_a(x)},$$

where $l_a(x) = a \cdot x$, for all $a \in \mathbb{F}^n$. Let $\mathcal{L}(f) = \max\limits_{a \in \mathbb{F}^n} |\mathcal{W}_f(a)|$. We define $\mathcal{F}(f)$ as

$$\mathcal{F}(f) = \mathcal{W}_f(0) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} = 2^n - 2\mathrm{w}(f).$$

Note that f is balanced if and only if $\mathcal{F}(f) = 0$.

Theorem 1. *Let $f \in B_n$. Then $\mathcal{N}(f) = 2^{n-1} - \frac{1}{2}\mathcal{L}(f)$.*

We say that $f \in B_n$ is *bent* if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ which can happen only for n even. Note that the highest possible value for $\mathcal{L}(f)$ is $2^{\frac{n}{2}}$ and this bound is achieved for bent functions (and only them).

The *(first-order) derivative* of f at a is defined by $D_a f(x) = f(x + a) + f(x)$ and the *(second-order) derivative* at a and b is $D_b D_a f(x) = f(x) + f(x + b) + f(x + a) + f(x + a + b)$ (these definitions are extended to v.B.f.'s in a similar way).

Theorem 2. *$f \in B_n$ is bent if and only if $D_a f$ is balanced for any nonzero a.*

For n odd, a B.f. f is called *semi-bent* if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$. A v.B.f. F in odd dimension is *almost-bent (AB)* if all its nontrivial components are semi-bent.

Theorem 3. *Let F be a v.B.f. Then F is a* permutation *if and only if all nontrivial components are balanced.*

Two B.f.'s $f, g : \mathbb{F}^n \to \mathbb{F}$ are said to be *affine equivalent* if there exist an affinity $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ such that $f = g \circ \varphi$. We denote this relation by $\sim_A$ and write $f \sim_A g$. Observe that $\sim_A$ is an equivalence relation.

Proposition 1. *Let $f, g \in B_n$ be such that $f \sim_A g$. Then $\mathrm{w}(f) = \mathrm{w}(g)$ and so f is balanced $\iff$ g is balanced.*

Proposition 2. *Let $f, g \in B_n$, $f \sim_A g$. Then $\{|\mathcal{W}_f(a)|\}_{a \in \mathbb{F}^n} = \{|\mathcal{W}_g(a)|\}_{a \in \mathbb{F}^n}$.*

Definition 1. *Let $f \in B_n$. For $k \in \mathbb{N}$, $L_k(f) = \sum_{a \in \mathbb{F}^n} |\mathcal{W}_f(a)|^k$ is called the* kth power moment *of the Walsh transform.*

Observe that, by Proposition 2, the following corollary holds.

Corollary 1. *Let $f, g \in B_n$, $f \sim_A g$. Then $L_k(f) = L_k(g)$ and $\mathcal{N}(f) = \mathcal{N}(g)$.*

From now on, if no confusion arises, for any $f, g \in B_n$ that are either $f \sim_A g$ or $f \sim_A g + 1$, we write $f \sim_A g/ + 1$. In the following theorem we report the classification of quadratic B.f.'s under affine equivalence.

Theorem 4. *Let $f \in B_n$ be quadratic. Then*

(i) $f \sim_A x_1x_2 + \cdots x_{2k-1}x_{2k} + x_{2i+1}$ with $k \leq \lfloor \frac{n-1}{2} \rfloor$ if f is balanced,
(ii) $f \sim_A x_1x_2 + \cdots x_{2k-1}x_{2k}/ + 1$ with $k \leq \lfloor \frac{n}{2} \rfloor$ if f is unbalanced.

2 On the weight of Boolean functions

In this section we classify the weight of some particular functions. We determine some conditions for these functions to be balanced. Any result not done by us has been cited. To meet the page limit, most proofs have been omitted.

Definition 2. *Let $f \in B_n$. We say that f is a* splitting function *if $\exists \bar{f} \sim_A f$ such that $\bar{f} = g(x_1, ..., x_i) + h(x_{i+1}, ..., x_n)$, with $i < n$, $g \in B_i$ and $h \in B_{n-i}$.*

Remark 1. If $g(x_1, ..., x_i)$ is in B_n then $\mathrm{w}(g) = 2^{n-i}\mathrm{w}(g_{\restriction \mathbb{F}^i})$ and $\mathcal{F}(g) = 2^{n-i}\mathcal{F}(g_{\restriction \mathbb{F}^i})$. Furthermore, g is balanced if and only if $g_{\restriction \mathbb{F}^i}$ is balanced and also $\mathcal{F}(g) = 0$ if and only if $\mathcal{F}(g_{\restriction \mathbb{F}^i}) = 0$.

Next we consider the weight and balancedness of splitting B.f.'s.

Lemma 1. *Let $f \in B_n$ be such that $f \sim_A g(x_1, ..., x_i) + h(x_{i+1}, ..., x_n)$, with $i < n$ Then*

$$\mathcal{F}(f) = \mathcal{F}(g_{\restriction \mathbb{F}^i})\mathcal{F}(h_{\restriction \mathbb{F}^{n-i}}) = 2^{-n}\mathcal{F}(g)\mathcal{F}(h).$$

Proof. Let $x = (x', x'')$ with $x' \in \mathbb{F}^i$ and $x'' \in \mathbb{F}^{n-i}$. So

$$\begin{aligned}\mathcal{F}(f) &= \sum_{x=(x',x'')\in\mathbb{F}^n} (-1)^{g(x')+h(x'')} = \sum_{x'\in\mathbb{F}^i} (-1)^{g(x')} \sum_{x''\in\mathbb{F}^{n-i}} (-1)^{h(x'')} \\ &= \mathcal{F}(g_{\restriction \mathbb{F}^i})\mathcal{F}(h_{\restriction \mathbb{F}^{n-i}}) = 2^{-n}\left(2^{n-i}\mathcal{F}(g_{\restriction \mathbb{F}^i})\right)\left(2^{i}\mathcal{F}(h_{\restriction \mathbb{F}^{n-i}})\right) = 2^{-n}\mathcal{F}(g)\mathcal{F}(h).\end{aligned}$$

Remark 2. Recall that $X = \{x_1, ..., x_n\}$. For $1 \leq i \leq t$, let $X_i \subset X$ be such that all X_i are pairwise disjoint. It is immediate, by Remark 1 and Lemma 1, that if $f(X) = f_1(X_1) + \cdots + f_t(X_t)$, with $|X_i| = n_i$, then $\mathcal{F}(f) = 2^{n-s}\prod_{i=1}^{t}\mathcal{F}(f_{i\,\restriction \mathbb{F}^{n_i}})$ with $s = n_1 + \cdots + n_t$.

Theorem 5. *Let $f \in B_n$ be such that $f \sim_A g(x_1, ..., x_i) + h(x_{i+1}, ..., x_n)$, with $i < n$. Then*

$$\begin{aligned}\mathrm{w}(f) &= 2^{n-i}\mathrm{w}(g_{\restriction \mathbb{F}^i}) + 2^i\mathrm{w}(h_{\restriction \mathbb{F}^{n-i}}) - 2\mathrm{w}(g_{\restriction \mathbb{F}^i})\mathrm{w}(h_{\restriction \mathbb{F}^{n-i}}) \\ &= \mathrm{w}(g) + \mathrm{w}(h) - 2^{1-n}\mathrm{w}(g)\mathrm{w}(h).\end{aligned}$$

We now present some results on balanced splitting functions.

Theorem 6. *Let $f \in B_n$ be such that $f \sim_A g(x_1, ..., x_i) + h(x_{i+1}, ..., x_n)$. Then f is balanced if and only if either g or h is balanced.*

Proof. f is balanced $\iff \mathcal{F}(f) = 0 \iff \big(\mathcal{F}(g_{\restriction \mathbb{F}^i}) = 0$ or $\mathcal{F}(h_{\restriction \mathbb{F}^{n-i}}) = 0\big) \iff$ either g or h is balanced.

Proposition 3. *Let $f \in B_n$, $\deg(f) = m$, be such that $f \sim_A \sum_{i=0}^{k-1} \prod_{j=1}^{m} x_{mi+j}$. Then $\mathrm{w}(f) = 2^{n-1} - 2^{n-mk-1}(2^m - 2)^k$ and $w(f+1) = 2^{n-1} + 2^{n-mk-1}(2^m - 2)^k$.*

Proof. Let $f_i = \prod_{j=1}^{m} x_{mi+j}$. Then, by Remark 2, $\mathcal{F}(f) = 2^{n-mk} \prod_{i=0}^{k-1} \mathcal{F}(f_{i\restriction_{\mathbb{F}^m}})$. But $f_{i\restriction_{\mathbb{F}^m}}(x) = 0$, for all $x \in \mathbb{F}^m \setminus \{\mathbf{1}\}$, so $\mathcal{F}(f_{i\restriction_{\mathbb{F}^m}}) = 2^m - 2$. Thus $\mathcal{F}(f) = 2^{n-mk}(2^m - 2)^k$. Hence $\mathrm{w}(f) = 2^{n-1} - \frac{1}{2}\mathcal{F}(f) = 2^{n-1} - \frac{1}{2}[2^{n-mk}(2^m - 2)^k] = 2^{n-1} - 2^{n-mk-1}(2^m - 2)^k$ and $\mathrm{w}(f+1) = 2^n - \mathrm{w}(f) = 2^{n-1} + 2^{n-mk-1}(2^m - 2)^k$.

Remark 3. All quadratic B.f.'s split (see Theorem 4) and are of the form given in Proposition 3 if unbalanced. So, by applying Proposition 3, $\mathrm{w}(f) = 2^{n-1} - 2^{n-k-1}$ and $\mathrm{w}(f+1) = 2^{n-1} + 2^{n-k-1}$ if f is unbalanced quadratic (note that in this case $m = 2$).

Now we study the weight and balancedness of B.f.'s in some particular form. The weight of a B.f. on $\mathbb{F}^n$ can be expressed in terms of the weights of other B.f.'s on $\mathbb{F}^{n-i}$, for some $i < n$.

Any B.f. can be expressed in the form

$$f = x_i g(x_1, ...x_{i-1}, x_{i+1}, ..., x_n) + h(x_1, ...x_{i-1}, x_{i+1}, ..., x_n).$$

To simplify this notation, we can write

$$f = x_1 g(x_2, ..., x_n) + h(x_2, ..., x_n). \tag{1}$$

Observe that $f = x_1 g(x_2, ..., x_n) + h(x_2, ..., x_n) = x_1(g + h) + (1 + x_1)h$. So any B.f. f on $\mathbb{F}^{n+1}$ can be written in the form

$$f \sim_A x_{n+1} g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n). \tag{2}$$

We call this form the *convolutional product* of g and h.

Let $g(x_{m+1}, ..., x_{m+n})$ and $h(x_{m+1}, ..., x_{m+n})$ be B.f.'s on $\mathbb{F}^n$ with $n, m \in \mathbb{N}$. Note that the convolutional product is a special case of functions in B_{m+n} defined by

$$f \sim_A \left(\prod_{j=1}^{m} x_j\right) g(x_{m+1}, ..., x_{m+n}) + \left(1 + \prod_{j=1}^{m} x_j\right) h(x_{m+1}, ..., x_{m+n}). \tag{3}$$

In fact, for any B.f. f, there exists a positive integer m such that f can be expressed in the form (3). We show that if the weight of the functions g and h on $\mathbb{F}^n$ is known, then the weight of a B.f. f on $\mathbb{F}^{m+n}$ which can be expressed in the form (3) is obtained.

Theorem 7. *Let $f \in B_{m+n}$ be a B.f. of the form (3). Then*
(i) $\mathrm{w}(f) = (2^m - 1)\mathrm{w}(h_{\restriction \mathbb{F}^n}) + \mathrm{w}(g_{\restriction \mathbb{F}^n})$,
(ii) f is balanced if both g and h are balanced,
(iii) f is unbalanced if one in $\{g, h\}$ is balanced and the other is not.

Remark 4. If $m = 1$ in Theorem 7 (that is, $f = (x_{n+1})g + (1 + x_{n+1})h$) then we have $\mathrm{w}(f) = \mathrm{w}(h_{\restriction \mathbb{F}^n}) + \mathrm{w}(g_{\restriction \mathbb{F}^n})$.

Finally, we consider the weight of cubic B.f.'s. In general, it is difficult to determine the weight for B.f.'s of degree greater than 2 (see [7]). Here we present a result which completely describes the weight of a special class of cubic functions. This result allows us to construct an algorithm that computes the weight of *any* cubic function.

We now state our classification theorem for the weight of the special class of cubic functions.

Theorem 8. *Let $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$ be a cubic B.f. such that $\deg(g), \deg(h) \leq 2$. Then $g \sim_A q = x_1x_2 + \cdots + x_{2k-1}x_{2k}$ or $g \sim_A \bar{q} = q + 1$, with $k \leq \lfloor \frac{n}{2} \rfloor$, if g is quadratic unbalanced; $h \sim_A r = x_1x_2 + \cdots + x_{2\ell-1}x_{2\ell}$ or $h \sim_A \bar{r} = r + 1$, with $\ell \leq \lfloor \frac{n}{2} \rfloor$, if h is quadratic unbalanced. Moreover,*

$$\mathrm{w}(f) = \begin{cases} 2^n & \text{if both } h \text{ and } g \text{ are balanced} \\ 2^{n-1} & \text{if } h \text{ (resp. } g\text{) is bal. quad. and } g \text{ (resp. } h\text{)} = 0 \\ 2^n + 2^{n-1} & \text{if } h \text{ (resp. } g\text{) is bal. quad. and } g \text{ (resp. } h\text{)} = 1 \\ 2^{n-1} \pm 2^{n-k-1} & \text{if } h \text{ is unbal. quad. and } g = 0 \\ 2^n + 2^{n-1} \pm 2^{n-k-1} & \text{if } h \text{ is unbal. quad. and } g = 1 \\ 2^{n-1} \pm 2^{n-\ell-1} & \text{if } h = 0 \text{ and } g \text{ is unbal. quad.} \\ 2^n + 2^{n-1} \pm 2^{n-\ell-1} & \text{if } h = 1 \text{ and } g \text{ is unbal. quad.} \\ 2^n \pm 2^{n-k-1} & \text{if } h \text{ is unbal. quad. and } g \text{ is bal.} \\ 2^n \pm 2^{n-\ell-1} & \text{if } h \text{ is bal. and } g \text{ is unbal. quad.} \\ 2^n - 2^{n-k-1} - 2^{n-\ell-1} & \text{if } h \sim_A q \text{ and } g \sim_A r \\ 2^n + 2^{n-k-1} + 2^{n-\ell-1} & \text{if } h \sim_A \bar{q} \text{ and } g \sim_A \bar{r} \\ 2^n + 2^{n-k-1} - 2^{n-\ell-1} & \text{if } h \sim_A \bar{q} \text{ and } g \sim_A r \\ 2^n - 2^{n-k-1} + 2^{n-\ell-1} & \text{if } h \sim_A q \text{ and } g \sim_A \bar{r}. \end{cases}$$

With the help of Theorem 8, we can give a description of balanced cubic B.f.'s of the class $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$, with $\deg(g), \deg(h) \leq 2$.

Corollary 2. *Using the same notation from Theorem 8, a cubic B.f. f is balanced if and only if one of the following holds: (i) both g and h are balanced, (ii) $g \sim_A q$ and $h \sim_A \bar{q}$, (iii) $g \sim_A \bar{q}$ and $h \sim_A q$.*

Now we consider cubic B.f.'s which cannot be expressed in the form described in Theorem 8. If a B.f. f is expressed in the form (1), that is, $f = x_1g(x_2, ..., x_n) + h(x_2, ..., x_n)$ then $\mathrm{w}(f) = \mathrm{w}((g + h)_{\restriction \mathbb{F}^{n-1}}) + \mathrm{w}(h_{\restriction \mathbb{F}^{n-1}})$. Since our interest is in cubic functions, it can be assumed that g is quadratic and h can be affine, quadratic or cubic. It becomes difficult to find the weight of f if h is cubic

since in this case it implies that $g+h$ is also cubic and finding $\mathrm{w}(h_{\restriction \mathbb{F}^{n-1}})$ and $\mathrm{w}((g+h)_{\restriction \mathbb{F}^{n-1}})$ is not easy. However, we can recursively repeat the process of decomposing the function f so that its weight is the sum of weights of some affine or quadratic functions on a vector space of dimension $< n$ over $\mathbb{F}$. For instance, further expressing $g+h$ and h in the form $g+h = x_2 g_1(x_3,...,x_n) + h_1(x_3,...,x_n)$ and $h = x_2 g_1'(x_3,...,x_n) + h_1'(x_3,...,x_n)$, the weight of f becomes $\mathrm{w}(f) = \mathrm{w}((g_1+h_1)_{\restriction \mathbb{F}^{n-2}}) + \mathrm{w}(h_{1\restriction \mathbb{F}^{n-2}}) + \mathrm{w}((g_1'+h_1')_{\restriction \mathbb{F}^{n-2}}) + \mathrm{w}(h'_{1\restriction \mathbb{F}^{n-2}})$. We use this idea to build an algorithm which computes the weight of cubic B.f.'s and its efficiency and simplicity relies on the known results about the weights of affine and quadratic functions.

Algorithm 1

The following algorithm computes the weight of any cubic function f on $\mathbb{F}^n$:

Input: f,
Output: $\mathrm{w}(f)$,
Step 1: express f in the form $f = x_1 g(x_2,...,x_n) + h(x_2,...,x_n)$ so that g is quadratic,
Step 2: if $\deg(h) \leq 2$, compute $\mathrm{w}(f)$ by using Theorem 8 and return $\mathrm{w}(f)$,
Step 3: otherwise, recursively compute the weights of $g+h$ and h by applying **Step 1** and **Step 2**,
Step 4: sum up all the weights found to obtain $\mathrm{w}(f)$.

3 Nonlinearity of Boolean functions

In this section, we consider the nonlinearity of B.f.'s. We begin with splitting functions.

Theorem 9 ([9]). *Let f be a quadratic B.f. denoted as in Theorem 4. Then $\mathcal{W}_f(a) \in \{0, \pm 2^{n-k}\}$ for $a \in \mathbb{F}^n$, and $\mathcal{N}(f) = 2^{n-1} - 2^{n-k-1}$.*

Corollary 3 ([10]). *Let $f \in B_n$ be a splitting function. Using the notation of Definition 2,*

$$\begin{aligned}\mathcal{N}(f) &= 2^i \mathcal{N}(h_{\restriction \mathbb{F}^{n-i}}) + 2^{n-i}\mathcal{N}(g_{\restriction \mathbb{F}^i}) - 2\mathcal{N}(g_{\restriction \mathbb{F}^i})\mathcal{N}(h_{\restriction \mathbb{F}^{n-i}}) \\ &= \mathcal{N}(g) + \mathcal{N}(h) - 2^{1-n}\mathcal{N}(g)\mathcal{N}(h).\end{aligned}$$

Now we consider the nonlinearity of a function with terms that depend on different variables and have the same degree. We claim the following.

Proposition 4. *Let $f \in B_n$, $\deg(f) = m$, such that $f \sim_A \sum_{t=0}^{k-1} \prod_{j=1}^{m} x_{mt+j}$ with $m > 1$. Then $\mathcal{N}(f) = \mathcal{N}(f+1) = 2^{n-1} - 2^{n-mk-1}(2^m - 2)^k$.*

Remark 5. In Proposition 4, f is a quadratic bent function if $m = 2$ and $k = n/2$ for n even but it is impossible for f to be bent when $m > 2$. Otherwise, $2^{n-mk-1}2^k(2^{m-1}-1)^k$ would be equal to $2^{\frac{n}{2}-1}$ for some positive integer k, contradicting the fact that $(2^{m-1}-1) \nmid 2^{\frac{n}{2}-1}$ since $(2^{m-1}-1)$ is odd and $2^{\frac{n}{2}-1}$ cannot be divisible by an odd number.

Theorem 10. *Let f be a B.f. of the form (3). Let $a = (a', a'') \in \mathbb{F}^m \times \mathbb{F}^n$ with $a' = (a'_1, ..., a'_m)$ and $a'' = (a''_1, ..., a''_n)$. Then*

(i) $\mathcal{W}_f(a) = \begin{cases} (2^m - 1)\,\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(a'') + \mathcal{W}_{g_{\restriction \mathbb{F}^n}}(a'') & \text{if } a' = 0 \\ (-1)^\lambda \left(\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(a'') - \mathcal{W}_{h_{\restriction \mathbb{F}^n}}(a'')\right) & \text{otherwise,} \end{cases}$
with $\lambda = a'_1 + \cdots + a'_m$,
(ii) $\mathcal{N}(f) \geq (2^m - 1)\mathcal{N}(h_{\restriction \mathbb{F}^n}) + \mathcal{N}(g_{\restriction \mathbb{F}^n})$.

Remark 6. Note that if $m = 1$, the nonlinearity of $f \sim_A x_{n+1}g + (1 + x_{n+1})h$ in Theorem 10 is $\mathcal{N}(f) \geq \mathcal{N}(h_{\restriction \mathbb{F}^n}) + \mathcal{N}(g_{\restriction \mathbb{F}^n})$.

It is immediate from Theorem 9 and Remark 6 that the following corollary holds.

Corollary 4. *Let f be as described in Theorem 8. Then*

$$\mathcal{N}(f) \geq \begin{cases} 2^{n-1} - 2^{n-k-1} & \text{if } g \text{ is quadratic and } h \text{ affine,} \\ 2^{n-1} - 2^{n-\ell-1} & \text{if } g \text{ is affine and } h \text{ quadratic,} \\ 2^n - 2^{n-k-1} - 2^{n-\ell-1} & \text{if both } g \text{ and } h \text{ are quadratic.} \end{cases}$$

Corollary 4 suggests a way of constructing B.f.'s with high non-linearity.

4 A Characterization of APN Functions

Our main results here are Theorem 13, its consequences and Theorem 16.

4.1 APN functions

In this subsection we present some definitions and known results on APN functions which can be found in [1,2,5,6].

Definition 3. *Define $\delta_F(a, b) = |\{x \in \mathbb{F}^n | D_aF(x) = b\}|$, for $a, b \in \mathbb{F}^n$ and v.B.f. F. The* differential uniformity of F is $\delta(F) = \max_{a \neq 0, b \in \mathbb{F}^n} \delta_F(a, b)$ *and always satisfies $\delta(F) \geq 2$. We call a function with $\delta(F) = 2$* Almost Perfectly Nonlinear (APN)*.*

Next we state the result which connects the fourth power moment of Walsh transform and any APN function.

Theorem 11. *Let F be a v.B.f. Then*

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} L_4(\lambda \cdot F) \geq 2^{3n+1}(2^n - 1).$$

Moreover, F is APN if and only if equality holds.

As a consequence of Theorem 11, the following corollary holds.

Corollary 5. *If F is APN then $\exists \lambda \in \mathbb{F}^n \setminus \{0\}$ such that $L_4(\lambda \cdot F) \leq 2^{3n+1}$.*

4.2 The parameter $\mathcal{M}(f)$

In this subsection we define an integer which is denoted by $\mathcal{M}(f)$, for a given B.f. f.

Definition 4. *For $a \in \mathbb{F}^n$ and $f \in B_n$, define $Z_a(f) := \{b \in \mathbb{F}^n | D_b D_a f = 0\}$, $U_a(f) := \{b \in \mathbb{F}^n | D_b D_a f = 1\}$ and $\mathcal{M}_a(f) := |Z_a(f)| - |U_a(f)|$. We define the parameter $\mathcal{M}(f)$ by*

$$\mathcal{M}(f) := \sum_{a \in \mathbb{F}^n \setminus \{0\}} \mathcal{M}_a(f).$$

Proposition 5. *Let $f \in B_n$. Then*

(i) $Z_a(f)$ is a vector space and has nonzero dimension for all $a \in \mathbb{F}^n$,
(ii) $U_a(f)$ is either a coset of $Z_a(f)$ or the empty set,
(iii) $\mathcal{M}_a(f) \in \{0, 2^j\}$ for some $j \in \{1, ..., n\}$.

Proposition 6. *If $g_1, g_2 \in B_n$ are such that $g_1 \sim_A g_2$, then $\mathcal{M}(g_1) = \mathcal{M}(g_2)$.*

Proposition 7. *Let $f \in B_n$ be a B.f. with $\deg(f) \leq 3$ and let $a \in \mathbb{F}^n$. Then $\mathcal{M}_a(f) = 0 \iff D_a f$ is balanced and $\mathcal{M}_a(f) = 2^n \iff D_a f$ is constant.*

Next we state the result which characterizes a quadratic or cubic bent function f by $\mathcal{M}(f)$. By Theorem 2 and Proposition 7, the following theorem holds.

Theorem 12. *For a quadratic or cubic $f \in B_n$, f is bent $\iff \mathcal{M}(f) = 0$.*

4.3 Relationship between $\mathcal{M}(f)$ and APN functions

In this subsection, for a given B.f. f, a relationship between the fourth power moment of the Walsh transform and the value $\mathcal{M}(f)$ is established, and consequently a characterization of APN functions based on the latter quantity is derived.

Lemma 2. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a v.B.f. of $\deg(F) \in \{2, 3\}$. Then*

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} L_4(\lambda \cdot F) = 2^{3n}(2^n - 1) + 2^{2n} \sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} \mathcal{M}(\lambda \cdot F).$$

By Lemma 2 and Theorem 11, the following theorem holds.

Theorem 13. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a v.B.f. with $\deg(F) = 2$ or 3. Then*

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} \mathcal{M}(\lambda \cdot F) \geq 2^n(2^n - 1).$$

Moreover, F is APN if and only if equality holds.

As a consequence of Theorem 13, the following corollary holds.

Corollary 6. *If a v.B.f. $F : \mathbb{F}^n \to \mathbb{F}^n$ is a quadratic or cubic APN then there is a nonzero $\lambda \in \mathbb{F}^n$ such that $\mathcal{M}(\lambda \cdot F) \leq 2^n$.*

We call $V(f) = \{a \in \mathbb{F}^n \mid D_a f \text{ is a constant}\}$ the *linear subspace* of a B.f. f.

Theorem 14. *For any quadratic f, $\mathcal{M}(f) = 2^n(2^k - 1)$ where $k = \dim V(f)$.*

Proof. $\mathcal{M}_a(f) = 0 \iff D_a f$ is balanced and $\mathcal{M}_a(f) = 2^n \iff D_a f$ is a constant (see Proposition 7). For a quadratic function f, $D_a f$ is constant $\iff a \in V(f)$ and $D_a f$ is balanced $\iff a \notin V(f)$. Thus $\mathcal{M}(f) = \sum_{a \in \mathbb{F}^n \setminus \{0\}} \mathcal{M}_a(f) = \sum_{a \in V(f) \setminus \{0\}} \mathcal{M}_a(f) = 2^n(2^k - 1)$, with $k = \dim V(f)$.

Lemma 3. *For n odd, a quadratic B.f. f is semi-bent $\iff \dim V(f) = 1$.*

Proof. Let $f \in B_n$ be quadratic. So f is semi-bent $\iff \mathcal{N}(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$ $\iff f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n$ or $f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1}/ + 1$ (see Theorem 9) $\iff \dim V(f) = 1$.

By Theorem 14 and Lemma 3, the following corollary holds.

Corollary 7. *For n odd, a quadratic B.f. f is semi-bent $\iff \mathcal{M}(f) = 2^n$.*

By Theorem 14, the following corollary holds.

Corollary 8. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a pure quadratic function. Then*

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} \mathcal{M}(\lambda \cdot F) = 2^n \sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} (2^{\dim V(\lambda \cdot F)} - 1). \tag{4}$$

Example 1. Let $F(x_1, x_2, x_3) = (f_1, f_2, f_3)$ where $f_1 = x_1x_3 + x_2x_3 + x_1$, $f_2 = x_2x_3 + x_1 + x_2$ and $f_3 = x_1x_2 + x_1 + x_2 + x_3$ are all in B_3. One can verify that all nontrivial components are quadratic. By Corollary 8, $\sum_{\lambda \in \mathbb{F}^3 \setminus \{0\}} \mathcal{M}(\lambda \cdot F) = 2^3 \cdot (2^3 - 1) = 56$ and so, by Theorem 13, we conclude that F is an APN function. Moreover, all components are balanced, implying that F is an APN permutation.

By applying Lemma 3, Corollary 8 and Theorem 13, we can deduce the only well-known result present in this subsection.

Theorem 15 ([4]). *Let $F : \mathbb{F}^n \to \mathbb{F}^n$, with n odd, be a pure quadratic function. Then F is APN if and only if it is AB.*

4.4 Second-order derivatives of APN functions

In this subsection, the Walsh transform in zero of the second-order derivatives of a function is linked to the fourth power moment, and consequently a natural characterization of APN functions is given based on the former.

Lemma 4. *For a v.B.f. $F : \mathbb{F}^n \to \mathbb{F}^n$,*

$$\sum_{\lambda \in \mathbb{F}^n \setminus \{0\}} L_4(\lambda \cdot F) = 2^{3n}(2^n - 1) + 2^n \sum_{\lambda, c \in \mathbb{F}^n \setminus \{0\}; b \in \mathbb{F}^n} \mathcal{F}(D_b D_c \lambda \cdot F).$$

Theorem 16. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a v.B.f. Then*

$$\sum_{\lambda, c \in \mathbb{F}^n \setminus \{0\}; b \in \mathbb{F}^n} \mathcal{F}(D_b D_c \lambda \cdot F) \geq 2^{2n}(2^n - 1).$$

Moreover, F is APN if and only if equality holds.

Acknowledgements

The results in this paper appear partially in the last author's MSc thesis and mostly in the first author's PhD thesis, both supervised by the second author.

References

1. Berger, T.-P., Canteaut, A., Charpin, P., Laigle-Chapuy. Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inf. Theory **52**(9), 4160-4170 (2006).
2. Beth, T., Ding, C.: On almost perfect nonlinear permutations. In: Advances in Cryptology - EUROCRYPT '93, vol vol 765, pp 65-76. Springer, Berlin, Heidelberg (1993). https://doi.org/10.1007/3-540-48285-7_7
3. Braeken, A., Borissov, Y., Nikova, S., Preneel B.: Classification of cubic $(n-4)$-resilient Boolean functions. IEEE Transactions on Information Theory **52**(4), 1670-1676 (2006).
4. Budaghyan, L., Helleseth, T., Li, N., Sun B.: Some Results on the Known Classes of Quadratic APN Functions. In: El Hajji, S., Nitaj, A., Souidi, E. (eds) Codes, Cryptology and Information Security, C2SI 2017, vol 10194, pp 3-16. Springer, Cham (2017).
5. Calderini, M., Sala, M., Villa I.: A note on APN permutations in even dimension, Finite Fields and Their Applications, **46**, 1-6 (2017).
6. Carlet, C.: Vectorial Boolean Functions for Cryptography. In: Crama, Y., Peter L. Hammer, P.-L. (eds.) Boolean models and methods in mathematics, computer science and engineering., vol 2, pp 398-470 Cambridge Univ. Press, Cambridge (2010).https://doi.org/10.1017/CBO9780511780448
7. Carlet C.: A transformation on boolean functions, its consequences on some problems related to Reed-Muller codes. In: Cohen G., Charpin P. (eds.) Adv. in crypt.-Eurocrypt'90. LNCS, vol 473, pp 42-50. Springer, Berlin, Heidelberg (1991). https://doi.org/10.1007/3-540-54303-1_116
8. Chee, S., Lee, S., Kim K.: Semi-bent Functions. In: Pieprzyk, J., Safavi-Naini, R. (eds.) Advances in Cryptology-ASIACRYPT'94. Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, vol 917, pp 107-118. Springer, Wollongong.(1994).
9. MacWilliams, F.-J., and Sloane, N.-J.-A..: The Theory of Error-Correcting Codes. Elsevier, New York (1977).
10. Wu, C., Feng, D.: Boolean Functions and Their Applications in Cryptography. Springer, New York (2016).