# Characterizations of Plateaued and Bent Functions in Characteristic $p$


Sihem Mesnager[1,2](✉)

[1] Department of Mathematics, University of Paris VIII, Saint-Denis, France
[2] LAGA, UMR 7539, CNRS, University of Paris XIII, Villetaneuse, France
smesnager@univ-paris8.fr



**Abstract.** We characterize bent functions and plateaued functions in terms of moments of their Walsh transforms. We introduce in any characteristic the notion of directional difference and establish a link between the fourth moment and that notion. We show that this link allows to identify bent elements of particular families. Notably, we characterize bent functions of algebraic degree 3.


## 1 Introduction

Binary bent functions are usually called Boolean bent functions. These functions were first introduced by Rothaus in [12]. Bent functions are closely related to other combinatorial and algebraic objects such as Hadamard difference sets, relative difference sets, planar functions and commutative semi-fields. Later, this notion has been generalized to that of $p$-ary bent functions [11]. Several studies on $p$-ary bent functions have been performed (a non exhaustive list is [5,7–10,13]). Most of them concern constructions of bent functions or studies of their properties. Another important family of binary functions is that of plateaued functions [3]. Like the notion of bent function, the notion of plateaued function can be generalized to $p$-ary plateaued functions (see [4] for instance). In this paper, we establish characterizations of bent functions and plateaued functions in terms of sums of powers of the Walsh transform (Theorems 1 and 3). We also introduce the notion of directional difference for $p$-ary functions, generalizing the directional derivative of Boolean functions (Definition 1). We then show that one can establish identities linking sums of fourth-powers of the Walsh transform and directional derivatives of a $p$-ary function (Proposition 1). We then deduce from our characterizations of all bent $p$-ary functions of algebraic degree 3 when $p$ is odd (Theorem 4). We finally establish a link between the bentness of all elements of a family of $p$-ary functions and counting zeros of their directional differences (Theorem 6 and Corollary 2).

## 2 Notation and Preliminaries

Let $p$ be a prime integer, $n \geq 1$ be an integer. We will denote $\mathbb{F}_{p^n}$ the finite field of size $p^n$ and $\mathbb{F}_{p^n}^{\star}$ the set of nonzero elements of $\mathbb{F}_{p^n}$. Let $\xi_p$ be a primitive



K.-U. Schmidt and A. Winterhof (Eds.): SETA 2014, LNCS 8865, pp. 72–82, 2014.
DOI: 10.1007/978-3-319-12325-7_6

$p$th-root of unity and set $\chi_p(a) = \xi_p^a$. Let $f$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The Walsh transform of $f$ at $w \in \mathbb{F}_{p^n}$ is defined as

$$\widehat{\chi_f}(w) = \sum_{x \in \mathbb{F}_{p^n}} \chi_p\Big(f(x) - Tr_p^{p^n}(wx)\Big).$$

Then $f$ is bent if and only if $\left|Waf(w)\right|^2 = p^n$ for every $w \in \mathbb{F}_{p^n}$. It is said to be *regular bent* if there exists $f^\star : \mathbb{F}_{p^n} \to \mathbb{F}_p$ such that $\widehat{\chi_f}(w) = \chi_p(f^\star(w))p^{\frac{n}{2}}$ for all $w \in \mathbb{F}_{p^n}$. The function $f^\star$ is called the *dual function* of $f$ (in characteristic 2, all bent functions are regular bent; when $p$ is odd, regular bent functions can exist only if $p \equiv 1 \mod 4$). A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is said to be *weakly regular bent* if, for all $w \in \mathbb{F}_{p^n}$, we have $\widehat{\chi_f}(w) = \epsilon\chi_p(f^\star(w))p^{\frac{n}{2}}$ for some complex number with $\left|\epsilon\right| = 1$ (in fact $\epsilon$ can only be $\pm 1$ or $\pm i$). For every function $f$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, we have

$$\sum_{w \in \mathbb{F}_{p^n}} \widehat{\chi_f}(w) = p^n \chi_p(f(0)). \tag{1}$$

Set $\left|z\right|^2 = z\bar{z}$ where $\bar{z}$ stands for the conjugate of $z$. Then

$$\sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^2 = p^{2n}. \tag{2}$$

In the sequel, we shall refer to (2) as the *Parseval identity.* If $\left|\widehat{\chi_f}(w)\right| \in \left\{0, p^{\frac{n+s}{2}}\right\}$ for some nonnegative integer $s$ then $f$ is said to be $s$-plateaued. With this definition, bent functions are 0-plateaued functions (in the case where $s = 0$, $\left|\widehat{\chi_f}(w)\right| \in \left\{0, p^{\frac{n}{2}}\right\}$ is equivalent to $\left|\widehat{\chi_f}(w)\right| = p^{\frac{n}{2}}$). The Parseval identity allows to compute the multiplicity of each value of the Walsh transform (when $p = 2$, a more precise statement has been shown in [2]).

**Lemma 1.** *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be $s$-plateaued. Then the absolute value of the Walsh transform $\widehat{\chi_f}$ takes $p^{n-s}$ times the value $p^{\frac{n+s}{2}}$ and $p^n - p^{n-s}$ times the value* 0.

*Proof.* If $N$ denotes the number of $w \in \mathbb{F}_{p^n}$ such that $\left|\widehat{\chi_f}(w)\right| = p^{\frac{n+s}{2}}$, then $\sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^2 = p^{n+s}N$. Now, according to Eq. (2), one must have that $p^{n+s}N = p^{2n}$, that is, $N = p^{n-s}$. The result follows.

A map $F$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ is said to be planar if and only if the function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ induced by the polynomial $F(X + a) - F(x) - F(a)$ is bijective for every $a \in \mathbb{F}_{p^n}^\star$. We finally introduce the directional difference.

**Definition 1.** *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. The directional difference of $f$ at $a \in \mathbb{F}_{p^n}$ is the map $D_a f$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined by*

$$\forall x \in \mathbb{F}_{p^n}, \quad D_a f(x) = f(x + a) - f(x).$$

## 3 New Characterizations of Plateaued Functions

Let $p$ be a positive prime integer. For any nonnegative integer $k$, we set

$$S_k(f) = \sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^{2k} \text{ and } T_k(f) = \frac{S_{k+1}(f)}{S_k(f)}$$

with the convention regarding $k = 0$ that $S_0(f) = p^n$ (in this case, $T_0(f) = \frac{S_1(f)}{S_0(f)} = p^n$). Let us make a preliminary but important remark : for every integer $A$ and every positive integer $k$, it holds

$$\sum_{w \in \mathbb{F}_{p^n}} \left(\left|\widehat{\chi_f}(w)\right|^2 - A\right)^2 \left|\widehat{\chi_f}(w)\right|^{2(k-1)}$$
$$= S_{k+1}(f) - 2AS_k(f) + A^2 S_{k-1}(f). \quad (3)$$

We are now going to deduce from (3) a characterization of plateaued functions in terms of moments of the Walsh transform (in Sect. 4, we shall specialize our characterization to bent functions, see Theorem 3).

**Theorem 1.** *Let $n$ and $k$ be two positive integers. Let $f$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then, the two following assertions are equivalent.*

1. *$f$ is plateaued, that is, there exists a nonnegative integer $s$ such that $f$ is $s$-plateaued.*
2. *$T_{k+1}(f) = T_k(f)$.*

*Proof.*

1. Suppose that $f$ is $s$-plateaued for some nonnegative integer $s$, that is, $\left|\widehat{\chi_f}(w)\right| \in \{0, p^{\frac{n+s}{2}}\}$. Then, by Lemma 1,

$$S_k(f) = \sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^{2k} = p^{n-s} \times p^{k(n+s)} = p^{(k+1)n+(k-1)s}$$
$$S_{k+1}(f) = p^{n-s} \times p^{(k+1)(n+s)} = p^{(k+2)n+ks}$$
$$S_{k+2}(f) = p^{n-s} \times p^{(k+2)(n+s)} = p^{(k+3)n+(k+1)s}.$$

Therefore

$$T_k(f) = \frac{p^{(k+2)n+ks}}{p^{(k+1)n+(k-1)s}} = p^{n+s}$$

and

$$T_{k+1}(f) = \frac{p^{(k+3)n+(k+1)s}}{p^{(k+2)n+ks}} = p^{n+s} = T_k(f).$$

2. Suppose $T_{k+1}(f) = T_k(f)$. According to (3)

$$\sum_{w \in \mathbb{F}_{p^n}} \left(\left|\widehat{\chi_f}(w)\right|^2 - T_k(f)\right)^2 \left|\widehat{\chi_f}(w)\right|^{2k}$$
$$= S_{k+2}(f) - 2T_k(f)S_{k+1}(f) + T_k^2(f)S_k(f)$$
$$= S_{k+1}(f)\left(T_{k+1}(f) - 2T_k(f) + T_k(f)\right) = 0$$

proving that $\left|\widehat{\chi_f}(w)\right| \in \{0, \sqrt{T_k(f)}\}$ for every $w \in \mathbb{F}_{p^n}$. Thus,

$$\sum_{w\in\mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^2 = T_k(f)\#\{w \in \mathbb{F}_{p^n} \mid \left|\widehat{\chi_f}(w)\right| = \sqrt{T_k(f)}\}.$$

Now, the Parseval identity (2) states that

$$\sum_{w\in\mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^2 = p^{2n}.$$

Therefore $T_k(f)$ divides $p^{2n}$ proving that $T_k(f) = p^\rho$ for some positive integer $\rho$. Now, one has $\#\{w \in \mathbb{F}_{p^n} \| \widehat{\chi_f}(w)| = \sqrt{T_k(f)}\} = p^{2n-\rho} \leq p^n$ which implies that $\rho \geq n$, that is, $\rho = n + s$ for some nonnegative integer $s$.

*Remark 1.* Specializing Theorem 1 to the case where $k = 1$, we get that $f$ is plateaued if and only if $T_2(f) = T_1(f)$, that is

$$S_3(f)S_1(f) - S_2^2(f) = p^{2n}S_3(f) - S_2^2(f) = 0.$$

*Remark 2.* In the proof, we have shown more than the sole equivalence between (1) and (2). Indeed, we have shown that if (2) holds then $f$ is $s$-plateaued and $\left|\widehat{\chi_f}(w)\right| \in \{0, \sqrt{T_k(f)}\}$.

In Theorem 1, we have considered the ratio of two consecutive sums $S_k(f)$. In fact, one can get a more general result than Theorem 1. Indeed, for every positive integer $k$ and every nonnegative integer $l$, we have

$$\sum_{w\in\mathbb{F}_{p^n}} \left(\left|\widehat{\chi_f}(w)\right|^{2l} - A\right)^2 \left|\widehat{\chi_f}(w)\right|^{2(k-1)} = S_{k+2l-1}(f) - 2AS_{k+l-1}(f) + A^2S_{k-1}(f). \quad (4)$$

Then, one can make the same kind of proof as that of Theorem 1 but with (4) in place of (3) (the proof being very similar, we omit it).

**Theorem 2.** *Let $n$, $k$ and $l$ be positive integers and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, the two following assertions are equivalent*

1. *$f$ is plateaued, that is, there exists a nonnegative integer $s$ such that $f$ is $s$-plateaued.*
2. $\frac{S_{k+2l}(f)}{S_{k+l}(f)} = \frac{S_{k+l}(f)}{S_k(f)}$.

## 4 The Case of Bent Functions

In this section, we shall specialize our study to bent functions and suppose that $p$ is a positive prime integer. In the whole section, $n$ is a positive integer. In Theorem 1, we have excluded the possibility to for the integer $k$ to be equal to 0 because it does concern both plateaued functions and bent functions. In fact, if we aim to characterize only bent functions, we are going to show that it follows from comparing $T_1(f) = \frac{S_2(f)}{S_1(f)} = \frac{S_2(f)}{p^{2n}}$ to $T_0(f) = \frac{S_1(f)}{S_0(f)} = p^n$.

**Theorem 3.** *Let $n$ be a positive integer. Let $f$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then*

$$S_2(f) = \sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^4 \geq p^{3n}$$

*and $f$ is bent if and only if $S_2(f) = p^{3n}$.*

*Proof.* If we apply (3) with $A = p^n$ at $k = 1$, we get that

$$\sum_{w \in \mathbb{F}_{p^n}} \left(\left|\widehat{\chi_f}(w)\right|^2 - p^n\right)^2 = S_2(f) - 2p^n S_1(f) + p^{2n} S_0(f).$$

Now, $S_0(f) = p^n$ and $S_1(f) = p^{2n}$ (Parseval identity, Eq. 2). Hence

$$\sum_{w \in \mathbb{F}_{p^n}} \left(\left|\widehat{\chi_f}(w)\right|^2 - p^n\right)^2 = S_2(f) - p^{3n}. \tag{5}$$

Since $\left(\left|\widehat{\chi_f}(w)\right|^2 - p^n\right)^2 \geq 0$ for every $w \in \mathbb{F}_{p^n}$, it implies that $S_2(f) \geq p^{3n}$. Now, $f$ is bent if and only if $\left|\widehat{\chi_f}(w)\right|^2 = p^n$ for every $w \in \mathbb{F}_{p^n}$. Therefore, $f$ is bent if and only if the left-hand side of Eq. (5) vanishes, that is, if and only if $S_2(f) = p^{3n}$.

In characteristic 2, identities have been established involving the Walsh transform of a Boolean function and its directional derivatives (see [1,3]). For instance, for every Boolean function $f$, $S_2(f)$ and the second-order derivatives of $f$ have been linked. We now show that one can link $S_2(f)$ and the directional difference defined in Definition 1.

**Proposition 1.** *Let $n$ be a positive integer. Let $f$ be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then*

$$\sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^4 = p^n \sum_{(a,b,x) \in \mathbb{F}_{p^n}^3} \chi_p(D_a D_b f(x)). \tag{6}$$

*Proof.* Since $|z|^4 = z^2 \overline{z}^2$ where $\overline{z}$ stands for the conjugate of $z$ and $\overline{\xi_p} = \xi_p^{-1}$, we have

$$\begin{aligned}
&\sum_{w \in \mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^4 \\
&= \sum_{w \in \mathbb{F}_{p^n}} \sum_{(x_1,x_2,x_3,x_4) \in \mathbb{F}_{p^n}^4} \chi_p\big(f(x_1) - f(x_2) + f(x_3) - f(x_4) \\
&\qquad\qquad - Tr_p^{p^n}(w(x_1 - x_2 + x_3 - x_4))\big).
\end{aligned}$$

Now,

$$\sum_{w \in \mathbb{F}_{p^n}} \chi_p\big(-Tr_p^{p^n}(w(x_1 - x_2 + x_3 - x_4))\big) = \begin{cases} p^n & \text{if } x_1 - x_2 + x_3 - x_4 = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Hence,

$$\sum_{w\in\mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^4 = p^n \sum_{(x_1,x_2,x_3)\in\mathbb{F}_{p^n}^3} \chi_p\big(f(x_1)-f(x_2)+f(x_3)-f(x_1-x_2+x_3)\big).$$

Now note that

$$D_{x_2-x_1}D_{x_3-x_2}f(x_1) = f(x_1)+f(x_3)-f(x_2)-f(x_1+x_3-x_2).$$

Then, since $(x_1,x_2,x_3)\mapsto(x_1,x_2-x_1,x_3-x_2)$ is a permutation of $\mathbb{F}_{p^n}^3$, we get

$$\sum_{w\in\mathbb{F}_{p^n}} \left|\widehat{\chi_f}(w)\right|^4 = p^n \sum_{(a,b,x)\in\mathbb{F}_{p^n}^3} \chi_p\big(D_aD_bf(x)\big).$$

*Remark 3.* In odd characteristic $p$, when $f$ is a quadratic form over $\mathbb{F}_{p^n}$, that is, $f(x)=\phi(x,x)$ for some symmetric bilinear map $\phi$ from $\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, then, $f(x+y)=f(x)+f(y)+2\phi(x,y)$. Let us now compute the directional differences of $f$ at $(a,b)\in\mathbb{F}_{p^n}$ :

$$\begin{aligned} D_bf(x) &= f(x+b)-f(x) = f(b)+2\phi(b,x)\\ D_aD_bf(x) &= 2\phi(b,x+a)-2\phi(b,x) = 2\phi(b,a). \end{aligned}$$

According to Proposition 1, one has

$$\begin{aligned} S_2(f) &= p^n \sum_{(a,b,x)\in\mathbb{F}_{p^n}^3} \chi_p(2\phi(b,a))\\ &= p^{2n}\sum_{b\in\mathbb{F}_{p^n}}\sum_{a\in\mathbb{F}_{p^n}} \chi_p(2\phi(b,a)). \end{aligned}$$

Now, classical results about character sums over finite abelian groups say that

$$\sum_{a\in\mathbb{F}_{p^n}} \chi_p(2\phi(b,a)) = \begin{cases} p^n & \text{if } \phi(b,\bullet)=0\\ 0 & \text{otherwise.}\end{cases}$$

Hence,

$$S_2(f) = p^{3n}\#\mathfrak{rad}(\phi)$$

where $\mathfrak{rad}(\phi)$ stands for the radical of $\phi$ : $\mathfrak{rad}(\phi)=\{b\in\mathbb{F}_{p^n}\mid\phi(b,\bullet)=0\}$. One can then conclude thanks to Theorem 3 that $f$ is bent if and only if $\mathfrak{rad}(\phi)=\{0\}$.

Suppose that $p$ is odd and consider now functions of the form

$$f(x) = Tr_p^{p^n}\left(\sum_{\substack{i,j,k=0\\ i\neq j, j\neq k, k\neq i}}^{n-1} a_{ijk}x^{p^i+p^j+p^k} + \sum_{\substack{i,j=0\\ i\neq j}}^{n-1} b_{ij}x^{p^i+p^j}\right). \tag{7}$$

We are going to characterize bent functions of that form thanks to Theorem 3 and Proposition 1. But before, let us note that we can rewrite the expression of $f$ as follows

$$\begin{aligned} f(x) &= Tr_p^{p^n}\left(\sum_{\substack{i,j,k=0\\ i\neq j, j\neq k, k\neq i}}^{n-1} a_{ijk}x^{p^i+p^j+p^k}\right) + Tr_p^{p^n}\left(\sum_{\substack{i,j=0\\ i\neq j}}^{n-1} b_{ij}x^{p^i+p^j}\right)\\ &= Tr_p^{p^n}\left(\sum_{\substack{i,j,k=0\\ i\neq j, j\neq k, k\neq i}}^{n-1} a_{ijk}^{p^{-i}}x^{1+p^{j-i}+p^{k-i}}\right) + Tr_p^{p^n}\left(\sum_{\substack{i,j=0\\ i\neq j}}^{n-1} b_{ij}x^{p^i+p^j}\right)\\ &= Tr_p^{p^n}\left(x\sum_{\substack{i,j,k=0\\ i\neq j, j\neq k, k\neq i}}^{n-1} a_{ijk}^{p^{-i}}x^{p^{j-i}+p^{k-i}}\right) + Tr_p^{p^n}\left(\sum_{\substack{i,j=0\\ i\neq j}}^{n-1} b_{ij}x^{p^i+p^j}\right). \end{aligned}$$

In the second equality, we have used the fact that $Tr_p^{p^n}$ is invariant under the Frobenius map $x \mapsto x^p$. Set

$$\psi(x,y) = \frac{1}{2}\sum_{\substack{i,j,k=0\\ i\neq j, j\neq k, k\neq i}}^{n-1} a_{ijk}^{p^{-i}}(x^{p^{j-i}}y^{p^{k-i}} + x^{p^{k-i}}y^{p^{j-i}})$$

$$\phi(x,y) = \frac{1}{2}Tr_p^{p^n}\left(\sum_{\substack{i,j=0\\ i\neq j}}^{n-1} b_{ij}(x^{p^i}y^{p^j} + x^{p^j}y^{p^i})\right),$$

Therefore, a function $f$ of the form (7) can be written

$$f(x) = Tr_p^{p^n}(x\psi(x,x)) + \phi(x,x) \qquad (8)$$

where $\psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is a symmetric bilinear map and $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is a symmetric bilinear form. We can now state our characterization.

**Theorem 4.** *Suppose that $p$ is odd. Let $\phi$ be a symmetric bilinear form over $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ and $\psi$ be a symmetric bilinear map from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Define $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ by $f(x) = Tr_p^{p^n}(x\psi(x,x)) + \phi(x,x))$ for $x \in \mathbb{F}_{p^n}$. For $(a,b) \in \mathbb{F}_{p^n}$, set $\ell_{a,b}(x) = Tr_p^{p^n}(\psi(a,b)x + a\psi(b,x) + b\psi(a,x))$. For every $a \in \mathbb{F}_{p^n}$, define the vector space $\mathfrak{K}_a = \{b \in \mathbb{F}_{p^n} \mid \ell_{a,b} = 0\}$. Then $f$ is bent if and only if $\{a \in \mathbb{F}_{p^n}, \phi(a,\bullet)\big|_{\mathfrak{K}_a} = 0\} = \{0\}$.*

*Proof.* According to Theorem 3 and Proposition 1, $f$ is bent if and only if

$$\sum_{(a,b,x)\in\mathbb{F}_{p^n}^3} \chi_p(D_bD_af(x)) = p^{2n}. \qquad (9)$$

Now, for $(a,b)\in\mathbb{F}_{p^n}^2$,

$$\begin{aligned}
D_af(x) &= Tr_p^{p^n}((x+a)\psi(a+x,a+x)-x\psi(x,x))\\
&\quad +\phi(x+a,x+a)-\phi(x,x)\\
&= Tr_p^{p^n}\big(a\psi(x,x)+2x\psi(a,x)+2a\psi(a,x)+x\psi(a,a)+a\psi(a,a)\big)\\
&\quad +2\phi(a,x)+\phi(a,a).\\
D_bD_af(x) &= Tr_p^{p^n}\big(2a\psi(b,x)+a\psi(b,b)+2b\psi(a,x)+2x\psi(a,b)+2b\psi(a,b)\\
&\quad +2a\psi(a,b)+b\psi(a,a)\big)+2\phi(a,b))\\
&= 2\ell_{a,b}(x)+Tr_p^{p^n}(a\psi(b,b)+b\psi(a,a)+2(a+b)\psi(a,b))+2\phi(a,b).
\end{aligned}$$

Note that, $\ell_{a,b}$ is a linear map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$. Furthermore, for any $a\in\mathbb{F}_{p^n}$ and $b\in\mathfrak{K}_a$, one has

$$\begin{aligned}
\ell_{a,b}(a) &= Tr_p^{p^n}(\psi(a,b)a+a\psi(b,a)+b\psi(a,a))=0,\\
\ell_{a,b}(b) &= Tr_p^{p^n}(\psi(a,b)b+a\psi(b,b)+b\psi(a,b))=0
\end{aligned}$$

which implies, summing those two equations, that

$$Tr_p^{p^n}(a\psi(b,b)+b\psi(a,a)+2(a+b)\psi(a,b))=0.$$

Hence,

$$\begin{aligned}
\sum_{(a,b,x)\in\mathbb{F}_{p^n}^3}\chi_p(D_bD_af(x)) &= \sum_{(a,b)\in\mathbb{F}_{p^n}^3}\chi_p(2\phi(a,b))\sum_{x\in\mathbb{F}_{p^n}}\chi_p(2\ell_{a,b}(x))\\
&= p^n\sum_{a\in\mathbb{F}_{p^n}}\sum_{b\in\mathfrak{K}_a}\chi_p(2\phi(a,b)).
\end{aligned}$$

Now, for every $a\in\mathbb{F}_{p^n}$, the map $b\in\mathfrak{K}_a\mapsto\phi(a,b)$ is linear over $\mathfrak{K}_a$. Therefore

$$\sum_{b\in\mathfrak{K}_a}\chi_p(2\phi(a,b))=\begin{cases}\#\mathfrak{K}_a & \text{if } \phi(a,\bullet)\big|_{\mathfrak{K}_a}=0\\ 0 & \text{otherwise}\end{cases}$$

Hence, according to (9), $f$ is bent if and only if

$$\sum_{(a,b,x)\in\mathbb{F}_{p^n}^3}\chi_p(D_aD_bf(x))=p^n\sum_{a\in\mathbb{F}_{p^n},\,\phi(a,\bullet)\big|_{\mathfrak{K}_a}=0}\#\mathfrak{K}_a=p^{2n},$$

that is, if and only if,

$$\sum_{a\in\mathbb{F}_{p^n},\,\phi(a,\bullet)\big|_{\mathfrak{K}_a}=0}\#\mathfrak{K}_a=p^n.$$

Now, if $a=0$, then $\mathfrak{K}_0=\mathbb{F}_{p^n}$ because $\ell_{0,b}=0$ for every $b\in\mathbb{F}_{p^n}$. Therefore, $f$ is bent if and only if

$$\sum_{a\in\mathbb{F}_{p^n}^\star,\,\phi(a,\bullet)\big|_{\mathfrak{K}_a}=0}\#\mathfrak{K}_a=0$$

which is equivalent to $\#\mathfrak{K}_a=0$ for every $a\in\mathbb{F}_{p^n}^\star$ such that $\phi(a,\bullet)\big|_{\mathfrak{K}_a}=0$.

We now turn our attention towards maps from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Let us extend the notion of bentness to those maps as follows.

**Definition 2.** *Let $F$ be a Boolean map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. For every $\lambda \in \mathbb{F}_{p^n}^{\star}$, define $f_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$ as : $f_\lambda(x) = Tr_p^{p^m}(\lambda F(x))$ for every $x \in \mathbb{F}_{p^n}$. Then $F$ is said to be bent if and only if $f_\lambda$ is bent for every $\lambda \in \mathbb{F}_{p^n}^{\star}$.*

Theorem 3 implies

**Theorem 5.** *Let $F$ be a map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then, $F$ is bent if and only if*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^{3n}(p^m - 1). \tag{10}$$

*Proof.* According to Theorem 3, for every $\lambda \in \mathbb{F}_{p^m}^{\star}$, $f_\lambda$ is bent if and only if $S_2(f_\lambda) = p^{3n}$ which gives (10). Conversely, suppose that (10) holds. Theorem 3 states that $S_2(f_\lambda) \geq p^{3n}$ for every $\lambda \in \mathbb{F}_{p^m}^{\star}$. Thus, one has necessarily, for every $\lambda \in \mathbb{F}_{p^n}^{\star}$, $S_2(f_\lambda) = p^{3n}$ implying that $f_\lambda$ is bent for every $\lambda \in \mathbb{F}_{p^n}$, proving that $F$ is bent.

We now show that one can compute the left-hand side of (10) by counting the zeros of the second-order directional differences.

**Proposition 2.** *Let $F$ be a Boolean map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^{n+m}\mathfrak{N}(F) - p^{4n}$$

*where $\mathfrak{N}(F)$ is the number of elements of $\{(a, b, x) \in \mathbb{F}_{p^n}^3 \mid D_aD_bF(x) = 0\}$.*

*Proof.* According to Proposition 1, we have

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^n \sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} \sum_{a,b,x \in \mathbb{F}_{p^n}} \chi_p\big(D_aD_bf_\lambda(x)\big).$$

Next, $D_aD_bf_\lambda = Tr_p^{p^m}(\lambda D_aD_bF)$. Therefore

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} \chi_p\big(Tr_p^{p^m}(\lambda D_aD_bF(x))\big).$$

That is

$$\sum_{\lambda \in \mathbb{F}_{p^m}^{\star}} S_2(f_\lambda) = p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \Big( \sum_{\lambda \in \mathbb{F}_{p^m}} \chi_p\big(Tr_p^{p^m}(\lambda D_aD_bF(x))\big)\Big) - p^{4n}.$$

We finally get the result from

$$\sum_{\lambda \in \mathbb{F}_{p^m}} \chi_p\big(Tr_p^{p^m}(\lambda D_aD_bF(x))\big) = \begin{cases} 0 & \text{if } D_aD_bF(x) \neq 0 \\ p^m & \text{if } D_aD_bF(x) = 0 \end{cases}$$

We then deduce from Theorem 3 a characterization of bentness in terms of zeros of the second-order directional differences.

**Theorem 6.** *Let $F$ be a map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then $F$ is bent if and only if $\mathfrak{N}(F) = p^{3n-m} + p^{2n} - p^{2n-m}$.*

*Proof.* $F$ is bent if and only if all the functions $f_\lambda$, $\lambda \in \mathbb{F}_{p^n}^\star$, are bent. Therefore, according to Proposition 3, if $F$ is bent then

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(f_\lambda) = (p^m - 1)p^{3n}.$$

Now, according to Proposition 2, one has

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(f_\lambda) = p^{n+m}\mathfrak{N}(F) - p^{4n}.$$

We deduce from the two above equalities that

$$\begin{aligned}\mathfrak{N}(F) &= p^{-n-m}(p^{4n} + (p^m - 1)p^{3n}) \\ &= p^{3n-m} + p^{2n} - p^{2n-m}.\end{aligned}$$

Conversely, suppose that $\mathfrak{N}(F) = p^{3n-m} + p^{2n} - p^{2n-m}$. Then

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(f_\lambda) = p^{n+m}\mathfrak{N}(F) - p^{4n} = p^{4n} + p^{3n+m} - p^{3n} - p^{4n} = p^{3n}(p^m - 1).$$

We then conclude by Theorem 5 that $F$ is bent.

Note that when $a = 0$ or $b = 0$, $D_aD_bF$ is trivially equal to 0. We state below a slightly different version of Theorem 6 to exclude those trivial cases to characterize the bentness of $F$.

**Corollary 1.** *Let $F$ be a map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then $F$ is bent if and only if $\mathfrak{N}^\star(F) = p^n(p^n - 1)(p^{n-m} - 1)$ where $\mathfrak{N}^\star(F)$ is the number of elements of $\{(a, b, x) \in \mathbb{F}_{p^n}^\star \times \mathbb{F}_{p^n}^\star \times \mathbb{F}_{p^n} \mid D_aD_bF(x) = 0\}$.*

*Proof.* It follows from Proposition 2 by noting that $\{(a, b, x) \in \mathbb{F}_{p^n}^3 \mid D_aD_bF(x) = 0\}$ contains the set $\{(a, 0, x),\ a, x \in \mathbb{F}_{p^n},\} \cup \{(0, a, x),\ a, x \in \mathbb{F}_{p^n}\}$ whose cardinality equals $p^n(1 + 2(p^n - 1)) = 2p^{2n} - p^n$. Hence, the cardinality of $\mathfrak{N}^\star(F)$ equals $p^{3n-m} + p^{2n} - p^{2n-m} - (2p^{2n} - p^n) = p^{3n-m} - p^{2n-m} + p^n - p^{2n} = p^{2n-m}(p^n - 1) + p^n(1 - p^n) = p^n(p^n - 1)(p^{n-m} - 1)$.

In the particular case of planar functions, Theorem 1 rewrites as follows

**Corollary 2.** *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Then, $F$ is planar if and only if, $D_aD_bF$ does not vanish on $\mathbb{F}_{p^n}$ for every $(a, b) \in \mathbb{F}_{p^n}^\star \times \mathbb{F}_{p^n}^\star$.*

*Proof.* $F$ is planar if and only if $F$ is bent ([6, Lemma 1.1]). Hence, according to Corollary 1, $F$ is planar if and only if $\mathfrak{N}^\star(F) = 0$ proving the result.

## References

1. Canteaut, A., Carlet, C., Charpin, P., Fontaine, C.: Propagation characteristics and correlation-immunity of highly nonlinear boolean functions. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 507–522. Springer, Heidelberg (2000)
2. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**(8), 2004–2019 (2003)
3. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
4. Cesmelioglu, A., Meidl, W.: A construction of bent functions from plateaued functions. Des. Codes Crypt. **66**(1–3), 231–242 (2013)
5. Coulter, R.S., Matthews, R.W.: Planar functions and planes of Lenz-Barlotti class II. Des. Codes Crypt. **10**(2), 167–184 (1997)
6. Helleseth, T., Hollmann, H., Kholosha, A., Wang, Z., Xiang, Q.: Proofs of two conjectures on ternary weakly regular bent functions. IEEE Trans. Inf. Theory **55**(11), 5272–5283 (2009)
7. Helleseth, T., Kholosha, A.: Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory **52**(5), 2018–2032 (2006)
8. Helleseth, T., Kholosha, A.: On the dual of monomial quadratic $p$-ary bent functions. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) SSC 2007. LNCS, vol. 4893, pp. 50–61. Springer, Heidelberg (2007)
9. Hou, X.-D.: $p$-ary and $q$-ary versions of certain results about bent functions and resilient functions. Finite Fields Appl. **10**(4), 566–582 (2004)
10. Hou, X.-D.: On the dual of a Coulter-Matthews bent function. Finite Fields Appl. **14**(2), 505–514 (2008)
11. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Comb. Theory, Ser. A **40**(1), 90–107 (1985)
12. Rothaus, O.S.: On "bent" functions. J. Comb. Theory, Ser. A **20**(3), 300–305 (1976)
13. Tan, Y., Yang, J., Zhang, X.: A recursive construction of p-ary bent functions which are not weakly regular. In: IEEE International Conference on Information Theory and Information Security (ICITIS), pp. 156–159 (2010)