Characterizations of Partially Bent and Plateaued Functions over Finite Fields

Sihem Mesnager[1,2,3], Ferruh Özbudak[4,5], and Ahmet Sınak[2,5,6]

[1] Department of Mathematics, University of Paris VIII, France
[2] LAGA, UMR 7539, CNRS, University of Paris VIII and University of Paris XIII, France
[3] Telecom ParisTech, France
[4] Department of Mathematics, Middle East Technical University, Turkey
[5] Institute of Applied Mathematics, Middle East Technical University, Turkey
[6] Department of Mathematics and Computer Sciences, Necmettin Erbakan University, Turkey
smesnager@univ-paris8.fr,ozbudak@metu.edu.tr,asinak@konya.edu.tr

Abstract. Plateaued and partially bent functions over finite fields have significant applications in cryptography, sequence theory, coding theory, design theory and combinatorics. They have been extensively studied due to their various desirable cryptographic properties. In this paper, we study on characterizations of partially bent and plateaued (vectorial) functions over finite fields, with the aim of clarifying their structure. We first redefine the notion of partially bent functions over any finite field $\mathbb{F}_q$, with q a prime power, and then provide a few characterizations of these functions in terms of their derivatives, Walsh power moments and autocorrelation functions. We next characterize partially bent (vectorial) functions over $\mathbb{F}_p$, with p a prime, by means of their second-order derivatives and Walsh power moments. We finally characterize plateaued functions over $\mathbb{F}_p$ in terms of their second-order derivatives, autocorrelation functions and Walsh power moments.

Keywords: p-ary functions · q-ary functions · partially bent · plateaued · additive character.

1 Introduction

The notion of bent Boolean functions, whose absolute Walsh transform takes only one nonzero value, had been initialized in 1966 and published [28] in 1976 by Rothaus (also indicated by Dillon in his thesis [14] in 1974), since then they have been widely studied by several researchers (see, e.g., [5,8,23]). In 1985, Kumar et al. [18] extended this notion to any residue class ring $\mathbb{Z}_k$ and the so-called *generalized bent functions* have been extensively studied in [1,7,15,19,21]. In 1991, Nyberg [27] introduced the notion of perfect nonlinear functions over $\mathbb{Z}_k$. It is worth mentioning that generalized bent and perfect nonlinear functions over $\mathbb{Z}_k$ are not equivalent for a positive integer k, in general. Nyberg, over $\mathbb{Z}_k$, showed that any perfect nonlinear function is a generalized bent function for any positive integer k, but the converse is true only if k is a prime number. In 1997, Coulter and Matthews [13] redefined bent functions over any finite field $\mathbb{F}_q$ with q a prime power, and discussed some of their properties and permutation behaviors. They showed that bent and perfect nonlinear functions are equivalent over $\mathbb{F}_q$. Additionally, Hou presented in [16] further new results on bent functions over $\mathbb{F}_q$.

Because of unbalancedness of bent functions, as an extension of the class of bent functions, Carlet introduced in [4] the class of *partially bent functions* and studied within these functions the propagation criterion. Partially bent functions are interesting in their own right and workable with respect to their significant cryptographic properties such as the balancedness, high nonlinearity, high correlation immunity and good propagation

criterion. The interest of these functions is further from cryptographic point of view since they involve bent functions. The notion of partially bent functions was extended to $\mathbb{F}_p$, with p any prime, and [12] gives a deeper understanding of p-ary partially bent functions in many contexts. Then, partially bent functions have been studied by several researchers (see, e.g., [2,5,12,23,30]). In this paper we redefine partially bent functions over $\mathbb{F}_q$, with q a prime power.

As an extension of partially bent functions, Zheng and Zhang [31] introduced *plateaued Boolean functions* which are functions whose squared Walsh transform takes two distinct values (one being zero). They have been deeply studied by several researchers (see, e.g., [5,6,10,23]). This notion was extended to $\mathbb{F}_p$, with p any prime, and the *p-ary plateaued functions* have been studied in [9,11,17,22,24]. Recently, this notion has been studied over $\mathbb{F}_q$, with q any prime power [26].

This paper is organized as follows. Section 2 fixes main notations and recalls the necessary background. Section 3 first redefines the notion of partially bent functions over $\mathbb{F}_q$, and next presents several characterizations of these functions in terms of their Walsh power moments, derivatives and autocorrelation functions. We also highlight that q-ary bent and q-ary partially bent functions are q-ary plateaued functions. Section 4 characterizes p-ary partially bent (vectorial) functions by their Walsh power moments and derivatives. In Section 5, we study on characterizations of p-ary plateaued functions by means of their Walsh power moments, derivatives and autocorrelation functions.

2 Preliminaries

For any set E, $\#E$ denotes the size of E and $E^\star = E \setminus \{0\}$. Given the complex number $z \in \mathbb{C}$, where $\mathbb{C}$ is the field of complex numbers, $|z|$ and $\bar{z}$ denote the absolute value and the conjugate of z, respectively. For a prime number p and a positive integer m, the finite field with p^m elements is denoted by $\mathbb{F}_q$, where $q = p^m$. For a positive integer n, the extension field $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ can be regarded as an n-dimensional vector space over $\mathbb{F}_q$, and denoted by $\mathbb{F}_q^n$. Hence, an element $\alpha \in \mathbb{F}_{q^n}$ can be viewed as a vector $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{F}_q^n$ where $\alpha_i \in \mathbb{F}_q$ for $1 \leq i \leq n$.

The *relative trace* of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is defined as $\mathrm{Tr}_q^{q^n}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$ and the *absolute trace* of $\beta \in \mathbb{F}_{p^m}$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}_p^{p^m}(\beta) = \beta + \beta^p + \cdots + \beta^{p^{m-1}}$. The trace function is linear and satisfies the transitivity property in a chain of extension fields, that is,

$$\mathrm{Tr}_p^{q^n}(\alpha) = \mathrm{Tr}_p^q\left(\mathrm{Tr}_q^{q^n}(\alpha)\right)$$

for $\alpha \in \mathbb{F}_{q^n}$ where $q = p^m$. *A primitive p-th root of unity* in $\mathbb{C}$ is denoted by $\xi_p = e^{2\pi i/p}$ where $i = \sqrt{-1}$, and its complex conjugation is its inverse, i.e., $\overline{\xi}_p = \xi_p^{-1}$. The function χ from $\mathbb{F}_q$ to $\mathbb{C}$ defined as

$$\chi(x) = \xi_p^{\mathrm{Tr}_p^q(x)} \tag{1}$$

for $x \in \mathbb{F}_q$ is called *the canonical additive character* of $\mathbb{F}_q$. Notice that for each $y \in \mathbb{F}_q$, the function χ_y defined as $\chi_y(x) = \chi(yx)$ for $x \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$ and every additive character of $\mathbb{F}_q$ is obtained in this way. For each character χ of $\mathbb{F}_q$, there is associated the *conjugate* character $\overline{\chi}$ defined as $\overline{\chi}(x) := \overline{\chi(x)}$ for $x \in \mathbb{F}_q$. The canonical

additive characters χ of $\mathbb{F}_q$ and ψ of $\mathbb{F}_q^n$ are connected by the identity $\chi(\mathrm{Tr}_q^{q^n}(\alpha)) = \psi(\alpha)$ for all $\alpha \in \mathbb{F}_q^n$. The following lemma gives the properties of additive characters of $\mathbb{F}_q$.

Lemma 1. *[20] Let $\chi : \mathbb{F}_q \to \mathbb{C}$ be an additive character as in (1). Then for all $x_1, x_2 \in \mathbb{F}_q$, we have $\chi(x_1 + x_2) = \chi(x_1)\chi(x_2)$ and $\overline{\chi}(x_1) = \chi(-x_1)$.*

Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. We can define a corresponding function χ_f from $\mathbb{F}_q^n$ to $\mathbb{C}$ by

$$\chi_f(x) = \chi(f(x)) = \xi_p^{\mathrm{Tr}_p^q(f(x))}.$$

The *Walsh-(Hadamard) transform* of f at $\omega \in \mathbb{F}_q^n$ is the Fourier transform $\widehat{\chi_f} : \mathbb{F}_q^n \to \mathbb{C}$ of the function χ_f defined by

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_q^n} \chi_f(x)\overline{\chi}(\omega \cdot x), \tag{2}$$

where $\chi : \mathbb{F}_q \to \mathbb{C}$ is any non-trivial additive character of $\mathbb{F}_q$ in (1) and " $\cdot$ " denotes an inner product in $\mathbb{F}_q^n$ over $\mathbb{F}_q$. It is worth noting that (2) can be also given without the conjugate of χ. If $\mathbb{F}_q^n$ is identified with $\mathbb{F}_{q^n}$, we can take $\omega \cdot x = \mathrm{Tr}_q^{q^n}(\omega x)$ for $\omega, x \in \mathbb{F}_q^n$. The Walsh support of f is the set $\{\omega \in \mathbb{F}_{q^n} : \widehat{\chi_f}(\omega) \neq 0\}$, denoted by $\mathrm{Supp}(\widehat{\chi_f})$. We denote $\mathcal{N}_{\widehat{\chi_f}} = \#\mathrm{Supp}(\widehat{\chi_f})$ and as is readily seen $\mathcal{N}_{\widehat{\chi_f}} \leq q^n$. For any nonnegative integer i, even Walsh power moment of f is defined by

$$S_i(f) = \sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^{2i}$$

with the convention $S_0(f) = q^n$. It is a well known fact that $S_1(f) = q^{2n}$, which is called *the Parseval identity*. A function f is k-th order correlation immune ($1 \leq k \leq n$) if

$$\widehat{\chi_f}(\omega) = 0; \qquad 1 \leq \mathrm{wt}(\omega) \leq k,$$

where $\mathrm{wt}(\omega)$ denotes the Hamming weight of $\omega \in \mathbb{F}_q^n$. A function f is said to be *balanced (or, permutation polynomial)* over $\mathbb{F}_q$ if

$$\widehat{\chi_f}(0) = 0,$$

i.e., $\#\{x \in \mathbb{F}_q^n : f(x) = l\} = q^{n-1}$ for each $l \in \mathbb{F}_q$; otherwise, f is called unbalanced. The derivative of f at point $a \in \mathbb{F}_q^n$ is the map $\mathcal{D}_a f$ from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ defined by

$$\mathcal{D}_a f(x) = f(x + a) - f(x)$$

for all $x \in \mathbb{F}_q^n$. The second-order derivative of f at point $(a, b) \in (\mathbb{F}_q^n)^2$ is given as $\mathcal{D}_b\mathcal{D}_a f(x) = f(x + a + b) - f(x + a) - f(x + b) + f(x)$ for all $x \in \mathbb{F}_q^n$. For $(a, b) \in (\mathbb{F}_q^n)^2$, readily $\mathcal{D}_b\mathcal{D}_a f(x) = \mathcal{D}_a\mathcal{D}_b f(x)$ for all $x \in \mathbb{F}_q^n$. The autocorrelation function of f is the map from $\mathbb{F}_q^n$ to $\mathbb{C}$ defined by

$$\Delta_f(a) = \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x))$$

for all $a \in \mathbb{F}_q^n$, where χ is any non-trivial additive character of $\mathbb{F}_q$ in (1). A function f satisfies the propagation criterion $PC(k)$ of degree k $(1 \leq k \leq n)$ if

$$\Delta_f(a) = 0; \qquad 1 \leq \mathrm{wt}(a) \leq k.$$

We denote by $\mathrm{Supp}(\Delta_f)$ the set of elements $a \in \mathbb{F}_q^n$ such that $\mathcal{D}_a f$ is not balanced, i.e.,

$$\mathrm{Supp}(\Delta_f) = \{a \in \mathbb{F}_q^n \ : \ \Delta_f(a) \neq 0\}. \tag{3}$$

Denote by $\mathcal{N}_{\Delta_f}$ the size of $\mathrm{Supp}(\Delta_f)$. The following lemma can be easily proven (see [4], in characteristic 2).

Lemma 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

i.) $\widehat{\overline{\chi_f}}(\omega) = \overline{\widehat{\chi_f}(-\omega)}$ *for all* $\omega \in \mathbb{F}_q^n$.
ii.) $|\widehat{\chi_f}(\omega)|^2 = \widehat{\Delta_f}(\omega)$ *for all* $\omega \in \mathbb{F}_q^n$.
iii.) $|\widehat{\chi_f}(0)|^2 = \sum_{a \in \mathbb{F}_q^n} \Delta_f(a)$.

We end this section with the following definitions for a p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. A function f is said to be a *p-ary bent* if $|\widehat{\chi_f}(\omega)|^2 = p^n$ for every $\omega \in \mathbb{F}_{p^n}$, and f is a *p-ary partially bent* if the derivative $\mathcal{D}_a f$ is either balanced or constant for all $a \in \mathbb{F}_{p^n}$. Moreover, f is said to be a *p-ary s-plateaued* if $|\widehat{\chi_f}(\omega)|^2 \in \{0, p^{n+s}\}$ for every $\omega \in \mathbb{F}_{p^n}$, where s is an integer with $0 \leq s \leq n$. Notice that the symbol " $*$ " denotes usual product over the ring of integers.

3 On the q-ary partially bent functions and their characterizations

This section first redefines the notion of partially bent functions over $\mathbb{F}_q$, where $q = p^m$ for a prime p and a positive integer m, and next characterizes these functions by means of their Walsh power moments, derivatives and autocorrelation functions.

3.1 On the notion of q-ary partially bent functions

The generalized bent and perfect nonlinear functions over $\mathbb{Z}_k$ for a positive integer k were introduced by Kumar et al. [18] and Nyberg [27], respectively. Then, these notions were redefined over $\mathbb{F}_q$ as follows in [13], where $q = p^m$ for a prime p and an integer $m > 1$.

Definition 1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is called a q-ary bent if $|\widehat{\chi_f}(\omega)|^2 = q^n$ for all $\omega \in \mathbb{F}_q^n$, and f is said to be a perfect nonlinear if the derivative $\mathcal{D}_a f$ is balanced for all nonzero $a \in \mathbb{F}_q^n$.*

Proposition 1. *([13, Theorem 2.3]) Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary bent if and only if f is perfect nonlinear.*

The following corollary can be easily derived from Proposition 1.

Corollary 1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, we have $\sum_{a \in \mathbb{F}_q^n} |\Delta_f(a)|^2 \geq q^{2n}$, with equality if and only if f is q-ary bent.*

In [26], the notion of plateaued functions was redefined over $\mathbb{F}_q$ as follows.

Definition 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and s be an integer with $0 \leq s \leq n$. Then, f is called a q-ary s-plateaued if $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$.*

The Walsh distribution of a q-ary plateaued function is given as follows.

Lemma 3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be an s-plateaued function. Then for $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^2$ takes q^{n-s} times the value q^{n+s} and $q^n - q^{n-s}$ times the value 0.*

The notion of linear translators for q-ary functions is given as follows.

Definition 3. *[23] Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. A nonzero element $\alpha \in \mathbb{F}_q^n$ is called a b-linear translator for a function f if the equation $f(x + u\alpha) - f(x) = ub$ holds for all $x \in \mathbb{F}_q^n$, $u \in \mathbb{F}_q$ and a fixed $b \in \mathbb{F}_q$.*

The linear translators of q-ary functions have the following properties.

Lemma 4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and let $\mathcal{L}_f$ be the set of linear translators of f. Let $\alpha \in \mathcal{L}_f$. Then we have the following.*

i.) $f(x + u\alpha) = f(x) + f(u\alpha) - f(0)$ *for all* $x \in \mathbb{F}_q^n$ *and* $u \in \mathbb{F}_q$.
ii.) $\mathcal{L}_f$ *is a linear subspace of* $\mathbb{F}_q^n$ *and it is called a linear space of* f.
iii.) $l(x) := f(x) - f(0)$ *is a linear function on* $\mathcal{L}_f$.

We are now going to redefine the notion of partially bent functions over $\mathbb{F}_q$. To do this, we first give a bound stating the trade-off between the number of nonzero values of the autocorrelation function and of the Walsh transform of q-ary functions. In the original paper of the notion of partially bent functions [4], Carlet, in characteristic 2, proved that this bound holds for every Boolean function and partially bent Boolean functions are defined to be these functions which the equality holds (for the p-ary case, see [12]).

Proposition 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$q^n \leq \mathcal{N}_{\Delta_f} * \mathcal{N}_{\widehat{\chi_f}}, \tag{4}$$

with equality if and only if the derivative $D_a f$ is either balanced or constant for all $a \in \mathbb{F}_q^n$.

Proof. We have $|\widehat{\chi_f}(0)|^2 = \sum_{a \in \mathbb{F}_q^n} \Delta_f(a)$ by Lemma 2 (*iii*). Then by (3) we have $|\widehat{\chi_f}(0)|^2 \leq q^n \mathcal{N}_{\Delta_f}$. Notice that $\mathcal{N}_{\Delta_f}$ is invariant if $f(x)$ is replaced with $f(x) - \omega \cdot x$ for all $\omega \in \mathbb{F}_q^n$, and so we have $|\widehat{\chi_f}(\omega)|^2 \leq q^n \mathcal{N}_{\Delta_f}$ for all $\omega \in \mathbb{F}_q^n$. Hence, from the Parseval identity we have

$$q^{2n} \leq \max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2) * \mathcal{N}_{\widehat{\chi_f}} \leq q^n \mathcal{N}_{\Delta_f} * \mathcal{N}_{\widehat{\chi_f}}. \tag{5}$$

For the equality case, assume that the equality in (4) holds. By (5), we have that $\max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2) * \mathcal{N}_{\widehat{\chi_f}} = q^{2n}$. By the Parseval identity, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ we have $|\widehat{\chi_f}(\omega)|^2 = \max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2)$, that is, there exits an integer s such that $|\widehat{\chi_f}(\omega)|^2 = q^{n+s}$, i.e., f is s-plateaued. For all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, by Lemma 2 (*ii*),

$$|\widehat{\chi_f}(\omega)|^2 = \sum_{a \in \mathrm{Supp}(\Delta_f)} \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x) - \omega \cdot a),$$

where we used that $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_q^n \setminus \mathrm{Supp}(\Delta_f)$. By Lemma 3, we have $\mathcal{N}_{\widehat{\chi_f}} = q^{n-s}$ and hence by (4), we get $\mathcal{N}_{\Delta_f} = q^s$. Then for all $a \in \mathrm{Supp}(\Delta_f)$, we have

$$\sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x) - \omega \cdot a) = q^n$$

for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, that is, $\mathcal{D}_a f$ is constant (since $\mathcal{D}_a f(x) = \omega \cdot a$ for all $x \in \mathbb{F}_q^n$).

Conversely, assume that $D_a f$ is either balanced or constant for all $a \in \mathbb{F}_q^n$. Then $\mathrm{Supp}(\Delta_f) = \mathcal{L}_f$ and there exists an integer s such that $\mathcal{N}_{\Delta_f} = q^s$. Our next aim is to find $\mathcal{N}_{\widehat{\chi_f}}$. For all $\omega \in \mathbb{F}_q^n$, by Lemma 2 (ii) we have

$$|\widehat{\chi_f}(\omega)|^2 = \sum_{a \in \mathcal{L}_f} \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x)) \overline{\chi}(\omega \cdot a).$$

By Lemma 4, if $a \in \mathcal{L}_f$, then $f(x+a) - f(x) = f(a) - f(0)$ for all $x \in \mathbb{F}_q^n$. Then for all $\omega \in \mathbb{F}_q^n$ we have

$$|\widehat{\chi_f}(\omega)|^2 = q^n \sum_{a \in \mathcal{L}_f} \chi(f(a) - f(0) - \omega \cdot a) = \begin{cases} q^{n+s}, & \text{if } f(a) - \omega \cdot a = f(0) \text{ on } \mathcal{L}_f, \\ 0, & \text{otherwise,} \end{cases}$$

where in the last equality we used that $f(a) - f(0) - \omega \cdot a$ is linear on $\mathcal{L}_f$. Then by the Parseval identity, we have $\mathcal{N}_{\widehat{\chi_f}} = q^{n-s}$. Hence, the equality in (4) holds. □

Definition 4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is called a q-ary partially bent if the derivative $\mathcal{D}_a f$ is either balanced or constant for all $a \in \mathbb{F}_q^n$.*

The definition of q-ary partially bent functions can be slightly revisited as follows.

Remark 1. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function with linear space $\mathcal{L}_f$ such that $\dim(\mathcal{L}_f) = s$ where s is an integer with $0 \leq s \leq n$. Then, f is said to be a q-ary s-partially bent if the derivative $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_q^n \setminus \mathcal{L}_f$. Clearly, $\mathcal{D}_a f$ is constant for all $a \in \mathcal{L}_f$.

The absolute Walsh transform of q-ary partially bent functions takes only one nonzero value (also possibly the value 0).

Proposition 3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. If f is q-ary s-partially bent, then $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$.*

In view of Proposition 3, the Walsh distribution of q-ary partially bent functions follows from the Parseval identity.

Lemma 5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be an s-partially bent function. Then for $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^2$ takes q^{n-s} times the value q^{n+s} and $q^n - q^{n-s}$ times the value 0.*

Remark 2. Any q-ary bent f is a q-ary partially bent function with $\mathcal{L}_f = \{0\}$ by Proposition 1. Over $\mathbb{F}_q$, any perfect nonlinear function is a partially bent function.

In the light of the above results, we can give the following natural consequence for q-ary functions.

Proposition 4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, f is q-ary s-partially bent if and only if f is q-ary s-plateaued. In particular, f is q-ary bent if and only if f is q-ary 0-plateaued.*

Remark 3. The set of q-ary bent functions is a proper subset of the set of q-ary partially bent functions. Similarly, the set of q-ary partially bent functions is a proper subset of the set of q-ary plateaued functions. Namely, a q-ary s-plateaued with $\dim(\mathcal{L}_f) < s$ is not a q-ary partially bent.

Remark 4. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is affine if and only if $\mathcal{N}_{\widehat{\chi_f}} = 1$ and f is q-ary bent if and only if $\mathcal{N}_{\Delta_f} = 1$, i.e., $\max_{a \in \mathbb{F}_{q^n}^*}(|\Delta_f(a)|) = 0$. Moreover, f is q-ary partially bent if and only if $|\Delta_f(a)| \in \{0, q^n\}$ for all $a \in \mathbb{F}_q^n$.

3.2 Characterizations of q-ary partially bent functions

In this subsection, we obtain several characterizations of q-ary partially bent functions by means of their Walsh power moments, derivatives and autocorrelation functions.

A link between the autocorrelation function and the second-order derivative of a q-ary function is given as follows (see [5], in characteristic 2).

Proposition 5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$\sum_{a \in \mathbb{F}_q^n} |\Delta_f(a)|^2 = \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)). \tag{6}$$

Proof. Since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, the left hand side of (6) is given as

$$\sum_{a \in \mathbb{F}_q^n} \sum_{b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(b)) \sum_{x \in \mathbb{F}_q^n} \overline{\chi}(\mathcal{D}_a f(x)) = \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(b) - \mathcal{D}_a f(x)) = \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)),$$

where in the last equality we used the bijective change of variable: $b \mapsto b + x$. □

The identity involving the fourth Walsh power moment and the second-order derivative of a q-ary function is constituted as follows (see [5] for binary case and [22] for p-ary case).

Proposition 6. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$S_2(f) = q^n \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)). \tag{7}$$

Proof. Since $|z|^4 = z^2\overline{z}^2$ for $z \in \mathbb{C}$, we have

$$\begin{aligned} \sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^4 &= \sum_{x,a,b,c \in \mathbb{F}_q^n} \chi(f(x) - f(a) + f(b) - f(c)) \sum_{\omega \in \mathbb{F}_q^n} \overline{\chi}(\omega \cdot (x - a + b - c)) \\ &= q^n \sum_{a,b,x \in \mathbb{F}_q^n} \chi(f(x) - f(a) + f(b) - f(x - a + b)) \end{aligned}$$

since $\sum_{\omega \in \mathbb{F}_q^n} \xi_p^{\mathrm{Tr}_p^{q^n}(-\omega(x-a+b-c))} = \begin{cases} q^n \text{ if } c = x - a + b, \\ 0 \text{ otherwise.} \end{cases}$

Hence, since $(a, b, x) \mapsto (x + a, x + a + b, x)$ is the permutation of $(\mathbb{F}_q^n)^3$, then (7) holds. □

The following link follows readily from Propositions 5 and 6.

Proposition 7. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then we have $S_2(f) = q^n \sum_{a\in\mathbb{F}_q^n} |\Delta_f(a)|^2$.*

The following characterization of partially bent functions by means of their autocorrelation functions can be given (see [5], in characteristic 2).

Proposition 8. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then*

$$\sum_{a\in\mathbb{F}_q^n} |\Delta_f(a)|^2 \geq q^{2n+s},$$

with equality if and only if f is q-ary s-partially bent.

Proof. Due to the fact that $\mathcal{D}_a f$ is constant for all $a \in \mathcal{L}_f$, we have $\sum_{a\in\mathcal{L}_f} |\Delta_f(a)|^2 = q^{2n+s}$. Moreover, we have

$$\sum_{a\notin\mathcal{L}_f} |\Delta_f(a)|^2 \geq 0,$$

with equality if and only if $\Delta_f(a)$ is zero (i.e., $\mathcal{D}_a f$ is balanced) for all $a \notin \mathcal{L}_f$. Hence, the proof is complete. □

The following can be directly derived from Propositions 5 and 8.

Corollary 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then we have*

$$\sum_{a,b,x\in\mathbb{F}_q^n} \chi(\mathcal{D}_a\mathcal{D}_b f(x)) \geq q^{2n+s},$$

with equality if and only if f is q-ary s-partially bent.

We derive directly from Propositions 7 and 8 a characterization of partially bent functions in terms of their fourth Walsh power moment.

Theorem 1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then*

$$S_2(f) \geq q^{3n+s},$$

with equality if and only if f is q-ary s-partially bent.

The sequence of even Walsh power moments of a q-ary partially bent is a simple geometric sequence.

Corollary 3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a q-ary s-partially bent. Then for every positive integer i, we have $S_i(f) = q^{n(i+1)+s(i-1)}$ and for every integer $j \geq 2$,*

$$S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f).$$

Proof. By Lemma 5, we have $S_i(f) = q^{n-s}(q^{n+s})^i = q^{n(i+1)+s(i-1)}$ for every positive integer i. The second assertion follows readily from the first assertion. □

We recall the strong properties of the Fourier transform of complex valued functions. For $G : \mathbb{F}_q^n \to \mathbb{C}$, let $\widehat{G} : \mathbb{F}_q^n \to \mathbb{C}$ be its Fourier transform. Then we have $\widehat{\widehat{G}}(u) = q^n G(-u)$

for all $u \in \mathbb{F}_q^n$. As is readily seen, $G(u) = 0$ for all $u \in \mathbb{F}_q^n$ if and only if $\widehat{G}(v) = 0$ for all $v \in \mathbb{F}_q^n$. Hence for two functions $G_1, G_2 : \mathbb{F}_q^n \to \mathbb{C}$,

$$G_1(u) = G_2(u),\ \forall u \in \mathbb{F}_q^n \Longleftrightarrow \widehat{G_1}(v) = \widehat{G}_2(v),\ \forall v \in \mathbb{F}_q^n. \tag{8}$$

We now give a powerful characterization of q-ary partially bent functions by means of their second-order derivatives (see [10] and [24] for bent Boolean functions and p-ary plateaued functions, respectively). Since the argument of the proof is similar to that of p-ary case, we only give a sketch.

Theorem 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Set*

$$\theta_f(x) = \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x))$$

for $x \in \mathbb{F}_{p^n}$. Then, f is q-ary s-partially bent if and only if $\theta_f(x) = q^{n+s}$ for all $x \in \mathbb{F}_q^n$. In particular, f is q-ary bent if and only if $\theta_f(x) = q^n$ for all $x \in \mathbb{F}_q^n$.

Proof. Put $\theta = q^{n+s}$. For a function f, $\theta_f(x) = \theta$ for all $x \in \mathbb{F}_q^n$ if and only if for all $x \in \mathbb{F}_q^n$

$$\sum_{a,b \in \mathbb{F}_q^n} \chi(f(a+b-x) - f(a) - f(b)) = \theta \chi(-f(x)) \tag{9}$$

(by the bijective change of variables: $a \mapsto a - x$ and $b \mapsto b - x$). We can easily see that the Fourier transforms of the left-hand side of (9) at $\omega \in \mathbb{F}_q^n$ is given by $\widehat{\chi_f}(\omega)\ \widehat{\chi_f}(\omega)\widehat{\chi_f}(-\omega)$ and of its right-hand side by $\theta\widehat{\chi_f}(\omega)$. By Lemma 2 (i), we have $\widehat{\chi_f}(\omega) = \overline{\widehat{\chi_f}(-\omega)}$. By (8), for all $x \in \mathbb{F}_q^n$, (9) holds if and only if for all $\omega \in \mathbb{F}_q^n$,

$$\overline{\widehat{\chi_f}(\omega)}\ \overline{\widehat{\chi_f}(\omega)}\widehat{\chi_f}(\omega) = \theta\overline{\widehat{\chi_f}(\omega)};$$

equivalently, $|\widehat{\chi_f}(\omega)|^2 \in \{0, \theta\}$ for all $\omega \in \mathbb{F}_q^n$ where $\theta = q^{n+s}$, that is, f is q-ary s-partially bent. In particular, for $s = 0$, $\theta_f(x) = q^n$ for all $x \in \mathbb{F}_q^n$ if and only if $|\widehat{\chi_f}(\omega)|^2 = q^n$ for all $\omega \in \mathbb{F}_q^n$ by the Parseval identity, i.e., f is q-ary bent. □

Notice that Theorem 2 says that any q-ary quadratic function is a q-ary partially bent function since the second-order derivative of a quadratic function is constant. We also deduce the following proposition by using the linear translators of a q-ary function f.

Proposition 9. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then for all $x \in \mathbb{F}_q^n$, $\sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)) \geq q^{n+s}$, with equality if and only if f is q-ary s-partially bent.*

Proposition 10. *[26] Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then for all $x \in \mathbb{F}_q^n$,*

$$\sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)}\ |\widehat{\chi_f}(\omega)|^2 = q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)).$$

The following corollary follows directly from Propositions 9 and 10.

Corollary 4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then we have for all $x \in \mathbb{F}_q^n$,*

$$\sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 \geq q^{2n+s},$$

with equality if and only if f is q-ary s-partially bent.

In the following sections, we assume that $m = 1$ (i.e., $q = p$), namely, f is a p-ary function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ where p is a prime.

4 Characterizations of p-ary partially bent (vectorial) functions

This section characterizes p-ary partially bent (vectorial) functions in terms of their Walsh power moments and second-order derivatives.

4.1 Characterizations of p-ary partially bent functions

In this subsection, we obtain some characterizations of p-ary partially bent functions by their fourth Walsh power moment and the value distribution of their second-order derivatives.

For a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, a corresponding function $f_\lambda := \lambda f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as $x \mapsto \lambda f(x)$ for every $\lambda \in \mathbb{F}_p^\star$. Then for any $\lambda \in \mathbb{F}_p^\star$, we have $\mathcal{D}_b\mathcal{D}_a\lambda f(x) = \lambda(\mathcal{D}_b\mathcal{D}_a f(x))$ at $(a, b) \in \mathbb{F}_{p^n}^2$ for every $x \in \mathbb{F}_{p^n}$. We denote by $\mathfrak{N}(f)$ the size of the set $K = \{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a f(x) = 0\}$.

Proposition 11. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then we have $\sum_{\lambda \in \mathbb{F}_p^\star} S_2(\lambda f) = p^{n+1}\mathfrak{N}(f) - p^{4n}$.*

Proof. By Proposition 6, we have

$$\begin{aligned}
\sum_{\lambda \in \mathbb{F}_p^\star} S_2(\lambda f) &= \sum_{\lambda \in \mathbb{F}_p^\star} \Big(p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a \lambda f(x)} \Big) \\
&= p^n \Big(\sum_{\lambda \in \mathbb{F}_p^\star} \sum_{(a,b,x) \in K} \xi_p^{\lambda \mathcal{D}_b\mathcal{D}_a f(x)} + \sum_{(a,b,x) \notin K} \sum_{\lambda \in \mathbb{F}_p^\star} \xi_p^{\lambda \mathcal{D}_b\mathcal{D}_a f(x)} \Big) \\
&= p^n \Big((p-1)\mathfrak{N}(f) - (p^{3n} - \mathfrak{N}(f)) \Big) = p^{n+1}\mathfrak{N}(f) - p^{4n},
\end{aligned}$$

where in the third equality we used that $1 + \xi_p + \xi_p^2 + \cdots + \xi_p^{p-1} = 0$. □

From Theorem 1 and Proposition 11, we derive a characterization of partially bent functions in terms of the zeros of their second-order derivatives.

Corollary 5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, f is p-ary s-partially bent if and only if $\mathfrak{N}(f) = p^{3n-1} + p^{2n+s} - p^{2n+s-1}$.*

Proof. Clearly, f is p-ary s-partially bent if and only if f_λ is p-ary s-partially bent for every $\lambda \in \mathbb{F}_p^\star$. Then by Theorem 1, f is p-ary s-partially bent if and only if

$$\sum_{\lambda \in \mathbb{F}_p^\star} S_2(f_\lambda) = (p-1)p^{3n+s};$$

equivalently, by Proposition 11, we have $\mathfrak{N}(f) = p^{3n-1} + p^{2n+s} - p^{2n+s-1}$. □

A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ with linear space $\mathcal{L}_f$ is p-ary partially bent if and only if the derivative $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_{p^n} \setminus \mathcal{L}_f$. It would be interesting to prove directly the following theorem without using partially bent-ness of f. To do this, we need the following well-known lemma (see [24] for vectorial case).

Lemma 6. *Let $h : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then $p^{2n-1} \leq \#\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : h(x_1) = h(x_2)\}$, with equality if and only if h is balanced.*

Theorem 3. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_{p^n} \setminus \mathcal{L}_f$ if and only if $\mathfrak{N}(f) = p^{3n-1} + p^{2n+s} - p^{2n+s-1}$.*

Proof. Clearly, for all $(a, b, x) \in \mathbb{F}_{p^n}^3$, $\mathcal{D}_b\mathcal{D}_a f(x) = 0$ if and only if

$$\mathcal{D}_a f(x) = \mathcal{D}_a f(x + b). \tag{10}$$

For all $a \in \mathcal{L}_f$, since the derivative $\mathcal{D}_a f$ is constant, we have

$$\#\{(a, b, x) \in \mathbb{F}_{p^n}^3 : a \in \mathcal{L}_f \text{ and } \mathcal{D}_b\mathcal{D}_a f(x) = 0\} = p^s p^n p^n = p^{2n+s}. \tag{11}$$

For all $a \in \mathbb{F}_{p^n} \setminus \mathcal{L}_f$, by Lemma 6, $\mathcal{D}_a f$ is balanced if and only if the number of pairs $(b, x) \in \mathbb{F}_{p^n}^2$ satisfying (10) is equal to p^{2n-1}; equivalently,

$$\#\{(a, b, x) \in \mathbb{F}_{p^n}^3 : a \notin \mathcal{L}_f \text{ and } \mathcal{D}_b\mathcal{D}_a f(x) = 0\} = (p^n - p^s)p^{2n-1}. \tag{12}$$

Hence, combining (11) and (12) concludes the result. □

4.2 Characterizations of p-ary vectorial s-partially bent functions

We first give the notion of vectorial p-ary s-partially bent functions and next provide their characterizations.

Definition 5. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a vectorial function. For every $\lambda \in \mathbb{F}_{p^m}^\star$, let $F_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$, defined by $F_\lambda(x) = \mathrm{Tr}_p^{p^m}(\lambda F(x))$, be its component function with linear space $\mathcal{L}_{F_\lambda}$.*

- *Then F is called a vectorial p-ary partially bent if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary partially bent.*
- *Assume that there exits an integer s with $0 \leq s \leq n$ such that $\dim(\mathcal{L}_{F_\lambda}) = s$ for every $\lambda \in \mathbb{F}_{p^m}^\star$. Then, F is called a vectorial p-ary s-partially bent if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary s-partially bent.*

Remark 5. The notion of vectorial partially bent functions coincides the notion of strongly-plateaued functions introduced in [6]. More precisely, all derivatives of a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ are either constant or balanced if and only if for all $a \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_p$, the size of the set $\{b \in \mathbb{F}_{p^n} : \mathcal{D}_a f(b) = \mathcal{D}_a f(x) + v\}$ is independent of $x \in \mathbb{F}_{p^n}$.

We can derive directly from Theorem 1 the following characterization of vectorial partially bent functions.

Theorem 4. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and for every $\lambda \in \mathbb{F}_{p^m}^\star$, let $F_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be its component function with linear space $\mathcal{L}_{F_\lambda}$ such that $\dim(\mathcal{L}_{F_\lambda}) = s$. Then F is vectorial p-ary s-partially bent if and only if*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(F_\lambda) = (p^m - 1)p^{3n+s} \tag{13}$$

Proof. Assume that F_λ is p-ary s-partially bent for every $\lambda \in \mathbb{F}_{p^m}^\star$. Then by Theorem 1, the assertion holds. Conversely, assume that (13) holds. By Theorem 1, for every $\lambda \in \mathbb{F}_{p^m}^\star$, we have

$$S_2(F_\lambda) \geq p^{3n+s},$$

with equality because of (13), which implies that F_λ is p-ary s-partially bent. This completes the proof. □

In [22], Mesnager showed that the left-hand side of (13) can be computed by counting the zeros of the second-order derivatives. We denote by $\mathfrak{N}(F)$ the size of the set $\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a F(x) = 0\}$.

Proposition 12. *[22] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and for every $\lambda \in \mathbb{F}_{p^m}^\star$, let $F_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be its component function. Then*

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

We then deduce a characterization of vectorial partially bent functions by means of zeros of their second-order derivatives.

Theorem 5. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and for every $\lambda \in \mathbb{F}_{p^m}^\star$, let $F_\lambda : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be its component function with linear space $\mathcal{L}_{F_\lambda}$ such that $\dim(\mathcal{L}_{F_\lambda}) = s$. Then F is vectorial p-ary s-partially bent if and only if $\mathfrak{N}(F) = p^{2n+s} + p^{3n-m} - p^{2n+s-m}$.*

Proof. By Theorem 4 and Proposition 12, F is s-partially bent if and only if $p^{3n+s}(p^m - 1) = p^{n+m}\mathfrak{N}(F) - p^{4n}$. Hence, the proof is complete. □

The following characterization of plateaued functions was given in [25].

Proposition 13. *[25, Theorem 7] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. For $v \in \mathbb{F}_{p^m}$, let $\mathcal{N}_F(v; x) = \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_b\mathcal{D}_a F(x) = v\}$ for $x \in \mathbb{F}_{p^n}$. Then there exists an integer s with $0 \leq s \leq n$ such that F is vectorial p-ary s-plateaued if and only if $\mathcal{N}_F(v; x)$ does not depend on $x \in \mathbb{F}_{p^n}$, nor on $v \in \mathbb{F}_{p^m}^\star$.*

We then deduce directly from Theorem 5 and Proposition 13 the following.

Corollary 6. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then F is vectorial p-ary s-partially bent if and only if $\#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_b\mathcal{D}_a F(x) = 0\} = p^{n+s} + p^{2n-m} - p^{n+s-m}$ for every $x \in \mathbb{F}_{p^n}$.*

5 Characterizations of p-ary plateaued functions

In this section, we characterize p-ary plateaued functions in terms of their Walsh power moments, autocorrelation functions and the value distribution of their derivatives.

We first recall the following well-known inequality.

Theorem 6 (Hölder's Inequality). *[29] Let $p_1, p_2 \in (1, \infty)$ with $\frac{1}{p_1} + \frac{1}{p_2} = 1$. Then, for all vectors $(x_1, x_2, \ldots, x_m), (y_1, y_2, \ldots, y_m) \in \mathbb{R}^m$ or $\mathbb{C}^m$, Hölder's Inequality states that*

$$\sum_{k=1}^{m} |x_k y_k| \leq \left(\sum_{k=1}^{m} |x_k|^{p_1} \right)^{\frac{1}{p_1}} \left(\sum_{k=1}^{m} |y_k|^{p_2} \right)^{\frac{1}{p_2}}.$$

The above inequality becomes equality if and only if for every $k \in \{1, \ldots, m\}$, $|x_k|^{p_1} = d|y_k|^{p_2}$ for some $d \in \mathbb{R}^+$. In particular, if $p_1 = p_2 = 2$, then this is called the Cauchy-Schwarz Inequality.

We are now going to deduce from Hölder's Inequality the following characterizations of plateaued functions in terms of even power moments of their Walsh transform.

Applying the Cauchy-Schwarz Inequality, for $x_k = |\widehat{\chi_f}(\omega)|^2$ and $y_k = |\widehat{\chi_f}(\omega)|^{2i}$ for all $\omega \in \mathbb{F}_{p^n}$, $1 \leq k \leq p^n$, we have

$$\left(\sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i+2} \right)^2 \leq \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^4 \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{4i},$$

that is, $S_{i+1}(f)^2 \leq S_2(f) S_{2i}(f)$, where the equality holds for one (and hence for all) $i \geq 1$ if and only if for all $\omega \in \mathbb{F}_{p^n}$, we have $|\widehat{\chi_f}(\omega)|^2 = d\,|\widehat{\chi_f}(\omega)|^{2i}$ for some $d \in \mathbb{R}^+$; equivalently, $|\widehat{\chi_f}(\omega)|^2$ is either the same positive integer or 0, that is, f is p-ary plateaued. This proves the following.

Theorem 7. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for every positive integer i, we have*

$$S_{i+1}(f)^2 \leq S_2(f) S_{2i}(f),$$

with equality for one (and hence for all) $i \geq 1$ if and only if f is p-ary plateaued.

Theorem 8. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for every integer $i \geq 2$, we have*

$$p^{2ni} \leq S_i(f) * \mathcal{N}_{\widehat{\chi_f}}^{(i-1)},$$

where the equality holds for one (and hence for all) $i \geq 2$ if and only if f is p-ary plateaued.

Proof. By Theorem 6, putting $x_k = |\widehat{\chi_f}(\omega)|^2$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ and $y_k = 1$, $1 \leq k \leq \mathcal{N}_{\widehat{\chi_f}}$, with $p_1 = i$ and $p_2 = \frac{i}{i-1}$, we have

$$\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} |\widehat{\chi_f}(\omega)|^2 \leq \left(\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} |\widehat{\chi_f}(\omega)|^{2i} \right)^{\frac{1}{i}} \left(\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} 1 \right)^{\frac{i-1}{i}},$$

namely by the Parseval identity, $p^{2ni} \leq S_i(f) * \mathcal{N}_{\widehat{\chi_f}}^{(i-1)}$, where the equality holds for one (and hence for all) $i \geq 2$ if and only if for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, $|\widehat{\chi_f}(\omega)|^2 = d$ for some $d \in \mathbb{R}^+$; equivalently, f is p-ary plateaued. The proof is complete. □

Proposition 14. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for every positive integer i, we have*

$$S_i(f)^2 \leq S_{2i}(f) * \mathcal{N}_{\widehat{\chi_f}},$$

with equality for one (and hence for all) $i \geq 1$ if and only if f is p-ary plateaued.

Proof. By Theorem 6, putting $x_k = |\widehat{\chi_f}(\omega)|^{2i}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ and $y_k = 1$, $1 \leq k \leq \mathcal{N}_{\widehat{\chi_f}}$, we have $S_i(f)^2 \leq S_{2i}(f) * \mathcal{N}_{\widehat{\chi_f}}$, where the equality holds for one (and hence for all) $i \geq 1$ if and only if $|\widehat{\chi_f}(\omega)|^2$ is the same positive integer for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$; equivalently, f is p-ary plateaued. The proof is complete. □

In particular, for $i = 1$, Proposition 14 (also for $i = 2$, Theorem 8) introduces the following bound stating the trade-off between the number of nonzero values of Walsh transform and the value of fourth Walsh power moment of a p-ary function, and this bound is satisfied only by plateaued functions.

Corollary 7. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then we have $p^{4n} \leq S_2(f) * \mathcal{N}_{\widehat{\chi_f}}$, with equality if and only if f is p-ary plateaued.*

The following bound can be clearly derived from Proposition 6 and Corollary 7.

Corollary 8. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $\theta_f = \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a \mathcal{D}_b f(x)}$. Then we have $p^{3n} \leq \theta_f * \mathcal{N}_{\widehat{\chi_f}}$, with equality if and only if f is p-ary plateaued.*

We derive from Proposition 5 and Corollary 8 the following bound, which was first observed in [31], in characteristic 2.

Corollary 9. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $\mathcal{A}_{\Delta_f} = \sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2$. Then we have $p^{3n} \leq \mathcal{A}_{\Delta_f} * \mathcal{N}_{\widehat{\chi_f}}$, with equality if and only if f is p-ary plateaued.*

The following result was first given in [31], in characteristic 2.

Proposition 15. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$p^{2n} \leq \mathcal{N}_{\widehat{\chi_f}} * \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2), \tag{14}$$

with equality if and only if f is p-ary plateaued.

Proof. Clearly, by the Parseval identity we have

$$p^{2n} = \sum_{\omega \in \mathbb{F}_p^n} |\widehat{\chi_f}(\omega)|^2 \leq \mathcal{N}_{\widehat{\chi_f}} * \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2).$$

Assume that the bound (14) is satisfied. By the Parseval identity, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, we have $|\widehat{\chi_f}(\omega)|^2 = \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2)$, that is, there exits an integer s such that $|\widehat{\chi_f}(\omega)|^2 = p^{n+s}$, i.e., f is s-plateaued. Conversely, by Lemma 5, we have $\mathcal{N}_{\widehat{\chi_f}} = p^{n-s}$ and $|\widehat{\chi_f}(\omega)|^2 = p^{n+s}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$. Hence, the proof is complete. □

We now deduce from the Parseval identity a characterization of plateaued functions in terms of their fourth Walsh power moment.

Proposition 16. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$S_2(f) \leq p^{2n} \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2),$$

with equality if and only if f is p-ary plateaued.

Proof. Clearly, we have

$$\sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^4 = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^2 |\widehat{\chi_f}(\omega)|^2 \leq \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^2 \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2); \tag{15}$$

equivalently, $S_2(f) \leq S_1(f) \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2)$. For the equality case, assume that f is plateaued. By Lemma 3, we conclude that the bound is satisfied. Conversely, by (15), for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, we have $|\widehat{\chi_f}(\omega)|^2 = \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2)$, that is, f is plateaued. □

We can derive directly from Propositions 6 and 16 the following bounds.

Proposition 17. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$. Set $\theta_f = \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a \mathcal{D}_b f(x)}$. Then we have*

$$\theta_f \leq p^n \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2), \tag{16}$$

with equality if and only if f is p-ary plateaued. Set $\mathcal{A}_{\Delta_f} = \sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2$. Equivalently, by Proposition 5 we have

$$\mathcal{A}_{\Delta_f} \leq p^n \max_{b \in \mathbb{F}_{p^n}} (|\widehat{\chi_f}(b)|^2),$$

with equality if and only if f is p-ary plateaued.

Notice that the equality case of (16), in characteristic 2, was observed in [3].

6 Conclusion

Some plateaued functions have attracted attention since their introduction in the literature due to their role in diverse domains of Boolean and vectorial functions for sequences and cryptography. In this paper, we provided several characterizations of p-ary plateaued functions via their Walsh power moments, autocorrelation functions and derivatives. We also characterized p-ary partially bent (vectorial) functions by their second-order derivatives and fourth Walsh power moments. Furthermore, for any prime power q, we redefined the notion of partially bent functions over $\mathbb{F}_q$ and next presented some of their characterizations in terms of their Walsh power moments, second-order derivatives and autocorrelation functions.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. The third author is supported by TÜBİTAK (the Scientific and Technological Research Council of Turkey), program no: BİDEB 2214/A.

References

1. Ambrosimov, A.: Properties of bent functions of q-valued logic over finite fields. Discrete Mathematics and Applications, **4**(4), 341–350 (1994)
2. Anbar, N., Meidl, W.: Quadratic functions and maximal artin–schreier curves. Finite Fields and Their Applications **30**, 49–71 (2014)
3. Canteaut, A., Carlet, C., Charpin, P., Fontaine, C.: On cryptographic properties of the cosets of r (1, m). IEEE Transactions on Information Theory **47**(4), 1494–1513 (2001)
4. Carlet, C.: Partially-bent functions. Designs, Codes and Cryptography **3**(2), 135–145 (1993)
5. Carlet, C.: Boolean functions for cryptography and error correcting codes. Boolean models and methods in mathematics, computer science, and engineering **2**, 257–397 (2010)
6. Carlet, C.: Boolean and vectorial plateaued functions and APN functions. IEEE Transactions on Information Theory **61**(11), 6272–6289 (2015)
7. Carlet, C., Dubuc, S.: On generalized bent and q-ary perfect nonlinear functions. In: Finite Fields and Applications, pp. 81–94. Springer (2001)
8. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Designs, Codes and Cryptography **78**(1), 5–50 (2016)
9. Carlet, C., Mesnager, S., Özbudak, F., Sınak, A.: Explicit characterizations for plateaued-ness of p-ary (vectorial) functions. In: Second International Conference on Codes, Cryptology and Information Security (C2SI-2017), In Honor of Claude Carlet. pp. 328–345. Springer (2017)
10. Carlet, C., Prouff, E.: On plateaued functions and their constructions. In: FSE. pp. 54–73. Springer (2003)
11. Çeşmelioğlu, A., Meidl, W.: A construction of bent functions from plateaued functions. Designs, codes and cryptography pp. 1–12 (2013)
12. Çesmelioglu, A., Meidl, W., Topuzoglu, A.: Partially bent functions and their properties. (2014)
13. Coulter, R.S., Matthews, R.W.: Bent polynomials over finite fields. Bulletin of the Australian Mathematical Society **56**(3), 429–437 (1997)
14. Dillon, J.F.: Elementary Hadamard difference sets. Ph.D. thesis (1974)
15. Hou, X.D.: q-ary bent functions constructed from chain rings. Finite Fields and Their Applications **4**(1), 55–61 (1998)
16. Hou, X.D.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields and Their Applications **10**(4), 566–582 (2004)
17. Hyun, J.Y., Lee, J., Lee, Y.: Explicit criteria for construction of plateaued functions. IEEE Transactions on Information Theory **62**(12), 7555–7565 (2016)
18. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. Journal of Combinatorial Theory, Series A **40**(1), 90–107 (1985)
19. Langevin, P.: On generalized bent functions. In: Eurocode'92, pp. 147–152. Springer (1993)
20. Lidl, R., Niederreiter, H.: Finite fields, vol. 20. Cambridge university press (1997)
21. Logachev, O.A., Salnikov, A., Yashchenko, V.V.: Bent functions on a finite abelian group. Discrete Mathematics and Applications **7**(6), 547–564 (1997)
22. Mesnager, S.: Characterizations of plateaued and bent functions in characteristic p. In: International Conference on Sequences and Their Applications. pp. 72–82. Springer (2014)
23. Mesnager, S.: Bent functions: Fundamentals and Results. Switzerland, Springer pp. 1-544 (2016)
24. Mesnager, S., Özbudak, F., Sınak, A.: Results on characterizations of plateaued functions in arbitrary characteristic. In: International Conference on Cryptography and Information Security in the Balkans. pp. 17–30. Springer (2015)
25. Mesnager, S., Özbudak, F., Sınak, A.: On the p-ary (cubic) bent and plateaued (vectorial) functions. Designs, Codes and Cryptography pp. 1–28 (2017)
26. Mesnager, S., Özbudak, F., Sınak, A., Cohen, G.: On q-ary plateaued functions over Fq and their explicit characterizations. European Journal of Combinatorics (2018)
27. Nyberg, K.: Constructions of bent functions and difference sets. In: Workshop on the Theory and Application of of Cryptographic Techniques. pp. 151–160. Springer (1990)
28. Rothaus, O.S.: On "bent" functions. Journal of Combinatorial Theory, Series A **20**(3), 300–305 (1976)
29. Rudin, W., et al.: Principles of mathematical analysis, vol. 3. McGraw-hill New York (1964)
30. Wang, X., Zhou, J.: Generalized partially bent functions. In: Future Generation Communication and Networking (FGCN 2007). vol. 1, pp. 16–21. IEEE (2007)
31. Zheng, Y., Zhang, X.M.: Plateaued functions. In: ICICS. vol. 99, pp. 284–300. Springer (1999)