On q-ary Plateaued Functions over $\mathbb{F}_q$ and their Explicit Characterizations[☆]

Sihem Mesnager[a,b,c], Ferruh Özbudak[d,e], Ahmet Sınak[b,e,f], Gérard Cohen[c]

[a] *Department of Mathematics, University of Paris VIII, France*
[b] *LAGA, UMR 7539, CNRS, University of Paris VIII and University of Paris XIII, France*
[c] *Telecom ParisTech, France*
[d] *Department of Mathematics, Middle East Technical University, Turkey*
[e] *Institute of Applied Mathematics, Middle East Technical University, Turkey*
[f] *Department of Mathematics and Computer Sciences, Necmettin Erbakan University, Turkey*

Abstract

Plateaued and bent functions play a significant role in cryptography, sequence theory, coding theory and combinatorics. Coulter and Matthews (1997) redefined bent functions over any finite field $\mathbb{F}_q$ where q is a prime power, and established their properties. The objective of this work is to redefine the notion of plateaued functions over $\mathbb{F}_q$, and present several explicit characterizations. We first introduce, over $\mathbb{F}_q$, the notion of q-ary plateaued functions, which relies on the concept of the Walsh-Hadamard transform in terms of canonical additive characters of $\mathbb{F}_q$. We also give an example of q-ary plateaued functions, which is not vectorial p-ary plateaued function. We then characterize q-ary plateaued functions by means of derivatives, the Walsh power moments and autocorrelation functions.

Keywords: q-ary functions, bent functions, plateaued functions, additive character.

[☆]In memoriam Michel Deza, PhD adviser of Gérard Cohen. Nostalgy of by-gone evenings at La Closerie des Lilas discussing ad libitum maths and life.

Email address: `smesnager@univ-paris8.fr`, `ozbudak@metu.edu.tr`, `sahmet@metu.edu.tr`,`cohen@enst.fr` (Gérard Cohen)

1. Introduction

Bent functions over $\mathbb{Z}_2$ were introduced by Rothaus [19] in the 1970s, and then generalized to any residue class ring $\mathbb{Z}_k$, where k is any positive integer, by Kumar et al. (1985) in [9]. In 1997, Coulter and Matthews redefined in [5] the notion of bent functions for any finite field $\mathbb{F}_q$, where q is a prime power. Bent functions have attracted a lot of research in the past four decades not only for their own sake as interesting combinatorial objects, but also for their relations to coding theory, combinatorics, design theory, sequence theory, and applications in cryptography. Since bent functions are unbalanced, Carlet [1] introduced a super class of bent functions: the notion of *partially bent functions*. As an extension of this notion, Zheng and Zhang [20] introduced, over $\mathbb{Z}_2$, the notion of *plateaued functions* whose absolute Walsh-Hadamard transform takes only one nonzero value (also possibly the value 0). They have been widely studied (see, e.g., [2, 3, 8, 14, 12, 21]) due to their cryptographic and combinatoric properties. Besides the useful properties of bent functions, they may have balanced-ness and correlation immunity. Indeed, some plateaued functions have low Hadamard transform, which protects against fast correlation attacks and linear cryptanalysis. Moreover, the order of resiliency and the nonlinearity of Boolean functions are strongly bounded by plateaued functions only.

Plateaued Boolean functions were extended to *p-ary plateaued functions*, and have been further studied in [4, 6, 7, 13, 15, 16]. More precisely, the first author introduced in [13] new characterizations of p-ary plateaued functions by the Walsh power moments, and then independently, Carlet [2] introduced different characterizations of plateaued Boolean (vectorial) functions in terms of the derivatives, autocorrelation functions and Walsh transform values. Recently, the authors [4, 15, 16] have extended those characterizations, and presented further characterizations of p-ary plateaued (vectorial) functions in terms of Walsh power moments, derivatives and autocorrelation functions. In this work, after introducing the notion of q-ary plateaued functions, we present several explicit characterizations of q-ary plateaued functions.

The paper is structured as follows. In Section 2, we collect main notations and set the necessary background. Section 3 introduces the notion of q-ary plateaued functions over $\mathbb{F}_q$, which relies on the concept of the Walsh-Hadamard transform in terms of canonical additive characters of $\mathbb{F}_q$. We shall give a concrete example to show the existence of q-ary plateaued functions, which is not vectorial p-ary plateaued function. Section 4 presents several characterizations of q-ary plateaued functions. More precisely, Subsections 4.1, 4.2 and 4.3 characterize q-ary plateaued functions in terms of the derivatives, Walsh power moments and autocorrelation functions, respectively. We finally conclude the paper.

2. Preliminaries

For any set E, $\#E$ denotes the size of E and $E^\star = E \setminus \{0\}$. Let $\mathbb{C}$ be the field of complex numbers. Given a complex number $z \in \mathbb{C}$, $|z|$ and $\bar{z}$ denote the module and the conjugate of z, respectively. For a prime p, $\mathbb{F}_p$ is the Galois field with p elements. For an integer $m \geq 1$, a finite extension field of degree m over $\mathbb{F}_p$ is denoted by $\mathbb{F}_q$ where $q = p^m$. For an integer $n \geq 1$, 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 $\mathbb{F}_q^n$. The *relative trace* of $\alpha \in \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is defined as $\mathrm{Tr}_q^{q^n}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$. The *absolute trace* of $\beta \in \mathbb{F}_{p^m}$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}_p^{p^m}(\beta) = \beta + \beta^p + \cdots + \beta^{p^{m-1}}$. *A primitive p-th root of unity* $e^{2\pi\sqrt{-1}/p}$ in $\mathbb{C}$ is denoted by ϵ_p. The complex conjugation of ϵ_p is its inverse, i.e., $\overline{\epsilon_p} = \epsilon_p^{-1}$. The function χ from $\mathbb{F}_q$ to $\mathbb{C}$ defined as

$$\chi(x) = \epsilon_p^{\mathrm{Tr}_p^q(x)} \text{ for all } x \in \mathbb{F}_q \tag{1}$$

is called *a canonical additive character* of $\mathbb{F}_q$. Notice that for each $y \in \mathbb{F}_q$, the function $\chi_y(x) = \chi(yx)$ for all $x \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$ and every additive character of $\mathbb{F}_q$ is obtained in this way. In particular, χ_0 is a *trivial* additive character of $\mathbb{F}_q$ defined as $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$. For each additive character χ of $\mathbb{F}_q$, there is associated the *conjugate* character $\overline{\chi}$ defined as $\overline{\chi}(x) = \overline{\chi(x)}$ for all $x \in \mathbb{F}_q$. The following well known properties of χ will be frequently used in the sequel. 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 χ and ψ be the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_q^n$, respectively. Then for all $\alpha \in \mathbb{F}_q^n$, they are connected by the identity $\chi(\mathrm{Tr}_q^{q^n}(\alpha)) = \psi(\alpha)$. The reader is referred to [10, Chapter 5] for further reading on characters of $\mathbb{F}_q$.

For a function f from $\mathbb{F}_q^n$ to $\mathbb{F}_q$, a corresponding function χ_f from $\mathbb{F}_q^n$ to $\mathbb{C}$ is defined by $\chi_f(x) := \chi(f(x)) = \epsilon_p^{\mathrm{Tr}_p^q(f(x))}$ for $x \in \mathbb{F}_q^n$. 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 as

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

where χ is an additive character of $\mathbb{F}_q$ and " $\cdot$ " denotes an inner product in $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Notice that (2) can be also given without the conjugate of χ. We remark that f is constant, if and only if, $\widehat{\chi_f}(\omega) = 0$ at any nonzero $\omega \in \mathbb{F}_{q^n}$ (see, e.g., [17]). The set of the complex values $\widehat{\chi_f}(\omega)$, called the Walsh coefficient of f at point ω, for all $\omega \in \mathbb{F}_{q^n}$ is called the Walsh spectrum of f. The Walsh support of f is the set $\{\omega \in \mathbb{F}_{q^n} : \widehat{\chi_f}(\omega) \neq 0\}$, which can be denoted by $\mathcal{W}_S$ and $\mathcal{N}_S = \#\mathcal{W}_S$, and as is readily seen that $\mathcal{N}_S \leq q^n$. For any nonnegative integer i, the Walsh power moment of q-ary function f is defined as

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

with the convention that $S_0(f) = q^n$. It is a well known fact that $S_1(f) = q^{2n}$ (*Parseval identity*). We now recall the following definitions (see in [5]). A q-ary function f is said to be *balanced* over $\mathbb{F}_q$ if f takes every value of $\mathbb{F}_q$ the same number, q^{n-1} times; otherwise, it is called unbalanced. The derivative (i.e., the first-order 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 $x \in \mathbb{F}_q^n$. The second-order derivative of f at point $(a, b) \in (\mathbb{F}_q^n)^2$ is $\mathcal{D}_b\mathcal{D}_a f(x) = f(x + a + b) - f(x + a) - f(x + b) + f(x)$ for $x \in \mathbb{F}_q^n$. 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 an additive character of $\mathbb{F}_q$ in (1) (see, e.g., [9]). For two functions $G_1, G_2 : \mathbb{F}_q^n \to \mathbb{C}$, the convolution of G_1 and G_2 is the map from $\mathbb{F}_q^n$ to $\mathbb{C}$ defined as

$$(G_1 \otimes G_2)(a) = \sum_{x \in \mathbb{F}_q^n} G_1(a-x)G_2(x) \tag{3}$$

for all $a \in \mathbb{F}_q^n$ (see, e.g., [17, Definition 10.1.18]).

Theorem 1. *[17, Theorem 10.1.19] The convolution theorem of Fourier analysis states that the Fourier transform of a convolution of two functions is the ordinary product of their Fourier transforms: $\widehat{G_1 \otimes G_2} = \widehat{G_1}\widehat{G_2}$, where G_1 and G_2 are two complex valued functions from $\mathbb{F}_q^n$ to $\mathbb{C}$. Moreover, we have*

$$\widehat{G_1} \otimes \widehat{G_2} = q^n \widehat{G_1 G_2}. \tag{4}$$

3. On the Notion of q-ary Plateaued Functions over $\mathbb{F}_q$

This section introduces the notion of q-ary plateaued functions over $\mathbb{F}_q$. We firstly recall that the notion of q-ary bent functions.

In 1997, the notion of bent functions was redefined in [5] for any finite field $\mathbb{F}_q$ (where $q = p^m$ for a prime p and an integer $m > 1$) as follows. A function f from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ is called *q-ary bent* if $|\widehat{\chi_f}(\omega)|^2 = q^n$ for all $\omega \in \mathbb{F}_q^n$. Now, we will redefine the notion of plateaued functions for any finite field $\mathbb{F}_q$. Notice that these notions rely on the concept of the Walsh-Hadamard transform in terms of canonical additive character of $\mathbb{F}_q$, given in (2).

Definition 1. *Let f be a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. Then, f is called q-ary plateaued if its absolute Walsh-Hadamard transform takes at most one nonzero value of μ, which is called* the amplitude *of the q-ary plateaued functions.*

For any n-variable q-ary plateaued function, there exists a nonzero value of μ such that $\mu^2 = q^r$ where $r \geq n$ since $\mathcal{N}_S \leq q^n$. Then a squared absolute Walsh-Hadamard transform of q-ary plateaued function is divisible by q^n, and hence, there exists an integer s with $0 \leq s \leq n$ such that $\mu^2 = q^{n+s}$. Hence, we say that f is *q-ary s-plateaued* (or, *q-ary plateaued of the amplitude* μ) if $|\widehat{\chi_f}(\omega)|^2 \in \{0, \mu^2\}$ for all $\omega \in \mathbb{F}_q^n$.

By MAGMA in [11], we have obtained several q-ary plateaued functions, which show their existence for prime power q.

Example 1. *Let $q = 4$ and $n = 3$. $\mathrm{Tr}_4^{4^3}(\xi^2 x + \xi x^3)$ is a 4-ary 0-plateaued function, and $\mathrm{Tr}_4^{4^3}(\xi^3 x^3)$ is a 4-ary 1-plateaued function, where $\mathbb{F}_{4^3}^\star = \langle \xi \rangle$ with $\xi^3 + \xi^2 + \xi + \psi^2 = 0$ for $\mathbb{F}_{2^2}^\star = \langle \psi \rangle$.*

The multiplicity of absolute Walsh coefficient of q-ary plateaued functions can be given by the Parseval identity (see in [13] for the p-ary case).

Lemma 1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be s-plateaued where s is an integer with $0 \leq s \leq n$. 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.*

Proof. Recall that $\mathcal{N}_S$ denotes the size of the Walsh support $\{\omega \in \mathbb{F}_q^n : |\widehat{\chi_f}(\omega)|^2 = q^{n+s}\}$ of s-plateaued f. Then, $\sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^2 = \mathcal{N}_S q^{n+s}$ and hence, $\mathcal{N}_S = q^{n-s}$ by the Parseval identity. Since $\#\mathbb{F}_q^n = q^n$, then we have $\#\{\omega \in \mathbb{F}_q^n : |\widehat{\chi_f}(\omega)|^2 = 0\} = q^n - q^{n-s}$. Hence, the result now follows. □

The following natural consequence can be given for q-ary functions.

Remark 1. *A function f is q-ary bent, if and only if, f is q-ary 0-plateaued. This follows from the Parseval identity, (which implies that q-ary plateaued is q-ary bent, if and only if, its absolute Walsh-Hadamard transform never takes the value 0).*

In [5], by choosing an m-dimensional basis of $\mathbb{F}_q$, a q-ary bent function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ is equivalent to a vectorial p-ary bent function from $\mathbb{F}_p^{mn}$ to $\mathbb{F}_p^m$, where $q = p^m$ for any prime p and a positive integer m. On the other hand, the following example shows that there exits a q-ary plateaued function which is not vectorial p-ary plateaued function for $q = 4$ and $p = 2$. Hence, a q-ary plateaued function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ with its Walsh-Hadamard transform may not correspond to a vectorial p-ary plateaued function from $\mathbb{F}_p^{mn}$ to $\mathbb{F}_p^m$ with the

Walsh-Hadamard transforms of its component functions for some cases. Then we can say that:

Remark 2. *The notion of q-ary plateaued functions is not equivalent to the one of vectorial p-ary plateaued functions, in general. This is the main reason of dealing with the notion of q-ary plateaued functions in this paper.*

Example 2. *Let $q = 4$ and $n = 3$ where $q = p^m$ for $p = 2$, $m = 2$. A function $f(x) = \mathrm{Tr}_4^{4^3}(\xi^4 x^{11} + \xi^4 x^7 + \xi^5 x^5)$ is 4-ary 1-plateaued where $\mathbb{F}_{4^3}^\star = \langle \xi \rangle$ with $\xi^3 + \xi^2 + \xi + \gamma^2 = 0$ for $\mathbb{F}_{2^2}^\star = \langle \gamma \rangle$. However, its component function $f_\gamma(x) = \mathrm{Tr}_2^4(\gamma f(x))$ is not plateaued function. Hence, f is not vectorial plateaued Boolean function from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$.*

Remark 3. *We should remark that the following presented characterizations of q-ary plateaued functions can not be given for vectorial p-ary functions. This is the other reason of working on q-ary plateaued functions in this paper. Notice that, by Remark 1, these characterizations are valid for q-ary bent functions.*

4. Characterizations of q-ary Plateaued Functions over $\mathbb{F}_q$

This section mainly extends to q-ary case some characterizations of p-ary plateaued functions given in [4, 16]. We present several characterizations of q-ary plateaued functions by means of the derivatives, Walsh power moments and autocorrelation functions. We present these characterizations, although some of them are interrelated, since they can provide useful information about the structure of q-ary plateaued functions.

4.1. Characterizations of q-ary Plateaued Functions by Derivatives

In this subsection, we firstly present a strong characterization of q-ary plateaued functions in terms of the second-order derivatives. To do this, we recall the well known properties of the Fourier transform of complex valued functions.
Let $G : \mathbb{F}_q^n \to \mathbb{C}$ be a function and let $\widehat{G} : \mathbb{F}_q^n \to \mathbb{C}$ be its Fourier transform

defined as $\widehat{G}(v) = \sum_{u\in\mathbb{F}_q^n} G(u)\overline{\chi}(v\cdot u)$ for all $v \in \mathbb{F}_q^n$. We have $\widehat{\widehat{G}}(u) = q^n G(-u)$ for all $u \in \mathbb{F}_q^n$. As is readily seen, $G(-u) = \frac{1}{q^n}\sum_{v\in\mathbb{F}_q^n} \widehat{G}(v)\overline{\chi}(v\cdot u)$ for all $u \in \mathbb{F}_q^n$. Then, we have $G(u) = 0$ 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,

$$G_1(u) = G_2(u),\ \forall u \in \mathbb{F}_q^n \iff \widehat{G}_1(v) = \widehat{G}_2(v),\ \forall v \in \mathbb{F}_q^n, \tag{5}$$

where G_1 and G_2 are two complex valued functions from $\mathbb{F}_q^n$ to $\mathbb{C}$.

Theorem 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Set $\theta_f(x) = \sum_{a,b\in\mathbb{F}_q^n} \chi(\mathcal{D}_b\mathcal{D}_a f(x))$ for all $x \in \mathbb{F}_q^n$. Then, f is q-ary plateaued, if and only if, $\theta_f(x) = \theta$ for all $x \in \mathbb{F}_q^n$. In other words, there exists an integer s with $0 \le s \le n$ such that f is q-ary s-plateaued, 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. For all $x \in \mathbb{F}_q^n$, $\theta_f(x) = \theta$ if and only if for all $x \in \mathbb{F}_q^n$,

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

(by the bijective change of variables: $a \mapsto a - x$ and $b \mapsto b - x$); equivalently, for all $x \in \mathbb{F}_q^n$

$$\sum_{a,b\in\mathbb{F}_q^n} \overline{\chi_f}(a)\overline{\chi_f}(b)\chi_g(x-a-b) = \theta\overline{\chi_f}(x),$$

where $g(y) := f(-y)$ for all $y \in \mathbb{F}_q^n$. Equivalently, using the convolution product in (3), for all $x \in \mathbb{F}_q^n$

$$\left(\overline{\chi_f} \otimes \overline{\chi_f} \otimes \chi_g\right)(x) = \theta\overline{\chi_f}(x). \tag{6}$$

By (4), the Fourier transform of left-hand side of (6) is equal to $\widehat{\overline{\chi_f}}(\omega)\,\widehat{\overline{\chi_f}}(\omega)\widehat{\chi_g}(\omega)$ for all $\omega \in \mathbb{F}_q^n$. Notice that for all $\omega \in \mathbb{F}_q^n$,

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

and $\widehat{\chi_g}(\omega) = \widehat{\chi_f}(-\omega)$. According to the bijectivity of the Fourier transform in (5), for all $x \in \mathbb{F}_q^n$, (6) holds if and only if for all $\omega \in \mathbb{F}_q^n$

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

Therefore, $\theta_f(x) = \theta$ for all $x \in \mathbb{F}_q^n$ if and only if $|\widehat{\chi_f}(\omega)|^2 \in \{0, \theta\}$ for all $\omega \in \mathbb{F}_q^n$, that is, f is q-ary plateaued where $\theta = q^{n+s}$. 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, that is, f is q-ary bent. $\square$

Notice that Theorem 2 can be proven without using the convolution product (see the proof of [16, Theorem 3] for the p-ary case). The following results can be readily derived from Theorem 2.

Corollary 1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be s-plateaued. Then, $\sum_{x \in \mathbb{F}_q^n} \theta_f(x) = q^{2n+s}$.*

Corollary 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Set $S_2(f) = \sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^4$. Then, f is q-ary plateaued, if and only if, for all $x \in \mathbb{F}_q^n$,*

$$S_2(f) = q^{2n}\theta_f(x). \tag{7}$$

Proof. Assume that f is q-ary s-plateaued. Then $S_2(f) = q^{3n+s}$ by Lemma 1, and $\theta_f(x) = q^{n+s}$ for all $x \in \mathbb{F}_q^n$ by Theorem 2. Hence, (7) holds for all $x \in \mathbb{F}_q^n$. Conversely, assume that (7) holds for all $x \in \mathbb{F}_q^n$, that is, $\theta_f(x) = \theta$ is constant for all $x \in \mathbb{F}_q^n$ where $\theta = q^{-2n}S_2(f)$. Thus, by Theorem 2, f is q-ary plateaued. $\square$

The following observation shows that the characterizations of q-ary plateaued functions by means of the second-order derivatives can be given by the first-order derivatives, which makes easier to check the plateaued-ness of q-ary functions.

Proposition 1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. For all $v \in \mathbb{F}_q$, $\#\{(a, b) \in (\mathbb{F}_q^n)^2 : \mathcal{D}_b\mathcal{D}_a f(x) = v\} = \#\{(a, b) \in (\mathbb{F}_q^n)^2 : \mathcal{D}_a f(b) - \mathcal{D}_a f(x) = v\}$ for all $x \in \mathbb{F}_q^n$.*

Proof. For each $x \in \mathbb{F}_q^n$, by the (bijective) change of variable: $b \mapsto b - x$, we have $\mathcal{D}_b\mathcal{D}_a f(x) = \mathcal{D}_{b-x}\mathcal{D}_a f(x) = f(b+a) - f(b) - f(x+a) + f(x) = \mathcal{D}_a f(b) - \mathcal{D}_a f(x)$ for all $a, b \in \mathbb{F}_q^n$. This completes the proof. $\square$

4.2. Characterizations of q-ary Plateaued Functions by Walsh Power Moments

This subsection presents several characterizations of q-ary plateaued functions by means of the even power moments of Walsh-Hadamard transform. We firstly introduce the following useful tools to characterize q-ary plateaued functions. For every nonnegative integers i and A, we have

$$\sum_{\omega\in\mathbb{F}_q^n}\Big(|\widehat{\chi_f}(\omega)|^2-A\Big)^2|\widehat{\chi_f}(\omega)|^{2i} \quad = S_{i+2}(f)-2AS_{i+1}(f)+A^2S_i(f)\geq 0. \quad (8)$$

For a positive integer i, there exists a positive integer A such that

$$S_i(f)A^2-2S_{i+1}(f)A+S_{i+2}(f)=0 \quad (9)$$

if and only if f is q-ary plateaued of amplitude μ where $A=\mu^2$. To exhibit a link between the Walsh power moments of q-ary plateaued functions, we shall consider some particular values of i in (8). More precisely, let $A=q^{n+s}$ for an integer s with $1\leq s\leq n$ and $i=1$, then f is q-ary s-plateaued if and only if $S_3(f)=2q^{n+s}S_2(f)-q^{4n+2s}$, and for $i=2$, then f is q-ary s-plateaued if and only if $S_4(f)=2q^{n+s}S_3(f)-q^{2n+2s}S_2(f)$. Notice that we have $S_3(f)\geq q^{4n+2s}$ if $S_2(f)\geq q^{3n+s}$, with equality, then $S_4(f)\geq q^{5n+3s}$.
We can give the following more general equation than (8). For every nonnegative integers A, i and j, we have

$$\sum_{\omega\in\mathbb{F}_q^n}\Big(|\widehat{\chi_f}(\omega)|^2-A\Big)^{2j}|\widehat{\chi_f}(\omega)|^{2i}\geq 0. \quad (10)$$

We consider some special values of i,j and A in (10). For $A=q^n$ and $i=0,j\geq 1$, f is q-ary bent if and only if the inequality (10) is an equality. Moreover, for $s\geq 1$, $A=q^{n+s}$, $i\geq 1$ and $j\geq 1$, f is q-ary s-plateaued if and only if the inequality (10) becomes an equality.
The sequence of the Walsh power moments of q-ary plateaued functions is a simple geometric sequence.

Theorem 3. *Let $f:\mathbb{F}_q^n\rightarrow\mathbb{F}_q$ be q-ary s-plateaued where s is an integer with $0\leq s\leq n$. Then for all an integer $i\geq 1$,*

$$S_i(f)=\sum_{\omega\in\mathbb{F}_q^n}|\widehat{\chi_f}(\omega)|^{2i}=q^{n(i+1)+s(i-1)}.$$

Moreover, we have $S_i(f)S_j(f)=S_{i+1}(f)S_{j-1}(f)$ for all integers $i\geq 1,j\geq 2$.

Proof. By Lemma 1, for a positive integer i, we have $S_i(f) = q^{n-s}(q^{n+s})^i = q^{n(i+1)+s(i-1)}$. Readily, the followings

$$\begin{aligned} S_i(f)S_j(f) &= q^{n(i+1)+s(i-1)}q^{n(j+1)+s(j-1)} = q^{n(i+j+2)+s(i+j-2)} \text{ and} \\ S_{i+1}(f)S_{j-1}(f) &= q^{n(i+2)+si}q^{nj+s(j-2)} = q^{n(i+j+2)+s(i+j-2)} \end{aligned}$$

are equal for all $i \geq 1$ and $j \geq 2$. Hence, the result follows. □

We now recall the following well known inequality to present next results.

Theorem 4 (Hölder's Inequality). *[18] 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 $\mathbb{C}^m$,*

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

where the equality holds, if and only if, for all $k \in \{1, \ldots, m\}$, there exists a nonnegative number c such that $|x_k|^{p_1} = c|y_k|^{p_2}$. If $p_1 = p_2 = 2$, then the above inequality is reduced to the Cauchy-Schwarz Inequality.

The Cauchy-Schwarz Inequality gives the following inequality, and its equality case yields the characterization of q-ary plateaued functions.

Theorem 5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then for all integer $i \geq 1$, $S_{i+1}(f)^2 \leq S_{i+2}(f)S_i(f)$, with equality for at least one $i \geq 1$, if and only if, f is q-ary plateaued.*

Proof. By Theorem 4, for $x_k = |\widehat{\chi_f}(\omega)|^i$ and $y_k = |\widehat{\chi_f}(\omega)|^{i+2}$ for all $\omega \in \mathbb{F}_q^n$, then we have

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

that is, $S_{i+1}(f)^2 \leq S_i(f)S_{i+2}(f)$ for $i \geq 1$, where the equality holds for at least one $i \geq 1$ if and only if for all $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^{2i} = c\,|\widehat{\chi_f}(\omega)|^{2i+4}$ for nonnegative c, equivalently, $|\widehat{\chi_f}(\omega)|$ is constant (also possibly the value 0), i.e., f is q-ary plateaued. □

Remark 4. *Notice that Theorem 5 can be also derived from (9). The reduced discriminant of (9),* $S_{i+1}(f)^2 - S_{i+2}(f)S_i(f) \leq 0$*, with equality if and only if* f *is* q*-ary plateaued.*

The plateaued-ness of q-ary functions can be checked by using only the values of fourth and sixth Walsh power moments.

Theorem 6. *Let* $f : \mathbb{F}_q^n \to \mathbb{F}_q$ *and* s *be an integer with* $1 \leq s \leq n$*. Then,* f *is* q*-ary* s*-plateaued, if and only if,* $S_2(f) = q^{3n+s}$ *and* $S_3(f) = q^{4n+2s}$*. Moreover,* f *is* q*-ary plateaued, if and only if,* $S_2(f)^2 = q^{2n}S_3(f)$*.*

Proof. Assume that f is q-ary s-plateaued. Then, the necessity directly follows from Theorem 3. Conversely, by (8) with $A = q^{n+s}$ at $i = 1$, we have

$$\sum_{\omega \in \mathbb{F}_q^n} \left(|\widehat{\chi_f}(\omega)|^2 - q^{n+s}\right)^2 |\widehat{\chi_f}(\omega)|^2 = S_3(f) - 2q^{n+s}S_2(f) + q^{2n+2s}S_1(f) = 0,$$

where we used the Parseval identity. Hence, $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$, i.e., f is q-ary s-plateaued. Moreover, the second statement follows from Theorem 5 for $i = 1$ and the Parseval identity. □

More precisely, as in the proof of Theorem 5, applying the Cauchy-Schwarz Inequality for $x_k = |\widehat{\chi}_f(\omega)|$ and $y_k = |\widehat{\chi}_f(\omega)|^{2i+1}$ for all $\omega \in \mathbb{F}_q^n$, we have $S_{i+1}(f)^2 \leq S_1(f)S_{2i+1}(f)$ for $i \geq 1$, where the equality holds for at least one $i \geq 1$ if and only if $|\widehat{\chi}_f(\omega)|^2$ is constant (with also possibly the value 0), i.e., f is q-ary plateaued. Hence we can give the following theorem.

Theorem 7. *Let* $f : \mathbb{F}_q^n \to \mathbb{F}_q$*. Then for all integer* $i \geq 1$*, we have*

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

with an equality for at least one $i \geq 1$*, if and only if,* f *is* q*-ary plateaued.*

We can derive from Theorems 3 and 7 the following one, which is more general case of Theorem 6.

Corollary 3. *Let* $f : \mathbb{F}_q^n \to \mathbb{F}_q$ *and* s *be an integer with* $1 \leq s \leq n$*. Then for any positive integer* i*,* $S_{i+1}(f) = q^{n(i+2)+si}$ *and* $S_{2i+1}(f) = q^{n(2i+2)+2is}$*, if and only if,* f *is* q*-ary* s*-plateaued.*

By Theorem 2, the following characterization can be given by considering the well known fact that a function is constant, if and only if, its Fourier transform is zero at any nonzero input.

Theorem 8. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then f is q-ary plateaued, if and only if, for all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$,*

$$\sum_{\omega \in \mathbb{F}_q^n} \widehat{\chi_f}(\alpha+\omega)\overline{\widehat{\chi_f}(\omega)}\ |\widehat{\chi_f}(\omega)|^2\ = 0. \tag{11}$$

Proof. For all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$, the left-hand side of (11) is

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

where we used the fact that $\sum_{\omega\in\mathbb{F}_q^n} \chi(-\omega\cdot(x-a+b-c)) = \begin{cases} q^n \text{ if } c = x-a+b, \\ 0 \ \text{ otherwise.}\end{cases}$

Hence, since $(x,a,b) \mapsto (x, x+a, x+a+b)$ is a permutation of $(\mathbb{F}_q^n)^3$, it equals

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

which is the Fourier transform at $\alpha \in \mathbb{F}_q^n \setminus \{0\}$ of $x \mapsto q^n \sum_{a,b\in\mathbb{F}_q^n} \chi(\mathcal{D}_b\mathcal{D}_a f(x))$ for $x \in \mathbb{F}_q^n$. Hence, thanks to the well known fact that a function is constant, if and only if, its Fourier transform vanishes at any nonzero input, (11) holds for all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$, if and only if, f is q-ary plateaued by Theorem 2. $\square$

Theorem 8 yields the following characterization of q-ary plateaued functions.

Corollary 4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Set $\psi_f(x) = \sum_{\omega\in\mathbb{F}_q^n} \chi(f(x)-\omega\cdot x)\overline{\widehat{\chi_f}(\omega)}|\widehat{\chi_f}(\omega)|^2$ for all $x \in \mathbb{F}_q^n$ and $S_2(f) = \sum_{\omega\in\mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^4$. Then, f is q-ary plateaued, if and only if, for all $x \in \mathbb{F}_q^n$*

$$S_2(f) = q^n\psi_f(x). \tag{12}$$

Proof. Assume that f is q-ary plateaued of amplitude μ, that is, $|\widehat{\chi_f}(\omega)|^2 \in$

$\{0, \mu^2\}$ for all $\omega \in \mathbb{F}_q^n$. Then, for all $x \in \mathbb{F}_q^n$,

$$\begin{aligned}\psi_f(x) &= \mu^2 \sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)} \\ &= \mu^2 \sum_{y \in \mathbb{F}_q^n} \chi(f(x) - f(y)) \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega \cdot (y - x)) = q^n \mu^2\end{aligned}$$

since $\sum_{\omega \in \mathbb{F}_q^n} \chi(\omega \cdot (y - x))$ is null if $y - x \neq 0$. By Theorem 3, $S_2(f) = q^{2n}\mu^2$. Hence, the assertion holds.

Conversely, assume that (12) holds, that is, ψ_f is a constant function for all $x \in \mathbb{F}_q^n$. Then the Fourier transform of ψ_f is null at any $\alpha \in \mathbb{F}_q^n \setminus \{0\}$, that is,

$$\begin{aligned}\widehat{\psi_f}(\alpha) &= \sum_{\omega \in \mathbb{F}_q^n} \sum_{x \in \mathbb{F}_q^n} \chi(f(x) - x \cdot (\alpha + \omega))\overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 \\ &= \sum_{\omega \in \mathbb{F}_q^n} \widehat{\chi_f}(\alpha + \omega)\overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 = 0.\end{aligned}$$

Hence, by Theorem 8, f is q-ary plateaued. □

We can easily give the following link between the Walsh transform and second-order derivative.

Proposition 2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, for all $x \in \mathbb{F}_q^n$,*

$$\sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 = q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)). \tag{13}$$

Proof. By definition $\widehat{\chi_f}$, for all $x \in \mathbb{F}_q^n$, the left-hand side of (13) is

$$\begin{aligned}&\sum_{a,b,c \in \mathbb{F}_q^n} \chi(f(x) - f(a) - f(b) + f(c)) \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega \cdot (a + b - c - x)) \\ &= q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(f(x) - f(a) - f(b) + f(a + b - x)) = q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x))\end{aligned}$$

where we used that $\sum_{\omega \in \mathbb{F}_q^n} \overline{\chi}(\omega \cdot (x - a - b + c))$ is null if $c \neq a + b - x$ in the first equality, and $(a, b, x) \mapsto (a + x, b + x, x)$ is a permutation of $(\mathbb{F}_q^n)^3$ in the last equality. The result now follows. □

By Proposition 2, the characterizations of q-ary plateaued functions, given in Corollaries 2 and 4, are equivalent. From Theorem 2 and Proposition 2, the following characterization of q-ary plateaued functions can be directly derived.

Corollary 5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and s be an integer with $1 \le s \le n$. Then, f is q-ary s-plateaued, if and only if, for all $x \in \mathbb{F}_q^n$*

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

4.3. Characterizations of Plateaued Functions by Autocorrelation Functions

We in the present subsection characterize q-ary plateaued functions in terms of the autocorrelation functions. To do this, we make use of the definition of plateaued functions.

According to the definition of plateaued functions, f is q-ary plateaued of amplitude μ, if and only if, the two functions $|\widehat{\chi_f}|^4$ and $\mu^2|\widehat{\chi_f}|^2$ are equal; equivalently by (5), their Fourier transforms are equal. We first compute the Fourier transform of function

$$|\widehat{\chi_f}(b)|^2 = \sum_{x,y \in \mathbb{F}_p^n} \chi(f(x) - f(y) - b \cdot (x-y))$$

for $b \in \mathbb{F}_q^n$, then for $a \in \mathbb{F}_q^n$

$$\widehat{|\widehat{\chi_f}(a)|^2} = \sum_{x \in \mathbb{F}_q^n} \sum_{y \in \mathbb{F}_q^n} \chi(f(x) - f(y)) \sum_{b \in \mathbb{F}_q^n} \overline{\chi}(b \cdot (x + a - y)) = q^n \overline{\Delta_f}(a)$$

since $\sum_{b \in \mathbb{F}_q^n} \overline{\chi}(b \cdot (x+a-y))$ is null if $y \neq x + a$. Hence, by using this and (4), the Fourier transform of $|\widehat{\chi_f}|^4$ is computed as follows:

$$\widehat{|\widehat{\chi_f}|^2 |\widehat{\chi_f}|^2} \quad = q^{-n}\left(\widehat{|\widehat{\chi_f}|^2} \otimes \widehat{|\widehat{\chi_f}|^2}\right) = q^n\left(\overline{\Delta_f} \otimes \overline{\Delta_f}\right). \tag{14}$$

Notice that, as is easily seen, for all $a \in \mathbb{F}_q^n$,

$$\Delta_f(a) = \sum_{x \in \mathbb{F}_q^n} \chi(f(x+a) - f(x)) = \sum_{x \in \mathbb{F}_q^n} \overline{\chi(f(x) - f(x+a))} = \overline{\Delta_f}(-a), \tag{15}$$

where in the last step we used the (bijective) change of variable: $x \mapsto x - a$. Then we conclude:

Theorem 9. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary plateaued of amplitude μ, if and only if, for all $x \in \mathbb{F}_q^n$*

$$\sum_{a \in \mathbb{F}_q^n} \Delta_f(a)\Delta_f(x-a) = \mu^2 \Delta_f(x).$$

Proof. As we said above, f is q-ary plateaued of amplitude μ, if and only if, $|\widehat{\chi_f}|^4$ and $\mu^2|\widehat{\chi_f}|^2$ are equal; equivalently by (5), $\overline{\Delta_f}\otimes\overline{\Delta_f}=\mu^2\overline{\Delta_f}$; equivalently by (15), $(\Delta_f\otimes\Delta_f)(x)=\mu^2\Delta_f(x)$ for all $x\in\mathbb{F}_q^n$. Hence, the proof is complete by (3). □

To give the next characterization, we first compute the Fourier transform of $|\widehat{\chi_f}|^6$, by (4) and (14), we have

$$\widehat{|\widehat{\chi_f}|^2|\widehat{\chi_f}|^4} \quad = q^{-n}\left(\widehat{|\widehat{\chi_f}|^2}\otimes\widehat{|\widehat{\chi_f}|^4}\right)=q^n\left(\overline{\Delta_f}\otimes\overline{\Delta_f}\otimes\overline{\Delta_f}\right).$$

Then, we say that f is plateaued of μ, if and only if, $|\widehat{\chi_f}|^6$ and $\mu^2|\widehat{\chi_f}|^4$ are equal, by (5) their Fourier transforms are equal, that is, $\Delta_f\otimes\Delta_f\otimes\Delta_f=\mu^2\Delta_f\otimes\Delta_f$. Hence we deduce:

Theorem 10. *Let $f:\mathbb{F}_q^n\to\mathbb{F}_q$. Then, f is q-ary plateaued of amplitude μ, if and only if, for all $x\in\mathbb{F}_q^n$*

$$\sum_{a,b\in\mathbb{F}_q^n}\Delta_f(a)\Delta_f(b)\Delta_f(x-a-b)=\mu^2\sum_{c\in\mathbb{F}_q^n}\Delta_f(c)\Delta_f(x-c).$$

5. Conclusion

Plateaued functions have important applications in the sequence theory, combinatoric and cryptography because of their desirable characteristics. The paper studies q-ary plateaued functions over $\mathbb{F}_q$. We firstly redefined the notion of q-ary plateaued functions. Then, it was highlighted that q-ary bent functions are q-ary plateaued functions. We next presented several explicit characterizations of q-ary plateaued functions in terms of the second-order derivatives, the moments of the Walsh transforms and the autocorrelation functions.

Acknowledgment

The third author is supported by TÜBİTAK (the Scientific and Technological Research Council of Turkey), program no: BİDEB 2214/A.

References

[1] Carlet, C.: Partially-Bent Functions. Design Codes and Cryptography 3(2), pp.135-145 (1993)

[2] Carlet, C.: Boolean and vectorial plateaued functions, and APN functions. IEEE T INFORM THEORY. 61 (11), pp. 6272 - 6289 (2015), On the Properties of Vectorial Functions with Plateaued Components and Their Consequences on APN Functions. International Conference on Codes, Cryptology, and Information Security. LNCS 9084, pp. 63–73. Springer (2015)

[3] Carlet, C., Prouff, E.: On plateaued functions and their constructions. International Workshop on Fast Software Encryption (FSE-2003), pp. 54-73. Springer Berlin Heidelberg (2003)

[4] Carlet, C., Mesnager, S., Özbudak, F., Sınak, A.: Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions. Second International Conference on Codes, Cryptology and Information Security (C2SI-2017), Editors: S. El Hajji, A. Nitaj, E. M. Souidi. In Honor of Claude Carlet. Proceedings, LNCS 10194, Springer, pp. 328-345, (2017)

[5] Coulter, R.S., Matthews, R.W.: Bent polynomials over finite fields. Bulletin of the Australian Mathematical Society. 56.03. pp. 429-437 (1997)

[6] Çeşmelioğlu, A., Meidl, W.: A construction of bent functions from plateaued functions. DESIGN CODE CRYPTOGR. 66(1-3), pp. 231–242 (2013)

[7] Hyun, J.Y., Lee, J., Lee, Y.: Explicit criteria for construction of plateaued functions. IEEE T INFORM THEORY. 62(12), pp. 7555 - 7565 (2016)

[8] Khoo, K., Gong, G., Stinson, D.R.: A New Characterization of Semi-bent and Bent Functions on Finite Fields. DESIGN CODE CRYPTOGR. 38(2) pp. 279-295 (2006)

[9] Kumar, P. V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties, Journal of Comb. Theory. Serie A-40, pp. 90-107 (1985)

[10] Lidl, R., Niederreiter, H.: Finite fields. Cambridge university press, (1997)

[11] MAGMA Computational Algebra System, the Computational Algebra Group at the University of Sydney, http://magma.maths.usyd.edu.au/

[12] Mesnager, S.: Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE T INFORM THEORY. 57(11), pp. 7443-7458 (2011)

[13] Mesnager, S.: Characterizations of plateaued and bent functions in characteristic p. In: 8th International Conference on SEquences and Their Applications (SETA 2014), LNCS, pp. 72-82. Springer, (2014)

[14] Mesnager, S.: Bent functions: fundamentals and results. Springer, New-York (2016)

[15] Mesnager, S., Özbudak, F., Sınak, A.: On the p-ary (Cubic) Bent and Plateaued (Vectorial) Functions. Preprint

[16] Mesnager, S., Özbudak, F., Sınak, A.: Results on Characterizations of Plateaued Functions in Arbitrary Characteristic. Cryptography and Information Security in the Balkans, BalkanCryptSec 2015, Revised Selected Papers, Pasalic, E., Knudsen, L.R.(eds.) LNCS 9540. pp. 17-30. Springer (2016)

[17] Mullen, G.L., Panario, D.: Handbook of finite fields. CRC Press (2013)

[18] Rudin, W.: Principles of mathematical analysis. New York: McGraw-Hill (1964)

[19] Rothaus, O.S.: On bent functions. J COMB THEORY A. 20, pp. 300-305 (1976)

[20] Zheng, Y., Zhang, X.M.: Plateaued functions. Information and Communication Security. pp. 284-300. Springer, Berlin Heidelberg (1999)

[21] Zheng, Y., Zhang, X.M.: Relationships between bent functions and complementary plateaued functions. International Conference on Information Security and Cryptology. pp. 60-75. Springer Berlin Heidelberg (1999)