Some results concerning global avalanche characteristics of two q-ary functions

Brajesh Kumar Singh

Department of Mathematics, School of Allied Sciences,
Graphic Era Hill University, Dehradun-248002 (Uttarakhand) INDIA
bksingh0584@gmail.com

Abstract. The global avalanche characteristics criteria was first introduced by Zhou et al. (Inform. Sci. 180(2) (2010) 256-265). This article is concerned with some new bounds on global avalanche characteristics of two q-ary functions. Based on the above result we obtain a bound on σ_f of $f \in \mathcal{B}_{n,q}$ in terms of σ'_{f_ℓ}s of the restricted functions on $\mathbb{Z}_{n-1}^q$, and construct a class of q-ary bent functions from 1-plateaued functions having dijoint Walsh spectra.

Keywords: q-ary functions; Walsh-Hadamard spectrum (WHT); autocorrelation; q-ary bent functions; GAC

1 Introduction

Boolean have wide applications in several areas including coding theory, communication systems and cryptography, particularly in stream ciphers and block ciphers. The design of conventional cryptographic systems relies on two fundamental principles: confusion and diffusion, introduced by Shannon [12]. The strict avalanche criteria (SAC) [1, 21] and propagation characteristics (PC) [7] have been studied to measure the local properties of Boolean functions. These properties are closely related to diffusion. In order to study the global properties of a Boolean function, an another criterion: global avalanche characteristics (GAC) has been introduced by Zhang and Zheng [16]. Further, the lower/upper bounds on the two indicators: the sum-of-squares indicator σ_f ($2^{2n} \leq \sigma_f \leq 2^{3n}$) and the absolute indicator $\triangle_f$ ($0 \leq \triangle_f \leq 2^n$) also derived in the same article [16]. The lower bounds on these two indicators for balanced Boolean functions are studied in [14] by Son et al. In order to measure the global avalanche characteristics between any two Boolean functions, a new criterion: the global avalanche characteristics of two Boolean functions (including the sum-of-squares indicator $\sigma_{f,g}$ and the absolute indicator $\triangle_{f,g}$) has been proposed by Zhou et al. [18]. The tight lower and the tight upper bounds on the two indicators: $0 \leq \triangle_{f,g} \leq 2^n$, $(|\mathcal{C}_{f,g}(\mathbf{0})|^2 \leq \sigma_{f,g} \leq 2^{3n})$ also derived in the same article.

A subclass of q-ary bent functions with optimal values of $\sigma_{f,g}$ and $\triangle_{f,g}$ is identified in Maiorana-McFarland class by Singh et al. [13, Thm. 4.4]. It is also demonstrated in the same article that $\sigma_{f,g} = q^{2n}$ if f is q-ary bent, the general bounds for SSMI and MI are presented. The SSMI of a q-ary s-plateaued function $f \in \mathcal{B}_{n,q}$ is q^{2n+s} [**?**]. Even the study on the relationship among σ_g, σ_f and $\sigma_{f,g}$ relationships of the sum-of-squares indicator between a q-ary function and the decomposition q-ary functions, etc is still open problem. Thus, based on the above discussion, the following questions raised:

a) What relationship exists among σ_f, σ_g and $\sigma_{f,g}$ for any two q-ary functions f, g?
b) What is a bound on σ_f, and what is the link between σ_f and σ_{f_ℓ} ($\ell \in \mathbb{Z}_q$), where $f = f_0||f_1|| \dots ||f_{q-1}$?
c) What is a construction method of balanced q-ary functions with good cryptographic properties ?

This article present some new bounds on the two indicators: $\sigma_{f,g}$ and $\triangle_{f,g}$. The relationship among $\sigma_{f,g}$, σ_f and σ_g is also presented.Based on the above result we obtain a bound on σ_f of $f \in \mathcal{B}_{n,q}$ in terms of σ'_{f_ℓ}s of the restricted functions on $\mathbb{Z}_{n-1}^q$, and construct a class of q-ary bent functions from 1-plateaued functions having dijoint Walsh spectra.

2 Basic definitions and notations

Let $\mathbb{Z}_q$ denote the ring of integers modulo q. A *q-ary function* is a function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ and $\mathcal{B}_{n,q}$ denotes the set of all such functions. Particularly, $\mathcal{B}_{n,2} = \mathcal{B}_n$ (for $q = 2$) denotes the set of classical Boolean functions on n variables. The Walsh Hadamard transform (WHT) of $f \in \mathcal{B}_{n,q}$ is a complex-valued function $\mathcal{H}_f : \mathbb{Z}_q^n \to \mathbb{C}$ defined as

$$\mathcal{H}_f(\mathbf{u}) = \frac{1}{q^{n/2}} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})+\langle \mathbf{x},\mathbf{u}\rangle}, \tag{2.1}$$

where $\langle \mathbf{x},\ \mathbf{u}\rangle$ denotes the usual inner product in $\mathbb{Z}_q^n$. It can be deduced that $\max\{|\mathcal{H}_f(\mathbf{u})| : \mathbf{u} \in \mathbb{Z}_q^n\} \geq 1$ for all $f \in \mathcal{B}_{n,q}$. The set of values $\{\mathcal{H}_f(\mathbf{u}) : \mathbf{u} \in \mathbb{Z}_q^n\}$ is referred to as the Walsh Hadamard spectrum (WHS) of the function f, which satisfies the Parseval's identity [6]:

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{H}_f(\mathbf{u})|^2 = q^n. \tag{2.2}$$

The q-ary functions with low absolute values of Walsh-Hadamard coefficients are of special interest in cryptography and coding theory and have many applications in different type of cryptosystems [6, 8, 11]. Kumar et al. [6] introduced the generalization of the notion classical *bent* Boolean function [8] and referred it as q-ary bent function. The q-ary function having "flat" WHS, in absolute, is said to be q-ary bent function. A function $f \in \mathcal{B}_{n,q}$ is q-ary bent if $|\mathcal{H}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$ [6, 15]. Alternatively, f is q-ary bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$ [6, 13]. A function $f \in \mathcal{B}_{n,q}$ is said to be q-ary m-plateaued if and and only if $|\mathcal{H}_f(\mathbf{u})| = \{0, q^{\frac{m}{2}}\}$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. The q-ary bent functions can be constructed using q-ary m-plateaued functions [2, 3].

The sum

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \zeta^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})} \tag{2.3}$$

is said to be cross-correlation between $f, g \in \mathcal{B}_{n,q}$ at $\mathbf{u}$. In particular, for $f = g$ the sum $\mathcal{C}_{f,f}(\mathbf{u}) = \mathcal{C}_f(\mathbf{u})$ is said to be autocorrelation of f at $\mathbf{u}$. Recently, two indicators: the *sum-of-squares-modulus indicator* (SSMI) $\sigma_{f,g}$ and the *modulus indicator*(MI) $\triangle_{f,g}$ between two q-ary functions $f, g \in \mathcal{B}_{n,q}$ [13] are defined by

$$\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|^2, \text{ and } \triangle_{f,g} = \max_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|. \tag{2.4}$$

In particular, the SSMI σ_f and MI $\triangle_f$ of a function $f \in \mathcal{B}_{n,q}$ is defined by

$$\sigma_f = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_f(\mathbf{u})|^2, \text{ and } \triangle_f = \max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{\mathbf{0}\}} |\mathcal{C}_f(\mathbf{u})|. \tag{2.5}$$

Further analysis their properties are also discussed in the same article.

In the following corollary, we summarise the properties discussed in [13, **?**] which we use to deduce our results.

Corollary 1. *[13] If $f, g \in \mathcal{B}_{n,q}$, then*

(a) $\sum_{\mathbf{e}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{e})\ \xi^{<-\mathbf{e},\ \mathbf{y}>} = q^n\mathcal{H}_f(\mathbf{y})\overline{\mathcal{H}_g(\mathbf{y})}$; *and* $\mathcal{C}_{f,g}(\mathbf{e}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{H}_f(\mathbf{y})\overline{\mathcal{H}_g(\mathbf{y})}\ \ \xi^{<\mathbf{e},\ \mathbf{y}>}$.

(b) $\mathcal{C}_f(\mathbf{e}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} |\mathcal{H}_f(\mathbf{y})|^2\, \xi^{<\mathbf{e},\mathbf{y}>}$; *and* $\sum_{\mathbf{e}\in\mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{e})\ \xi^{<-\mathbf{e},\ \mathbf{y}>} = q^n\, |\mathcal{H}_f(\mathbf{y})|^2$.

Corollary 2. *[?] If $f, g \in \mathcal{B}_{n,q}$ and $\mathbf{v} \in \mathbb{Z}_q^n$, then*

(a) $\sum_{\mathbf{a}\in\mathbb{Z}_q^n} C_f(\mathbf{a})\overline{C_g(\mathbf{a})}\xi^{\langle \mathbf{a},\mathbf{v}\rangle} = q^n \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mid \mathcal{H}_f(\mathbf{u}) \mid^2 \mid \mathcal{H}_g(\mathbf{u}+\mathbf{v}) \mid^2$.

(b) $\sigma_{f,g} = q^n \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mid \mathcal{H}_f(\mathbf{u}) \mid^2 \mid \mathcal{H}_g(\mathbf{u}) \mid^2$; *and* $\sigma_f = q^n \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mid \mathcal{H}_f(\mathbf{u}) \mid^4$.

3 The new Bounds on $\sigma_{f,g}$ and $\delta_{f,g}$

The proof of [20, Theorem 3.2] is obtained for $q = 2$ is very complicated. We provide an alternative proof of the generalization of [20, Theorem 3.2] for q-ary functions in the following

Theorem 1. *Let $f, g \in \mathcal{B}_{n,q}$, then*

$$\sigma_{f,g} \leq \sqrt{\sigma_f \sigma_g}. \tag{3.1}$$

Proof. Let $f, g \in \mathcal{B}_{n,q}$. Since the Cauchy-Schwarz inequality for any two vectors $\mathbf{x} = (x_1, x_2, \dots, x_n), \mathbf{y} = (y_1, y_2, \dots, y_n) \in \mathbb{R}^n$ states that

$$\sum_{i=1}^{n} x_i y_i \leq \left(\sum_{i=1}^{n} x_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} x_i^2\right)^{\frac{1}{2}} \tag{3.2}$$

Therefore,

$$\begin{aligned} \sigma_{f,g} &= \sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{H}_f(\mathbf{u})|^2 |\mathcal{H}_g(\mathbf{u})|^2 \\ &\leq \left[\sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{H}_f(\mathbf{u})|^4\right]^{\frac{1}{2}} \left[\sum_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{H}_g(\mathbf{u})|^4\right]^{\frac{1}{2}} = \sqrt{\sigma_f \sigma_g}. \end{aligned} \tag{3.3}$$

Further, the inequality $\sqrt{ab} \leq \frac{a+b}{2}$ holds for any two positive real number a, b. Hence we have Corollary 3 below, is the generalization of Theorem 1 of [19] (obtained for $q = 2$).

Corollary 3. *Let $f, g \in \mathcal{B}_{n,q}$, then*

$$0 \leq \sigma_{f,g} \leq \frac{\sigma_f + \sigma_g}{2}. \tag{3.4}$$

Let us define $f_{\mathbf{v}}(x_{n-r}, \dots, x_1) = f(x_n = v_r, \dots, x_{n-r+1} = v_1, x_{n-r}, \dots, x_1)$ for any $\mathbf{v} = (v_r, \dots, v_1)$. The following results is obtained by Singh et al [13]

Lemma 1. *[13, Lemma 3.1] If $\mathbf{u} \in \mathbb{Z}_q^r$, $\mathbf{w} \in \mathbb{Z}_q^{n-r}$ and $f \in \mathcal{B}_{n,q}$, then autocorrelation of f at $\mathbf{uv}$ is given by*

$$\mathcal{C}_f(\mathbf{uw}) = \sum_{\mathbf{v} \in \mathbb{Z}_q^r} \mathcal{C}_{f_{\mathbf{v}}, f_{\mathbf{v} \oplus \mathbf{u}}}(\mathbf{w}),$$

where $\mathbf{uw}$ is the vector concatenation of $\mathbf{u} = (u_r, \dots, u_1) \in \mathbb{Z}_q^r$ and $\mathbf{w} = (w_{n-r}, \dots, w_1) \in \mathbb{Z}_q^{n-r}$ defined by $\mathbf{uw} = (\mathbf{u}, \mathbf{w}) = (u_r, \dots, u_1, w_{n-r}, \dots, w_1)$.

In the following theorem, we provide a relationship among σ_f of $f \in \mathcal{B}_{n,q}$ and their restrictions (decomposition q-ary functions) $f_\ell \in \mathcal{B}_{n-1,q}, \ell \in \{0, 1, \dots, q-1\}$.

Theorem 2. *Let $f_\ell \in \mathcal{B}_{n-1,q}$ $(\ell = 0, 1, \dots, q-1)$, and if a q-ary function $f : \mathbb{Z}_q \times \mathbb{Z}_q^{n-1} \to \mathbb{Z}_q$ is expressed by $f = f_0 || f_1 || \dots || f_{q-1}$, i.e.,*

$$f(\mathbf{x}, x_n) = f_{x_n}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{Z}_n^q, x_n \in \mathbb{Z}_q. \tag{3.5}$$

Then

$$\sigma_f = \sigma_{f_0} + \sigma_{f_1} + \dots + \sigma_{f_{q-1}} + 4 \sum_{0=i<j<q} \sigma_{f_i, f_j}, \tag{3.6}$$

whenever $\sum_{\mathbf{w} \in \mathbb{Z}_q^{n-1}} \mathcal{C}_{f_i, f_j}(\mathbf{w}) \overline{\mathcal{C}_{f_k, f_l}(\mathbf{w})} = 0$ for all $i, j, k, l \in \mathbb{Z}_q$ such that $i \neq k$ and $j \neq l$.

Proof. It is evident that $\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|^2 = \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{v})\overline{\mathcal{C}_g(\mathbf{v})}$ for all $f, g \in \mathcal{B}_{n,q}$, see [13, Cor. 4.6]. Let $f_\ell \in \mathcal{B}_{n-1,q}$ $(\ell = 0, 1, \ldots, q-1)$ such that $\sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \mathcal{C}_{f_i,f_j}(\mathbf{w})\overline{\mathcal{C}_{f_k,f_l}(\mathbf{w})} = 0$ for all $i, j, k, l \in \mathbb{Z}_q$ such that $i \neq k$ and $j \neq l$, then

$$\begin{aligned}
\sigma_f &= \sum_{u\in\mathbb{Z}_q} \sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} |\mathcal{C}_f(u\mathbf{w})|^2 = \sum_{u\in\mathbb{Z}_q} \sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \left(\sum_{\ell\in\mathbb{Z}_q} \mathcal{C}_{f_\ell,f_{\ell+u}}(\mathbf{w})\right) \overline{\left(\sum_{z\in\mathbb{Z}_q} \mathcal{C}_{f_z,f_{z+u}}(\mathbf{w})\right)} \\
&= \sum_{\ell\in\mathbb{Z}_q} \sum_{z\in\mathbb{Z}_q} \left(\sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \mathcal{C}_{f_\ell}(\mathbf{w})\overline{\mathcal{C}_{f_z}(\mathbf{w})} + \sum_{u\neq 0} \sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \mathcal{C}_{f_\ell,f_{\ell+u}}(\mathbf{w})\overline{\mathcal{C}_{f_z,f_{z+u}}(\mathbf{w})}\right) \\
&= \sum_{\ell\in\mathbb{Z}_q} \sum_{z\in\mathbb{Z}_q} \sigma_{f_\ell,f_z} + \sum_{u\neq 0} \sum_{\ell\in\mathbb{Z}_q} \sum_{z\in\mathbb{Z}_q} \left(\sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \mathcal{C}_{f_\ell,f_{\ell+u}}(\mathbf{w})\overline{\mathcal{C}_{f_z,f_{z+u}}(\mathbf{w})}\right) \\
&= \sum_{i=0}^{q-1} \sigma_{f_i} + 2 \sum_{0=i<j<q} \sigma_{f_i,f_j} + \sum_{u\neq 0} \sum_{\ell\in\mathbb{Z}_q} \left(\sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \left|\mathcal{C}_{f_\ell,f_{\ell+u}}(\mathbf{w})\right|^2\right) \qquad (3.7) \\
&\qquad + \sum_{u\neq 0} \sum_{\ell\neq z, z\in\mathbb{Z}_q} \left(\sum_{\mathbf{w}\in\mathbb{Z}_q^{n-1}} \mathcal{C}_{f_\ell,f_{\ell+u}}(\mathbf{w})\overline{\mathcal{C}_{f_z,f_{z+u}}(\mathbf{w})}\right) \\
&= \sum_{i=0}^{q-1} \sigma_{f_i} + 2 \sum_{0=i<j<q} \sigma_{f_i,f_j} + \sum_{u\neq 0} \sum_{\ell\in\mathbb{Z}_q} \sigma_{f_\ell,f_{\ell+u}} \\
&= \sum_{i=0}^{q-1} \sigma_{f_i} + 4 \sum_{0=i<j<q} \sigma_{f_i,f_j},
\end{aligned}$$

which completes the proof.

It is to be noted that the smaller value of σ_f (i.e., for better GAC) of f correspond to low values of the autocorrelation spectrum of f [16]. From Theorem 2 it is evident that the decomposition of q-ary function is important to construct q-ary functions with good GAC. Two functions $f, g \in \mathcal{B}_{n,q}$ are said to be perfectly uncorrelated if $\mathcal{C}_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$. Further, if $\mathcal{H}_f(\mathbf{u})\mathcal{H}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$ for all $\mathbf{u} \in \mathbb{Z}_q^n$, then f, g are said to be q-ary functions with disjoint WHS. It can be seen that two functions with disjoint WHS are always perfectly uncorrelated. These properties are widely used in binary case to construct highly nonlinear balance Boolean functions with good GAC, see [10] and the references therein. The following results are consequence of Theorem 2

Corollary 4. *Let f be a q-ary function as defined in* (3.5)*, then*

1. $\sigma_f = \sigma_{f_0} + \sigma_{f_1} + \ldots + \sigma_{f_{q-1}}$ *if and only if f_i, f_j are perfectly uncorrelated for all $i \neq j$, $i, j \in \{0, 1, \ldots, q-1\}$.*
2. $\sum_{i=0}^{q-1} \sigma_{f_i} \leq \sigma_f \leq \sum_{i=0}^{q-1} \sigma_{f_i} + 4\sum_{0=i<j<q} \sigma_{f_i,f_j}$.

Thus, the concatenated function have minimum SSMI if their decomposition q-ary functions are pairwise perfectly uncorrelated. The following are some constructions of q-ary functions smaller values for σ_f and $\triangle_f$.

Lemma 2. *Let ℓ be a non negative integer and $\mathbf{z}_\ell \in \mathbb{Z}_q^m$ be any fixed vector. Define a q-ary function f_ℓ : $\mathbb{Z}_q^{n-m} \times \mathbb{Z}_q^m \to \mathbb{Z}_q$ by*

$$f_\ell(\mathbf{x}, \mathbf{y}) = g_\ell(\mathbf{x}) + \langle \mathbf{z}_\ell, \mathbf{y}\rangle \text{ for all } \mathbf{x} \in \mathbb{Z}_q^{n-m}, \mathbf{y} \in \mathbb{Z}_q^m, \qquad (3.8)$$

where $g_{\mathbf{z}_\ell} \in \mathcal{B}_{n-m,q}$. Then

(a) $|\mathcal{H}_{f_\ell}(\mathbf{u}, \mathbf{v})| = q^{\frac{m}{2}}\mathcal{H}_{g_\ell}(\mathbf{u})\delta_{\mathbf{0}}(\mathbf{z} + \mathbf{v})$*, where $\delta_{\mathbf{0}}(\mathbf{u}) = 0$ if $\mathbf{u} \neq \mathbf{0}$ and $\delta_{\mathbf{0}}(\mathbf{0}) = 1$.*

(b) $\mathcal{H}_{f_1}(\mathbf{u},\mathbf{v})\mathcal{H}_{f_2}(\mathbf{u},\mathbf{v}) = 0$ *for all* $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^{n-m} \times \mathbb{Z}_q^m$*, whenever* $\mathbf{z}_1 \neq \mathbf{z}_2$*,*

(c) $\sigma_{f_\ell} = q^{3m}\sigma_{g_\ell}$*,*

(d) If $g_{\mathbf{z}_\ell}$ *is a q-ary bent, then* $\sigma_{f_\ell} = q^{2n+m}$ *and* $|\mathcal{H}_{f_\ell}(\mathbf{u},\mathbf{v})| = q^{\frac{m}{2}}\delta_{\mathbf{0}}(\mathbf{z}+\mathbf{v})$*, that is,* f_ℓ *is m-plateaued q-ary function.*

Proof. Let $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^{n-m} \times \mathbb{Z}_q^m$. Then,

$$\begin{aligned}\mathcal{H}_{f_\ell}(\mathbf{u},\mathbf{v}) &= \frac{1}{q^{\frac{n}{2}}} \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{Z}_q^{n-m}\times\mathbb{Z}_q^m} \zeta^{f_\ell(\mathbf{x},\mathbf{y})+\langle\mathbf{u},\mathbf{x}\rangle+\langle\mathbf{v},\mathbf{y}\rangle} \\ &= \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_q^{n-m}} \zeta^{g_\ell(\mathbf{x})+\langle\mathbf{u},\mathbf{x}\rangle} \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \zeta^{\langle\mathbf{z}_\ell+\mathbf{v},\mathbf{y}\rangle} = q^{\frac{m}{2}}\mathcal{H}_{g_\ell}(\mathbf{u})\delta_{\mathbf{0}}(\mathbf{v}+\mathbf{z}_\ell)\end{aligned} \tag{3.9}$$

Part (b) follows from the property $\delta_{\mathbf{0}}(\mathbf{x})\delta_{\mathbf{0}}(\mathbf{y}) = 0$ if $\mathbf{x} \neq \mathbf{y}$ and part (a).

Now, using (3.9), we have

$$\begin{aligned}\sigma_{f_\ell} &= q^n \sum_{(\mathbf{u},\mathbf{v})\in\mathbb{Z}_q^{n-m}\times\mathbb{Z}_q^m} |\mathcal{H}_{f_\ell}(\mathbf{u},\mathbf{v})|^4 \\ &= q^n \sum_{\mathbf{u}\in\mathbb{Z}_q^{n-m}} \sum_{\mathbf{v}\in\mathbb{Z}_q^m} \left(q^{\frac{m}{2}}\right)^4 |\mathcal{H}_{g_\ell}(\mathbf{u})|^4 \delta_{\mathbf{0}}(\mathbf{v}+\mathbf{z}_\ell) = q^{n+2m} \sum_{\mathbf{u}\in\mathbb{Z}_q^{n-m}} |\mathcal{H}_{g_\ell}(\mathbf{u})|^4 = q^{3m}\sigma_{g_\ell}.\end{aligned}$$

Further, if g_ℓ q-ary is bent, then $\sigma_{g_\ell} = q^{2(n-m)}$ and $|\mathcal{H}_{g_\ell}(\mathbf{u})| = 1$ for all $\mathbf{u}$. Hence part (d) follows from part (a) and (c).

The following is the construction of $(m-1)$-plateaued q-ary function in $n+1$ variables by m-plateaued q-ary function in n variables.

Construction 1. Let $t = n+1$, $\mathbf{z}_\ell \in \mathbb{Z}_q^m$ for $\ell \in \{0,1,\ldots,q-1\}$ such that $\mathbf{z}_i \neq \mathbf{z}_j$ for all $i \neq j$. Define a q-ary function $f : \mathbb{Z}_q^{n-m} \times \mathbb{Z}_q^m \times \mathbb{Z}_q \to \mathbb{Z}_q$ by

$$f(\mathbf{x},\mathbf{y},x_t) = f_{x_t}(\mathbf{x},\mathbf{y}), \tag{3.10}$$

where f_ℓ are q-ary m-plateaued functions as constructed in (3.8). Then f is $(m-1)$-plateaued.

Theorem 3. *Let* $f \in \mathcal{B}_{t,q}$ *as defined in Construction* 1*, then* $\sigma_f = q^{2t-(m-1)}$*, that is* f *is* $(m-1)$*-plateaued q-ary function.*

Proof. Since $\mathcal{H}_{f_i}(\mathbf{u},\mathbf{v})\mathcal{H}_{f_j}(\mathbf{u},\mathbf{v}) = 0$ for $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^{n-m} \times \mathbb{Z}_q^m$ whenever $i \neq j$ and $i,j \in \{0,1,\ldots,q-1\}$. This implies that $\mathcal{C}_{f_i,f_j}(\mathbf{u},\mathbf{v}) = 0$ for all $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_q^{n-m} \times \mathbb{Z}_q^m$, that is f_i, f_j are perfectly uncorrelated for all $i \neq j$. Hence by using Corollary 4

$$\sigma_f = q^{2n+m+1} = q^{2t+(m-1)}, \tag{3.11}$$

which completes the proof.

4 Conclusion

The article presents an upper bound on the two indicators: $\sigma_{f,g}$ and $\triangle_{f,g}$ of two q-ary functions f and g. A relationship among $\sigma_{f,g}$, σ_f and σ_g is also presented. Based on the above result we obtain a bound on σ_f of $f \in \mathcal{B}_{n,q}$ in terms of σ_{f_ℓ}'s of the restricted functions on $\mathbb{Z}_{n-1}^q$, and construct a class of q-ary bent functions from 1-plateaued functions having dijoint Walsh spectra.

References

1. C. M. Adams and S. E. Tavers, Generating and counting binary bent sequences, IEEE Trans. Inform. Theory 36 (5) (1990) 1170-1173.
2. A. Çeşmelioğlu and W. Meidl, Bent functions of maximal degree, IEEE Trans. Inform. Theory, 58 (2) (2012), pp. 1186-1190.
3. A. Çeşmelioğlu and W. Meidl, A construction of bent functions from plateaued functions, Des. Codes Cryptogr., 66 (2013), pp. 231-242.
4. T. Helleseth, P. V. Kumar, Sequences with Low Correlation, In Handbook of Coding Theory, North-Holland, Amsterdam, (1998), pp. 1765-1853.
5. X. Hou, q-ary bent functions constructed from chain rings, Finite Fields and Applications, 4 (1998), pp. 55-61.
6. P. V. Kumar, R. A. Scholtz, L. R. Welch, Generalized bent functions and their properties, Journal of Combinatoirial Theory, Ser. A 1(40) (1985), pp. 90-107.
7. B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandewalle, Propagation characteristics of Boolean functions, in Advances in Cryptology-Eurocrypt'90, LNCS 437 Springer (1991) 155-165.
8. O. S. Rothaus, On bent functions, J. Combin. Theory, Ser. A 20 (1976) 300-305.
9. P. Sarkar and S. Maitra, Constructions of nonlinear Boolean functions with important cryptographic properties, In Advances in Cryptology-Eurocrypt 2000, LNCS 1807, Springer (2008) 485-506.
10. P. Sarkar and S. Maitra, Cross-correlation analysis of cryptographically useful Boolean functions, Theory of Computing Systems 35 (2002) 39-57.
11. K-U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA, IEEE Trans. on Inform. Theory, 55 (4)(2009) 1824-1832.
12. C. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28 (1949) 656-715.
13. D. Singh, M. Bhaintwal, B. K. Singh, Some results on q-ary bent functions, Int. J. Comput. Math. DOI:10.1080/00207160.2013.766330.
14. J.J. Son, J. I. Lim, S. Chee and S. H. Sung, Global avalanche characteristics and nonlinearity of balanced Boolean functions, Inform. Proc. Lett. 65 (1998) 139-144.
15. N. Tokareva, Generalizations of bent functions: A survey, J. Appl. Indust. Math. 5(1) (2011) 110-129.
16. X. M. Zhang and Y. Zheng, GAC-The criterion for global acalanche criteria of cryptographic functions, J. Uni. Comput. Sci. 1(5) (1995) 316-333.
17. Y. Zheng and X. M. Zhang, Relationship between bent functions and complementary plateaued functions, LNCS 1787 (1999) 60-75.
18. Y. Zhou, M. Xie and G. Xiao, On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Inform. Sci. 180 (2010) 256-265.
19. Y. Zhou, X. Dong, W. Zhang and B. Zeng, New bounds on the sum-of-squares indicator, 7th International Conference on Communications and Networking, CHINACOM-2012 China, 173-178.
20. Y. Zhou, W. Zhang, S. Zhu and G. Xiao, The global avalanche characteristics of two Boolean functions and algebraic immunity, Int. J. Comput. Math. 89(16) (2012) 2165-2179.
21. A. F. Webster, Plaintext/ciphertext bit dependencies in cryptographic systems, Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Canada, 1985.