Some properties of q-ary functions based on spectral analysis

Deep Singh* and Maheshanand Bhaintwal

Department of Mathematics,
Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
deepsinghspn@gmail.com,mahesfma@iitr.ernet.in

Abstract

In this paper, we generalize some existing results on Boolean functions to the q-ary functions defined over $\mathbb{Z}_q$, where $q \geq 2$ is an integer, and obtain some new characterization of q-ary functions based on spectral analysis. We provide a relationship between Walsh-Hadamard spectra of two p-ary functions f and g (for p a prime) and their derivative $D_{f,g}$. We provide a relationship between the Walsh-Hadamard spectra and the decompositions of any two p-ary functions. Further, we investigate a relationship between the Walsh-Hadamard spectra and the autocorrelation of any two q-ary functions.

Key words: Boolean functions; q-ary functions; Walsh-Hadamard spectrum; Crosscorrelation

1 Introduction

In recent years, the Walsh-Hadamard spectrum has become an important tool for research in cryptography, especially in the design and characterization of cryptographically significant Boolean functions used in various type of cryptosystems. Xiao and Massey [14] have provided some results on spectrum characterization of correlation immune functions. Sarkar and Maitra [7] have generalized these results and showed that the Walsh-Hadamard spectrum of an n-variable, m correlation immune function is divisible by 2^{m+1}. Recently, Sarkar and Maitra [8], and Zhou et al. [16] have provided some interesting results based on spectral analysis of Boolean functions.

A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function. Several authors have proposed various generalizations of Boolean functions and have analyzed the effect of the Walsh-Hadamard spectrum on them. Kumar et al. [5] have generalized the notion of classical bent functions by considering functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $q \geq 2$ and n are positive integers. These functions are also known as q-ary functions [12]. The q-ary functions are of special interest in cryptography and coding theory. According to Siegenthaler [10], it is not possible to construct an n-variable Boolean function with algebraic degree more than one and correlation immunity $n-1$, whereas it is possible to construct such q-ary functions. For example, the function $f(\mathbf{x}, \mathbf{y}) = \mathbf{x} + \mathbf{y}^3$ from $\mathbb{Z}_5^2$ to $\mathbb{Z}_5$ has algebraic degree 3 and correlation immunity 1. Thus, the q-ary functions can achieve better cryptographic bounds than Boolean functions.

The additive group $\mathbb{Z}_q$, the ring of integers modulo q, is isomorphic to $\mathbb{U}_q = \{1, \xi, \ldots, \xi^{q-1}\}$, the multiplicative group of complex q^{th} roots of unity. We denote the set of all q-ary functions by $\mathcal{B}_{n,q}$. The Walsh-Hadamard spectrum of any $f \in \mathcal{B}_{n,q}$ is a complex-valued function from $\mathbb{Z}_q^n$ to $\mathbb{C}$, the set of complex numbers, and defined as follows

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) + <\mathbf{x}, \mathbf{u}>},$$

where $< \mathbf{x},\ \mathbf{u} >$ denotes the usual inner product in $\mathbb{Z}_q^n$.

* Research supported by NBHM (DAE), INDIA.

A function $f \in \mathcal{B}_{n,q}$ is *generalized bent* (or *q-ary bent*) if $|\mathcal{W}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$. The Boolean *bent* functions were introduced by Rothaus [6]. It is to be noted that the generalized bent functions exist for every value of q and n, except when n is odd and $q = 2$ mod 4, whereas Boolean bent functions exist only for even n [5]. For more results on q-ary bent functions we refer to [1–4, 13]. Generalized bent functions are widely applicable in Code-Division Multiple-Access (CDMA) communications systems [9].

The *derivative* of $f, g \in \mathcal{B}_{n,q}$ at $\mathbf{a} \in \mathbb{Z}_q^n$ is defined as $D_{f,g}(\mathbf{a}) = f(\mathbf{x}) - g(\mathbf{x}+\mathbf{a})$, and for $f = g$, $D_f(\mathbf{a}) = f(\mathbf{x}) - f(\mathbf{x}+\mathbf{a})$ is called derivative of f at $\mathbf{a} \in \mathbb{Z}_q^n$.

Let $f, g \in \mathcal{B}_{n,q}$. Then the sum

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

is called the *cross-correlation* between the function f and g at $\alpha \in \mathbb{Z}_q^n$. Moreover, for $f = g$, the sum $\mathcal{C}_{f,f}(\alpha) = \mathcal{C}_f(\alpha)$ is called the *autocorrelation* of f at α.

The *sum-of-squares-of-modulus indicator* (SSMI) [11] of $f, g \in \mathcal{B}_{n,q}$ is defined as

$$\sigma_{f,g} = \sum_{\alpha \in \mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\alpha)|^2,$$

and in particular, for $f = g$, the sum-of-squares-of-modulus indicator (SSMI) [11] of $f \in \mathcal{B}_{n,q}$ is defined as

$$\sigma_f = \sum_{\alpha \in \mathbb{Z}_q^n} |\mathcal{C}_f(\alpha)|^2.$$

The following result is an important property and is extensively used in the paper.

Lemma 1. *[11, Lemma 2.1] Let $\alpha \in \mathbb{Z}_q^n$. Then*

$$\sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{<\alpha,\, \mathbf{x}>} = \begin{cases} q^n, & \text{if } \alpha = 0, \\ 0, & \text{otherwise} \,. \end{cases} \tag{1}$$

The following Lemma provides a relationship between the crosscorrelation and the autocorrelation of $f, g \in \mathcal{B}_{n,q}$.

Lemma 2. *[11, Corollary 3] Let $f, g \in \mathcal{B}_{n,q}$. Then*

$$\sigma_{f,g} = \sum_{\alpha \in \mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\alpha)|^2 = \sum_{\mathbf{a} \in \mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{a})\overline{\mathcal{C}_g(\mathbf{a})}.$$

2 Main Results

In the following Lemma, we generalize a result of Sarkar and Maitra [8, Corollary 3.3] (obtained for $p = 2$) to the p-ary functions, where p is a prime. Further, in Theorem 1 we provide a relationship between Walsh-Hadamard spectra of the derivative $D_{f,g}(\mathbf{a})$ and $f, g \in \mathcal{B}_{n,p}$. This result is a generalization of [15, Theorem 1].

Throughout the paper p is considered to be a prime.

Lemma 3. *Let $f, g, h \in \mathcal{B}_{n,p}$ such that $h(\mathbf{x}) = f(\mathbf{x}) - g(\mathbf{x})$. Then*

$$\mathcal{W}_h(\beta) = \frac{1}{p^n} \sum_{\alpha \in \mathbb{Z}_p^n} \mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)},\ \forall\ \beta \in \mathbb{Z}_p^n.$$

Proof. Using Lemma 1, for any $\beta \in \mathbb{Z}_p^n$, we have

$$\begin{aligned}\sum_{\alpha\in\mathbb{Z}_p^n} \mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)} &= \sum_{\alpha\in\mathbb{Z}_p^n}\sum_{\mathbf{x}\in\mathbb{Z}_p^n} \xi^{f(\mathbf{x})+<\alpha+\beta,\mathbf{x}>} \sum_{\mathbf{y}\in\mathbb{Z}_p^n} \xi^{-g(\mathbf{y})-<\alpha,\mathbf{y}>} \\ &= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_p^n} \xi^{f(\mathbf{x})-g(\mathbf{y})+<\beta,\mathbf{x}>} \sum_{\alpha\in\mathbb{Z}_p^n} \xi^{<\alpha,\mathbf{x}-\mathbf{y}>} \\ &= p^n \sum_{\mathbf{x}\in\mathbb{Z}_p^n} \xi^{f(\mathbf{x})-g(\mathbf{x})+<\beta,\mathbf{x}>} = p^n \sum_{\mathbf{x}\in\mathbb{Z}_p^n} \xi^{h(\mathbf{x})+<\beta,\mathbf{x}>} \\ &= p^n \mathcal{W}_h(\beta).\end{aligned} \tag{2}$$

This completes the proof.

Theorem 1. *Let $f, g \in \mathcal{B}_{n,p}$ and $\beta \in \mathbb{Z}_p^n$. Then*

$$\mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta) = \frac{1}{p^n}\sum_{\alpha\in\mathbb{Z}_p^n} \xi^{<\alpha,\mathbf{e}>}\mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)}, \quad \textit{and} \tag{3}$$

$$\mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)} = \sum_{\mathbf{e}\in\mathbb{Z}_p^n} \xi^{-<\alpha,\mathbf{e}>}\mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta). \tag{4}$$

Proof. Let $g_{\mathbf{e}} = g(\mathbf{e}+\mathbf{x})$. Then we have

$$\mathcal{W}_{g_{\mathbf{e}}}(\alpha) = \xi^{-<\alpha,\mathbf{e}>}\mathcal{W}_g(\alpha). \tag{5}$$

From Lemma 3, replacing g by $g_{\mathbf{e}}$ and h by $D_{f,g}(\mathbf{e})$, we have

$$\mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta) = \frac{1}{p^n}\sum_{\alpha\in\mathbb{Z}_p^n} \mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_{g_{\mathbf{e}}}(\alpha)} \tag{6}$$

Combining equations (5) and (6), we obtain (3).

Now, from Lemma 1 and (3), we have

$$\begin{aligned}\sum_{\mathbf{e}\in\mathbb{Z}_p^n} \xi^{-<\alpha,\mathbf{e}>}\mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta) &= \sum_{\mathbf{e}\in\mathbb{Z}_p^n} \xi^{-<\alpha,\mathbf{e}>}\frac{1}{p^n}\sum_{\mathbf{x}\in\mathbb{Z}_p^n} \xi^{<\mathbf{x},\mathbf{e}>}\mathcal{W}_f(\mathbf{x}+\beta)\overline{\mathcal{W}_g(\mathbf{x})} \\ &= \frac{1}{p^n}\sum_{\mathbf{x}\in\mathbb{Z}_p^n} \mathcal{W}_f(\mathbf{x}+\beta)\overline{\mathcal{W}_g(\mathbf{x})}\sum_{\mathbf{e}\in\mathbb{Z}_p^n} \xi^{<\mathbf{e},\mathbf{x}-\alpha>} \\ &= \mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)}.\end{aligned} \tag{7}$$

In particular, if $f = g$ and $\beta = \mathbf{0}$ in (3), then we have the following corollary.

Corollary 1. *If $f \in \mathcal{B}_{n,p}$, then the autocorrelation of f is given by*

$$\mathcal{C}_f(\mathbf{e}) = \frac{1}{p^n}\sum_{\alpha\in\mathbb{Z}_p^n} \xi^{<\alpha,\mathbf{e}>}|\mathcal{W}_f(\alpha)|^2. \tag{8}$$

By putting $\mathbf{e} = \mathbf{0}$ in Corollary 1 we obtain

$$\sum_{\alpha\in\mathbb{Z}_p^n} |\mathcal{W}_f(\alpha)|^2 = p^{2n},$$

which is known as Parseval's identity in the generalized setup.

In Theorem 2 and Theorem 3 below, we generalize the results of Zhou et. al [16, Lemma 3 and Theorem 6] (obtained for $p = 2$) to the p-ary functions.

Theorem 2. *Let $f, g \in \mathcal{B}_{n,p}$, where p is a prime, and V be a subspace of $\mathbb{Z}_p^n$ with $\dim(V) = k$. Then for any $\beta \in \mathbb{Z}_p^n$, we have*

$$\sum_{\alpha \in V} \mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)} = p^k \sum_{\mathbf{e} \in V^\perp} \mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta),$$

where $V^\perp$ denotes the dual of V, i.e., $V^\perp = \{\mathbf{x} \in \mathbb{Z}_p^n : \forall \mathbf{y} \in V, \mathbf{x}\cdot\mathbf{y} = 0\}$.

Proof. From Theorem 1, we have

$$\begin{aligned}\sum_{\alpha \in V} \mathcal{W}_f(\alpha+\beta)\overline{\mathcal{W}_g(\alpha)} &= \sum_{\alpha \in V}\sum_{\mathbf{e}\in\mathbb{Z}_p^n} \xi^{-<\alpha,\mathbf{e}>}\mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta) \\ &= \sum_{\mathbf{e}\in\mathbb{Z}_p^n} \mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta)\sum_{\alpha\in V}\xi^{-<\alpha,\mathbf{e}>} \\ &= p^k \sum_{\mathbf{e}\in V^\perp}\mathcal{W}_{D_{f,g}(\mathbf{e})}(\beta).\end{aligned}$$

In particular, if $f = g$, then we have the following corollary.

Corollary 2. *Let $f, g \in \mathcal{B}_{n,p}$ and V be the subspace of $\mathbb{Z}_p^n$ with $\dim(V) = k$. Then*

$$\sum_{\alpha\in V} |\mathcal{W}_f(\alpha+\beta)|^2 = p^k \sum_{\mathbf{e}\in V^\perp} \xi^{<\beta,\mathbf{e}>}\overline{\mathcal{W}_{D_f(\mathbf{e})}(\mathbf{0})},\ \forall\ \beta \in \mathbb{Z}_p^n.$$

Let W be a subspace of $\mathbb{Z}_p^n$ with $\dim(W) = k$. The *decomposition* of f with respect to W is the sequence $\{f_a : a \in V\}$, where V is a subspace such that $\mathbb{Z}_p^n$ is the direct sum of W and V, and f_a is the function of k variables from W to $\mathbb{Z}_p$, defined as $f_a(\mathbf{x}) = f(\mathbf{a}+\mathbf{x})$ for any $\mathbf{x} \in W$ [16]. In the following theorem, we investigate a relationship between the Walsh-Hadamard spectrum of $f, g \in \mathcal{B}_{n,p}$ and the Walsh-Hadamard spectrum of the decompositions of f and g with respect to a subspace V of $\mathbb{Z}_p^n$.

Theorem 3. *Let W be a subspace of $\mathbb{Z}_p^n$ with $\dim(W) = k$, and $\{f_a : a \in V\}$ and $\{g_a : a \in V\}$ be the decompositions of f and g with respect to W. Then*

$$\sum_{\alpha\in W^\perp} \mathcal{W}_f(\alpha)\overline{\mathcal{W}_g(\alpha)} = p^k \sum_{a\in V} \mathcal{W}_{f_a}(\mathbf{0})\overline{\mathcal{W}_{g_a}(\mathbf{0})}$$

Proof. For any $\mathbf{e} \in \mathbb{Z}_p^n$, we have

$$\mathcal{C}_{f,g}(\mathbf{e}) = \sum_{\mathbf{z}\in\mathbb{Z}_p^n} \xi^{f(\mathbf{z})-g(\mathbf{z}+\mathbf{e})} = \sum_{\mathbf{a}\in V}\sum_{\mathbf{x}\in W} \xi^{f_a(\mathbf{x})-g_a(\mathbf{x}+\mathbf{e})} = \sum_{\mathbf{a}\in V}\sum_{\mathbf{x}\in W}\xi^{f(\mathbf{a}+\mathbf{x})-g(\mathbf{a}+\mathbf{x}+\mathbf{e})}$$

From Theorem 2, for $\beta = \mathbf{0}$, we have

$$\begin{aligned}&\sum_{\alpha\in W^\perp} \mathcal{W}_f(\alpha)\overline{\mathcal{W}_g(\alpha)} = p^k\sum_{\mathbf{e}\in W}\mathcal{C}_{f,g}(\mathbf{e}) = p^k \sum_{\mathbf{e}\in W}\left(\sum_{\mathbf{z}\in\mathbb{Z}_p^n}\xi^{f(\mathbf{z})-g(\mathbf{z}+\mathbf{e})}\right) \\ &= p^k\sum_{\mathbf{e}\in W}\left(\sum_{\mathbf{a}\in V}\sum_{\mathbf{x}\in W}\xi^{f(\mathbf{a}+\mathbf{x})-g(\mathbf{a}+\mathbf{x}+\mathbf{e})}\right) = p^k\sum_{\mathbf{a}\in V}\sum_{\mathbf{x}\in W}\xi^{f(\mathbf{a}+\mathbf{x})}\sum_{\mathbf{e}\in W}\xi^{-g(\mathbf{a}+\mathbf{x}+\mathbf{e})} \\ &= p^k\sum_{\mathbf{a}\in V}\sum_{\mathbf{x}\in W}\xi^{f(\mathbf{a}+\mathbf{x})}\sum_{\mathbf{y}\in W}\xi^{-g(\mathbf{a}+\mathbf{y})} = p^k\sum_{\mathbf{a}\in V}\mathcal{W}_{f_a}(\mathbf{0})\overline{\mathcal{W}_{g_a}(\mathbf{0})}.\end{aligned} \tag{9}$$

In particular, if $f = g$, then we have the following corollary.

Corollary 3. *Let W be a subspace of $\mathbb{Z}_p^n$ of dimension k and $\{f_a : a \in V\}$ be the decomposition of f with respect to W. Then*

$$\sum_{\alpha \in W^\perp} |\mathcal{W}_f(\alpha)|^2 = p^{\frac{2k-n}{2}} \sum_{\mathbf{a} \in V} |\mathcal{W}_{f_a}(\mathbf{0})|^2.$$

For any $\alpha \in \mathbb{Z}_q^n$, where $q \geq 2$ is any integer, we have

$$| W_f(\alpha) |^2 = \sum_{a \in \mathbb{Z}_q^n} \xi^{<\mathbf{a},\alpha>} \overline{C_f(a)} = \sum_{a \in \mathbb{Z}_q^n} \xi^{<-a,\alpha>} C_f(a). \tag{10}$$

In particular, if $\alpha = 0$ then

$$| W_f(0) |^2 = \sum_{a \in \mathbb{Z}_q^n} C_f(a).$$

In the following theorem, we provide a relationship between the Walsh-Hadamard spectrum and the autocorrelation of any two q-ary functions.

Theorem 4. *Let $f, g \in \mathcal{B}_{n,q}$. Then for any $\beta \in \mathbb{Z}_q^n$, we have*

$$\sum_{\alpha \in \mathbb{Z}_q^n} | W_f(\alpha) |^2 | W_g(\alpha + \beta) |^2 = q^n \sum_{a \in \mathbb{Z}_q^n} C_f(a) \overline{C_g(a)} \xi^{<a,\beta>}. \tag{11}$$

Proof. From (10), for any $\beta \in \mathbb{Z}_q^n$, we have

$$\begin{aligned}
\sum_{\alpha \in \mathbb{Z}_q^n} | W_f(\alpha) |^2 | W_g(\alpha + \beta) |^2 &= \sum_{\alpha \in \mathbb{Z}_q^n} \sum_{a \in \mathbb{Z}_q^n} \xi^{<-a,\alpha>} C_f(a) \sum_{b \in \mathbb{Z}_q^n} \xi^{<b,\alpha+\beta>} \overline{C_g(b)} \\
&= \sum_{\alpha \in \mathbb{Z}_q^n} \sum_{a \in \mathbb{Z}_q^n} \sum_{b \in \mathbb{Z}_q^n} C_f(a) \overline{C_g(b)} \xi^{<-a+b,\alpha>+<b,\beta>} \\
&= \sum_{a \in \mathbb{Z}_q^n} \sum_{b \in \mathbb{Z}_q^n} C_f(a) \overline{C_g(b)} \xi^{<b,\beta>} \sum_{\alpha \in \mathbb{Z}_q^n} \xi^{<-a+b,\alpha>} \\
&= q^n \sum_{a \in \mathbb{Z}_q^n} C_f(a) \overline{C_g(a)} \xi^{<a,\beta>}
\end{aligned}$$

In particular, if $f = g$, then we have the following corollary.

Corollary 4. *Let $f \in \mathcal{B}_{n,q}$. Then for any $\beta \in \mathbb{Z}_q^n$, we have*

$$\sum_{\alpha \in \mathbb{Z}_q^n} | W_f(\alpha) |^2 | W_f(\alpha + \beta) |^2 = q^n \sum_{a \in \mathbb{Z}_q^n} | C_f(a) |^2 \xi^{<a,\beta>}. \tag{12}$$

Further, if $\beta = 0$, then

$$\sum_{\alpha \in \mathbb{Z}_q^n} | W_f(\alpha) |^4 = q^n \sum_{a \in \mathbb{Z}_q^n} | C_f(a) |^2 = q^n \sigma_f.$$

If $\beta = 0$ in (11), then by using Lemma 2 we obtain the following corollary which appears in [11, Theorem 6 (a)].

Corollary 5. *Let $f, g \in \mathcal{B}_{n,q}$. Then*

$$\sigma_{f,g} = \frac{1}{q^n} \sum_{\alpha \in \mathbb{Z}_q^n} | W_f(\alpha) |^2 | W_g(\alpha) |^2 .$$

A function $f \in \mathcal{B}_{n,q}$ is called *q-ary semi-bent* if for any $\mathbf{a} \in \mathbb{Z}_q^n$ (i) $\mid W_f(\mathbf{a}) \mid \in \{0, q^{\frac{n+1}{2}}\}$ for odd n, and (ii) $\mid W_f(\mathbf{a}) \mid \in \{0, q^{\frac{n+2}{2}}\}$ for even n.

Theorem 5. *Let $f_1 \in \mathcal{B}_{r,q}$ and $f_2 \in \mathcal{B}_{s,q}$, where r and s are odd positive integers. Then a function $f \in \mathcal{B}_{r+s,q}$ expressed as*

$$f(x_{r+s}, \ldots, x_{r+1}, x_r, \ldots, x_1) = f_1(x_r, \ldots, x_1) + f_2(x_{r+s}, \ldots, x_{r+1}),$$

is q-ary semi-bent if f_1 and f_2 both are q-ary semi-bent functions.

Proof. Let $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. We compute,

$$\begin{aligned}\mathcal{W}_f(\mathbf{u}, \mathbf{v}) &= \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s} \xi^{f(\mathbf{x},\mathbf{y}) + <\mathbf{u},\mathbf{x}> + <\mathbf{v},\mathbf{y}>} \\ &= \sum_{\mathbf{x} \in \mathbb{Z}_q^r} \xi^{f_1(\mathbf{x}) + <\mathbf{u},\mathbf{x}>} \sum_{\mathbf{y} \in \mathbb{Z}_q^s} \xi^{f_2(\mathbf{y}) + <\mathbf{v},\mathbf{y}>} = \mathcal{W}_{f_1}(\mathbf{u}) \mathcal{W}_{f_2}(\mathbf{v}).\end{aligned} \tag{13}$$

Since f_1 and f_2 both are q-ary semi-bent, therefore $|\mathcal{W}_{f_1}(\mathbf{u})| \in \{\mathbf{0}, q^{\frac{r+1}{2}}\}$ and $|\mathcal{W}_{f_2}(\mathbf{v})| \in \{\mathbf{0}, q^{\frac{s+1}{2}}\}$. This implies that $|\mathcal{W}_f(\mathbf{u}, \mathbf{v})| = |\mathcal{W}_{f_1}(\mathbf{u})||\mathcal{W}_{f_2}(\mathbf{v})| \in \{\mathbf{0}, q^{\frac{r+s+2}{2}}\}$, for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Hence f is q-ary semi-bent.

In the following theorem, we provide a relationship on crosscorrelation between two q-ary functions on $(n+1)$-variables in terms of their crosscorrelation on n-variables.

Theorem 6. *Let $f, g \in \mathcal{B}_{n+1,q}$ such that*

$$f(\mathbf{x}, x_{n+1}) = f_1(\mathbf{x}) + x_{n+1}, \quad g(\mathbf{x}, x_{n+1}) = g_1(\mathbf{x}) + x_{n+1},$$

where $f_1, g_1 \in \mathcal{B}_{n,q}$. Then the crosscorrelation between f and g is

$$\mathcal{C}_{f,g}(\mathbf{u}, u_{n+1}) = \xi^{-u_{n+1}} \mathcal{C}_{f_1,g_1}(\mathbf{u}).$$

Further, if $f \in \mathcal{B}_{n,q}$ is any bent function then the autocorrelation of f is given by

$$\mathcal{C}_f(\mathbf{u}, u_{n+1}) = \begin{cases} q^n, & \text{if } \mathbf{u} = 0, \\ 0, & \text{otherwise} . \end{cases}$$

Proof. We have

$$\begin{aligned}\mathcal{C}_{f,g}(\mathbf{u}, u_{n+1}) &= \sum_{\mathbf{x}, x_{n+1} \in \mathbb{Z}_q^n \times \mathbb{Z}_q} \xi^{f(\mathbf{x}, x_{n+1}) - g(\mathbf{x}+\mathbf{u}, x_{n+1}+u_{n+1})} \\ &= \sum_{\mathbf{x}, x_{n+1} \in \mathbb{Z}_q^n \times \mathbb{Z}_q} \xi^{f_1(\mathbf{x}) + x_{n+1} - g_1(\mathbf{x}+\mathbf{u}) - x_{n+1} - u_{n+1}} \\ &= \xi^{-u_{n+1}} \sum_{\mathbf{x}, x_{n+1} \in \mathbb{Z}_q^n \times \mathbb{Z}_q} \xi^{f_1(\mathbf{x}) - g_1(\mathbf{x}+\mathbf{u})} \\ &= \xi^{-u_{n+1}} \mathcal{C}_{f_1,g_1}(\mathbf{u}).\end{aligned} \tag{14}$$

Hence, $|\mathcal{C}_{f,g}(\mathbf{u}, u_{n+1})| = |\mathcal{C}_{f_1,g_1}(\mathbf{u})|$. The second part follows from (14) by setting $f = g$ (that is, $f_1 = g_1$).

3 Acknowledgement

The work of the first author was supported by NBHM (DAE), INDIA.

References

1. Carlet, C., Dubuc, S.: On generalized bent and q-ary perfect nonlinear functions, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications, Proceedings of Fq5, Springer, Berlin, 81-94 (2000).
2. Hou, X.: q-ary bent functions constructed from chain rings. Finite Fields and Applications 4, 55-61 (1998).
3. Hou, X.: Bent functions, partial difference sets, and quasi-Frobenius rings. Designs, Codes and Cryptography 20, 251-268 (2000).
4. Hou, X.: p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields and Applications 10, 566-582 (2004).
5. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. Journal of Combinatirial Theory, Ser. A 1(40), 90-107 (1985).
6. Rothaus, O.S.: On bent functions. Journal of Combinatorial Theory 20, 300-305 (1976).
7. Sarkar, P., Maitra, S.: Constructions of nonlinear Boolean functions with important cryptographic properties. In Advances in Cryptology-Eurocrypt 2000, LNCS 1807, 485-506, (2000).
8. Sarkar, P., Maitra, S.: Cross-correlation analysis of cryptographically useful Boolean functions. Theory of Computing Systems 35, 39-57 (2002).
9. Schmidt, K-U.: Quaternary constant-amplitude codes for multicode CDMA. IEEE Transactions on Information Theory 55 (4), 1824-1832 (2009).
10. Siegenthaler, T.: Correlation immunity of nonlinear combining functions for cryptographic applications. IEEE Transactions on Information Theory, 30, 776-780 (1984).
11. Singh, D., Bhaintwal, M., Singh, B. K.: Some results on q-ary bent functions. Cryptology ePrint Archives, http://www.eprint.iacr.org/2012/037.pdf
12. Solé, P., Tokareva, N.: Connections between quaternary and binary bent functions. Cryptology ePrint Archives, http://www.eprint.iacr.org/2009/544.
13. Tokareva N.: Generalizations of bent functions: A survey. Cryptology ePrint Archives, http://eprint.iacr.org/2011/111.pdf
14. Xiao, G. Z., Messey, J. L.: A Spectral Characterization of Correlation-Immune Combing Functions. IEEE Transactions on Information Theory, 34(3): 569-571, (1988).
15. Zhuo, Z., Chong, J., Cao, H., Xiao, G.: Spectral analysis of two Boolean functions and their derivatives, Chinese Journal of Electronics 20 (4), 747-749, (2011).
16. Zhou, G., Xie, M., Xiao, G.: On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Information Sciences 180, 256-265, (2010).