Some results on q-ary bent functions

Deep Singh*, Maheshanand Bhaintwal and Brajesh Kumar Singh

Department of Mathematics,
Indian Institute of Technology Roorkee, Roorkee 247667 INDIA
deepsinghspn@gmail.com,mahesfma@iitr.ernet.in,bksingh0584@gmail.com

Abstract

Kumar et al.(1985) have extended the notion of classical bent Boolean functions in the generalized setup on $\mathbb{Z}_q^n$. They have provided an analogue of classical Maiorana-McFarland type bent functions. In this paper, we study the crosscorrelation of a subclass of such generalized Maiorana-McFarland (GMMF) type bent functions. We provide a construction of quaternary ($q = 4$) bent functions on $n + 1$ variables in terms of their subfunctions on n-variables. Analogues of sum-of-squares indicator and absolute indicator of crosscorrelation of Boolean functions are defined in the generalized setup. Further, q-ary functions are studied in terms of these indictors and some upper bounds of these indicators are obtained. Finally, we provide some constructions of balanced quaternary functions with high nonlinearity under Lee metric.

Key words: q-ary bent functions; Walsh-Hadamard transform; Parseval's identity; GMMF type bent functions; Crosscorrelation

1 Introduction

Let $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ denote the set of integers, real numbers and complex numbers, respectively, and let $\mathbb{Z}_q$ denote ring of integers modulo q. The additive group $\mathbb{Z}_q$ is isomorphic to $\mathbb{U}_q = \{1, \xi, \ldots, \xi^{q-1}\}$, the multiplicative group of complex q^{th} roots of unity. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function. Recently, several generalizations of Boolean functions have been proposed by several authors and effect of Walsh-Hadamard transform on them has been studied. The classical *bent* functions were introduced by Rothaus [8]. For an excellent survey on existing generalizations of bent functions we refer to [13]. Kumar et al. [6] have generalized the notion of classical bent functions by considering functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, where $q \geq 2$ is any positive integer. Let $\mathcal{B}_{n,q}$ denote the set of such generalized q-ary functions.

The Walsh-Hadamard transform of $f \in \mathcal{B}_{n,q}$ is a complex-valued function from $\mathbb{Z}_q^n$ to $\mathbb{C}$ defined as follows

$$\mathcal{W}_f(\mathbf{u}) = \frac{1}{q^{\frac{n}{2}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \xi^{f(\mathbf{x}) + <\mathbf{x}, \mathbf{u}>},$$

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

A function $f \in \mathcal{B}_{n,q}$ is generalized bent (or q-ary bent) if $|\mathcal{W}_f(\mathbf{u})| = 1$ for every $\mathbf{u} \in \mathbb{Z}_q^n$. It has been proved in [6] that 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. Kumar et al. [6] have provided an analogue of classical Maiorana-McFarland class of bent functions in the generalized setup and discussed several properties of these functions. For more results on q-ary bent functions we refer to [1–4]. Generalized bent functions are widely applicable in Code-Division Multiple-Access (CDMA) communications systems [10]. Solé and Tokareva have investigated systematically the links between Boolean bent functions [8], generalized bent Boolean functions [12], and quaternary bent functions [6]. Recently, Zadda and Parraud [5] have introduced the notion of balancedness and nonlinearity for quaternary functions.

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

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

* Research supported by NBHM (DAE), INDIA.

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

It follows from Shannon's basic design principles *confusion and diffusion* [11] of secret key cryptosystems, that the constituent Boolean functions of secret key system should have low crosscorrelation and certain uniformity properties. Recently, Sarkar and Maitra [9], and Zhou et al. [14] have reported some interesting results in this direction. Zhou et al. [14] have introduced two new indicators: sum-of-squares indicator and the absolute indicator. These two indicators of crosscorrelation between two Boolean functions are called the global avalanche characteristics (GAC) between them. Analogous to these two indicators, we define two similar indicators: sum-of-squares-of-modulus indicator (SSMI) and modulus indicator (MI) of crosscorrelation between two functions in the generalized setup.

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

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

and the modulus indicator (MI) of $f, g \in \mathcal{B}_{n,q}$ is defined as

$$\triangle_{f,g} = \max_{\mathbf{u} \in \mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|.$$

The (periodic) crosscorrelation of sequences is relevant to CDMA applications. Kumar et al. [7] have introduced a large family of quaternary sequences with low correlation.

1.1 Preliminaries on quaternary functions

In this section, we discuss some basic results on quaternary functions.

The *support* of function $f \in \mathcal{B}_{n,4}$ is defined as $Supp(f) = \{u \in \mathbb{Z}_4^n : \ f(u) \neq 0\}$. Further, the *relative support* of f is defined as $Supp_j(f) = \{u \in \mathbb{Z}_4^n : f(u) = j\}$ for all $j \in \mathbb{Z}_4$ and $\eta_j(f)$ denotes the size of $Supp_j(f)$. A function $f \in \mathcal{B}_{n,4}$ is *balanced* if and only if for all $j \in \mathbb{Z}_4$, $\eta_j = 4^{n-1}$. The Hamming weight $w_H(f)$ of f is the size of its support i.e., $\eta_1(f)+\eta_2(f)+\eta_3(f)$ and the Hamming distance between two functions $f, g \in \mathcal{B}_{n,4}$ is defined by $d_H(f, g) = w_H(f - g)$. The Lee weights w_L of $0, 1, 2, 3$ in $\mathbb{Z}_4$ are $0, 1, 2, 1$ respectively and the Lee weight $w_L(u)$ of an element $u \in \mathbb{Z}_4^n$ is the rational sum of the Lee weight of its components. The Lee distance $d_L(u, v)$ between two elements $u, v \in \mathbb{Z}_4^n$ is $w_L(u + v)$. The Lee weight $w_L(f)$ of $f \in \mathcal{B}_{n,4}$ is $\eta_1(f) + 2\eta_2(f) + \eta_3(f)$ and the Lee distance between two functions $f, g \in \mathcal{B}_{n,4}$ is defined by $d_L(f, g) = w_L(f - g)$. Define $\mathcal{W}_f^2(\mathbf{u}) = \frac{1}{2^n} \sum_{\mathbf{x} \in \mathbb{Z}_4^n} (-1)^{f(\mathbf{x}) + <\mathbf{x},\mathbf{u}>}$.

Definition 1. *Let $\mathcal{A}_{n,4}$ be set of all affine functions in $\mathcal{B}_{n,4}$. The nonlinearity of $f \in \mathcal{B}_{n,4}$ is defined as $nl_4^H(f) = \min_{g \in \mathcal{A}_{n,4}} d_H(f, g)$ under Hamming metric and $nl_4^L(f) = \min_{g \in \mathcal{A}_{n,4}} d_L(f, g)$ under Lee metric.*

A function $f \in \mathcal{B}_{n,4}$ is quaternary bent if and only if $|\mathcal{W}_f(\mathbf{u})| = 1$, i.e., $\mathcal{W}_f(\mathbf{u}) \in \{\pm 1, \pm \imath\}$ for all $\mathbf{u} \in \mathbb{Z}_4^n$.

The following proposition is [5, Proposition 3] in terms of normalized Wlash-Hadamard transform.

Proposition 1. *The nonlinearity of $f \in \mathcal{B}_{n,4}$ under Lee metric is given by*

$$\begin{aligned} nl_4^L(f) &= 4^n - 2^n \max_{\mathbf{u} \in \mathbb{Z}_4^n, \beta \in \mathbb{Z}_4} \{Re[\imath^\beta \mathcal{W}_F(\mathbf{u})]\} \\ &= 4^n - 2^n \max_{\mathbf{u} \in \mathbb{Z}_4^n} \{|Re[\mathcal{W}_F(\mathbf{u})]|, |Im[\mathcal{W}_F(\mathbf{u})]|\}, \end{aligned}$$

where $Re[z]$ and $Im[z]$ respectively denote the real and imaginary part of the complex number z.

Proposition 2. *[5, Theorem 2] Let $f \in \mathcal{B}_{n,4}$ be quaternary bent. Then*

$$nl_4^L(f) = 4^n - 2^n.$$

Proposition 3. *[5, Proposition 1] A function $f \in \mathcal{B}_{n,4}$ is balanced if and only if $\mathcal{W}_f(\mathbf{0}) = \mathcal{W}_f^2(\mathbf{0}) = 0$.*

2 Properties of Walsh-Hadamard transform in the generalized setup

Lemma 1. *Let n be a positive integer and $\mathbf{u} \in \mathbb{Z}_q^n$, then*

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

Proof. Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ and $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ be in $\mathbb{Z}_q^n$. Then

$$\begin{aligned} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{<\mathbf{u},\ \mathbf{x}>} &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{u_1x_1+u_2x_2+\ldots+u_nx_n} = \prod_{i=1}^{n} \sum_{x_i\in\mathbb{Z}_q} \xi^{u_ix_i} \\ &= \prod_{i=1}^{n} \left(\frac{1-(\xi^{u_i})^q}{1-\xi^{u_i}} \right) = \begin{cases} q^n, & \text{if } u_i = 0, \forall i = 1, \ldots, n, \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Theorem 1. *If $f, g \in \mathcal{B}_{n,q}$ and $\mathbf{u}, \mathbf{y} \in \mathbb{Z}_q^n$, then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\ \xi^{<\mathbf{u},\ \mathbf{y}>} = q^n \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}, \text{ and}$$

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}\ \xi^{<-\mathbf{u},\ \mathbf{y}>}.$$

Proof. The cross-correlation between f and g is

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

Therefore, using Lemma 1, we have

$$\begin{aligned} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\xi^{<\mathbf{u},\ \mathbf{y}>} &= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})+<\mathbf{u},\ \mathbf{y}>} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{x}+\mathbf{u})+<\mathbf{u},\ \mathbf{y}>} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{u})+<\mathbf{x}-\mathbf{u},\ \mathbf{y}>} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})+<\mathbf{x},\ \mathbf{y}>} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-(g(\mathbf{u})+<\mathbf{u},\ \mathbf{y}>)} \\ &= q^n \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}. \end{aligned}$$

Therefore,

$$\begin{aligned} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}\xi^{<-\mathbf{u},\ \mathbf{y}>} &= \frac{1}{q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{v})\xi^{<\mathbf{v},\ \mathbf{y}>+<-\mathbf{u},\ \mathbf{y}>} \\ &= \frac{1}{q^n} \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{v}) \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{<\mathbf{v}-\mathbf{u},\ \mathbf{y}>} \\ &= \mathcal{C}_{f,g}(\mathbf{u}). \end{aligned}$$

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

Corollary 1. *Let f be a q-ary function on $\mathbb{Z}_q^n$ then the autocorrelation of f is given as*

$$\mathcal{C}_f(\mathbf{x}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{y})|^2 \xi^{-<\mathbf{x},\ \mathbf{y}>}.$$

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

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{y})|^2 = q^n,$$

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

The following corollary is due to Kumar et al. [6, Property 4]. An alternative proof of this result follows from Lemma 1 and Corollary 1.

Corollary 2. *A function $f \in \mathcal{B}_{n,q}$ is q-ary bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{0\}$.*

3 Characterizations of q-ary bent functions

Let $\mathbf{v} = (v_r, \ldots, v_1)$. We define

$$f_{\mathbf{v}}(x_{n-r}, \ldots, x_1) = f(x_n = v_r, \ldots, x_{n-r+1} = v_1, x_{n-r}, \ldots, x_1).$$

For any $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_q^r$ and $\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{Z}_q^{n-r}$, we define the vector concatenation $\mathbf{uw}$ as

$$\mathbf{uw} = (\mathbf{u}, \mathbf{w}) = (u_r, \ldots, u_1, w_{n-r}, \ldots, w_1).$$

Lemma 2. *Let $\mathbf{u} \in \mathbb{Z}_q^r$, $\mathbf{w} \in \mathbb{Z}_q^{n-r}$ and f be an n-variable generalized q-ary function on $\mathbb{Z}_q^n$. Then autocorrelation of f is given by*

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

Proof. We compute,

$$\begin{aligned}\mathcal{C}_f(\mathbf{uw}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{uw})} = \sum_{\mathbf{v}\in\mathbb{Z}_q^r}\sum_{\mathbf{z}\in\mathbb{Z}_q^{n-r}} \xi^{f(\mathbf{vz})-f(\mathbf{vz}+\mathbf{uw})} \\ &= \sum_{\mathbf{v}\in\mathbb{Z}_q^r}\sum_{\mathbf{z}\in\mathbb{Z}_q^{n-r}} \xi^{f_{\mathbf{v}}(\mathbf{z})-f_{\mathbf{v}+\mathbf{u}}(\mathbf{z}+\mathbf{w})} = \sum_{\mathbf{v}\in\mathbb{Z}_q^r} \mathcal{C}_{f_{\mathbf{v}}, f_{\mathbf{v}+\mathbf{u}}}(\mathbf{w}).\end{aligned}$$

Any two q-ary functions f and g are said to have *complementary autocorrelation* if and only if $\mathcal{C}_f(\mathbf{u}) + \mathcal{C}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$.

Theorem 2. *Any two generalized q-ary functions f and g on $\mathbb{Z}_q^n$ have complementary autocorrelation if and only if*

$$|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2 = q, \text{ for all } \mathbf{u} \in \mathbb{Z}_q^n.$$

Proof. Suppose f and g are two generalized q-ary functions on $\mathbb{Z}_q^n$ possess complimentary autocorrelation then

$$q^n(|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2) = \sum_{\mathbf{x}\in\mathbb{Z}_q^n} (\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}))\xi^{<\mathbf{u},\mathbf{x}>} = q^{n+1}.$$

Which implies, $|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2 = q$, for all $\mathbf{u} \in \mathbb{Z}_q^n$.

Conversely, suppose that $|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2 = q$, for all $\mathbf{u} \in \mathbb{Z}_q^n$. Then

$$\begin{aligned}\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}) &= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} (|\mathcal{W}_f(\mathbf{u})|^2 + |\mathcal{W}_g(\mathbf{u})|^2)\xi^{<\mathbf{u},\mathbf{x}>} \\ &= 2\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{<\mathbf{u},\mathbf{x}>} = 2^{n+1}\delta_{\mathbf{0}}(\mathbf{u}),\end{aligned}$$

and therefore, if $\mathbf{u} \neq 0$, then $\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}) = 0$. Therefore, f and g have complementary autocorrelation.

The following theorem is a slightly generalized version of Theorem 3 by Tokareva [13].

Theorem 3. *Let $f_1 \in \mathcal{B}_{r,q}$ and $f_2 \in \mathcal{B}_{s,q}$. Then a function $g \in \mathcal{B}_{r+s,q}$ expressed as*

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

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

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

$$\begin{aligned} \mathcal{W}_g(\mathbf{u}, \mathbf{v}) &= \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{Z}_4^r \times \mathbb{Z}_4^s} \imath^{g(\mathbf{x},\mathbf{y}) + <\mathbf{u},\mathbf{x}> + <\mathbf{v},\mathbf{y}>} \\ &= \sum_{\mathbf{x} \in \mathbb{Z}_4^r} \imath^{f_1(\mathbf{x}) + <\mathbf{u},\mathbf{x}>} \sum_{\mathbf{y} \in \mathbb{Z}_4^s} \imath^{f_2(\mathbf{y}) + <\mathbf{v},\mathbf{y}>} = \mathcal{W}_{f_1}(\mathbf{u}) \mathcal{W}_{f_2}(\mathbf{v}). \end{aligned} \tag{2}$$

Suppose f_1 and f_2 both are q-ary bent, then $|\mathcal{W}_{f_1}(\mathbf{u})| = 1$ and $|\mathcal{W}_{f_2}(\mathbf{v})| = 1$. This implies that , $|\mathcal{W}_g(\mathbf{u}, \mathbf{v})| = |\mathcal{W}_{f_1}(\mathbf{u})||\mathcal{W}_{f_2}(\mathbf{v})| = 1$, for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^r \times \mathbb{Z}_q^s$. Hence g is q-ary bent.

Conversely, we assume g is q-ary bent function, our aim is to show that the functions f_1 and f_2 are q-ary bent functions. Let us suppose that f_1 is not q-ary bent, then there exists $\mathbf{u} \in \mathbb{Z}_q^r$ such that $|\mathcal{W}_{f_1}(\mathbf{u})| > 1$. This implies that $|\mathcal{W}_{f_2}(\mathbf{v})| < 1$ for every $\mathbf{v} \in \mathbb{Z}_q^s$, as $1 = |\mathcal{W}_{f_1}(\mathbf{u})||\mathcal{W}_{f_2}(\mathbf{v})|$. This contradicts the fact that $\sum_{\mathbf{b} \in \mathbb{Z}_q^s} |\mathcal{W}_{f_2}(\mathbf{b})|^2 = q^s$.

3.1 Construction of quaternary bent functions in $\mathcal{B}_{n+1,4}$ from the functions in $\mathcal{B}_{n,4}$

Theorem 4. *Let n be a positive integer. A function $h \in \mathcal{B}_{n+1,4}$ expressed as*

$$h(x_{n+1}, x_n, \ldots, x_1) = (1 + x_{n+1}) f(x_n, \ldots, x_1) + x_{n+1} g(x_n, \ldots, x_1),$$

where $f, g \in \mathcal{B}_{n,4}$, is quaternary bent if and only if

(i) $|\sum_{j=0}^{3} \mathcal{W}_{h_j}(\mathbf{u})| = 2$, *for all* $\mathbf{u} \in \mathbb{Z}_4^n$.

(ii) $\frac{\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})} = \phi(\mathbf{u})$ *and* $\frac{\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})} = \imath\psi(\mathbf{u})$ *where* $\phi(\mathbf{u}), \psi(\mathbf{u}) \in \mathbb{R}$.

(iii) $\sum_{j=0}^{3} |\mathcal{W}_{h_j}(\mathbf{u})|^2 = 4$ *for all* $\mathbf{u} \in \mathbb{Z}_4^n$ *and*

$$\mathcal{W}_{h_0}(\mathbf{u})\overline{\mathcal{W}_{h_2}(\mathbf{u})} + \overline{\mathcal{W}_{h_0}(\mathbf{u})}\mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u})\overline{\mathcal{W}_{h_3}(\mathbf{u})} + \overline{\mathcal{W}_{h_1}(\mathbf{u})}\mathcal{W}_{h_3}(\mathbf{u}) = 0.$$

Proof. Let us identify $(x_{n+1}, x_n, \ldots, x_1) \in \mathbb{Z}_4^{n+1}$ with $(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. Suppose that the function

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

is quaternary bent. The Walsh-Hadamard transform of h at $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ is

$$\begin{aligned} \mathcal{W}_h(a, \mathbf{u}) &= \frac{1}{4^{\frac{n+1}{2}}} \sum_{(x_{n+1},\mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n} \imath^{h(x_{n+1},\mathbf{x}) + a x_{n+1} + <\mathbf{u},\ \mathbf{x}>} \\ &= \frac{1}{2^{n+1}} \sum_{j=0}^{3} \sum_{\mathbf{x} \in \mathbb{Z}_4^n} \imath^{h_j(\mathbf{x}) + aj + <\mathbf{u},\ \mathbf{x}>} = \frac{1}{2} \sum_{j=0}^{3} \imath^{aj} \mathcal{W}_{h_j}(\mathbf{u}) \\ &= \frac{1}{2}(\mathcal{W}_{h_0}(\mathbf{u}) + \imath^a \mathcal{W}_{h_1}(\mathbf{u}) + (-1)^a \mathcal{W}_{h_2}(\mathbf{u}) + (-\imath)^a \mathcal{W}_{h_3}(\mathbf{u})). \end{aligned} \tag{3}$$

Since h is quaternary bent, $|\mathcal{W}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. This implies that

$$|\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})| = 2. \tag{4}$$

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) + \imath(\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u}))| = 2. \tag{5}$$

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})| = 2. \tag{6}$$

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) - \imath(\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u}))| = 2. \tag{7}$$

Combining (4) and (6), we obtain

$$\frac{\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})} = -\overline{\left(\frac{\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})}\right)}, \text{provided} \quad \mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u}) \neq 0,$$

which implies that $\frac{\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})}$ is purely imaginary, i.e.,

$$\frac{\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})} = \imath\psi(\mathbf{u}), \text{where } \psi(\mathbf{u}) \in \mathbb{R}. \tag{8}$$

Similarly on combining (5) and (7), we obtain that

$$\frac{\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})}{\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})} = \phi(\mathbf{u}), \text{where } \phi(\mathbf{u}) \in \mathbb{R}. \tag{9}$$

Solving (5) and (9) we have

$$\begin{aligned} &|\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 \, |(\imath + \phi(\mathbf{u}))|^2 = 4 \\ i.e., \; &|\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 \left(1 + \frac{|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})|^2}{|\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2}\right) = 4 \\ i.e., \; &|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})|^2 + |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 = 4. \end{aligned} \tag{10}$$

Similarly, from (6) and (8), we have

$$|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})|^2 + |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 = 4. \tag{11}$$

On combining (10) and (11), we obtain

$$\mathcal{W}_{h_0}(\mathbf{u})\overline{\mathcal{W}_{h_2}(\mathbf{u})} + \overline{\mathcal{W}_{h_0}(\mathbf{u})}\mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u})\overline{\mathcal{W}_{h_3}(\mathbf{u})} + \overline{\mathcal{W}_{h_1}(\mathbf{u})}\mathcal{W}_{h_3}(\mathbf{u}) = 0. \tag{12}$$

Similarly, (11) and (12) provides $\sum_{j=0}^{3} |\mathcal{W}_{h_j}(\mathbf{u})|^2 = 4$.

Conversely, suppose that the conditions (i), (ii) and (iii) are true. Condition (ii) implies that the terms $\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})$ and $\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})$ (as well as $\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})$ and $\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})$) can not be zero simultaneously. Suppose $\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) = 0$ then $|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})| = 2$ (as well as, if $\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u}) = 0$ then $|\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})| = 2$). Now consider the case when neither $|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})| \, |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})| \neq 0$ nor $|\mathcal{W}_{h_0}(\mathbf{u}) + \mathcal{W}_{h_2}(\mathbf{u})| \, |\mathcal{W}_{h_1}(\mathbf{u}) + \mathcal{W}_{h_3}(\mathbf{u})| \neq 0$.

Let $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ be arbitrary. Condition (i) implies that $|\mathcal{W}_h(0, \mathbf{u})| = 1$.
Using condition (ii) and (iii) we have

$$\begin{aligned} 4 \; &|\mathcal{W}_h(1, \mathbf{u})|^2 = |\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u}) + \imath(\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u}))|^2 \\ &= |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 |\phi(\mathbf{u}) + \imath|^2 = |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2 \left(1 + \phi^2(\mathbf{u})\right) \\ &= \left(|\mathcal{W}_{h_0}(\mathbf{u}) - \mathcal{W}_{h_2}(\mathbf{u})|^2 + |\mathcal{W}_{h_1}(\mathbf{u}) - \mathcal{W}_{h_3}(\mathbf{u})|^2\right) = \sum_{j=1}^{3} |\mathcal{W}_{h_j}(\mathbf{u})|^2 \\ &- \left(\mathcal{W}_{h_0}(\mathbf{u})\overline{\mathcal{W}_{h_2}(\mathbf{u})} + \overline{\mathcal{W}_{h_0}(\mathbf{u})}\mathcal{W}_{h_2}(\mathbf{u}) + \mathcal{W}_{h_1}(\mathbf{u})\overline{\mathcal{W}_{h_3}(\mathbf{u})} + \overline{\mathcal{W}_{h_1}(\mathbf{u})}\mathcal{W}_{h_3}(\mathbf{u})\right) = 4, \end{aligned}$$

which implies that $|\mathcal{W}_h(1, \mathbf{u})| = 1$.

Similarly for $a = 2, 3$ we have from condition (ii) and (iii) that $|\mathcal{W}_h(a, \mathbf{u})| = 1$. Therefore, $|\mathcal{W}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$.

4 Two indicators of cross-correlation for q-ary functions

The following result for the binary case were shown in [14]. One can straightforwardly infer by modifying those results hold under the current notion, as well.

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

(1) $\triangle_{f,g} = 0$ *if and only if* $f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})$ *is balanced for any* $\mathbf{u} \in \mathbb{Z}_q^n$.
(2) $\triangle_{f,g} = q^n$ *if and only if* $f(\mathbf{x}) = g(\mathbf{x}+\mathbf{u}) + a$, $a \in \mathbb{Z}_q$ *for some* $\mathbf{u} \in \mathbb{Z}_q^n$.
(3) $0 \le \triangle_{f,g} \le q^n$.

Any two q-ary functions f and g are said to be *perfectly uncorrelated* [9] if $\mathcal{W}_f(\mathbf{u})\mathcal{W}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$.

Theorem 6. *Let $f, g \in \mathcal{B}_{n,q}$. Then*

(*a*) $|\mathcal{C}_{f,g}(0)|^2 \le \sigma_{f,g} \le q^{3n}$
(*b*) $\sigma_{f,g} = q^{3n}$ *if and only if f and g are affine functions.*
(*c*) $\sigma_{f,g} = |\mathcal{C}_{f,g}(0)|^2$ *if and only if f and g are either generalized bents or perfectly uncorrelated.*

Proof. (*a*) Using Theorem 1 and Cauchy inequality, $\left(\sum_i a_i b_i\right)^2 \le \sum_i a_i^2 \sum_i b_i^2$ for all $a_i, b_i \in \mathbb{R}$, we have

$$\begin{aligned}
\sigma_{f,g} &= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{f,g}(\mathbf{u})} \\
&= \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x})\overline{\mathcal{W}_g(\mathbf{x})}\xi^{<-\mathbf{u},\ \mathbf{x}>} \overline{\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{y})\overline{\mathcal{W}_g(\mathbf{y})}\xi^{<-\mathbf{u},\ \mathbf{y}>}} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{W}_f(\mathbf{x})\overline{\mathcal{W}_f(\mathbf{y})\mathcal{W}_g(\mathbf{x})}\mathcal{W}_g(\mathbf{y}) \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{<\mathbf{u},\ \mathbf{y}-\mathbf{x}>} \\
&= q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 |\mathcal{W}_g(\mathbf{x})|^2 \le q^n \left(\sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})\mathcal{W}_g(\mathbf{x})|\right)^2 \\
&\le q^n \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{x})|^2 \sum_{\mathbf{x}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{x})|^2 = q^{3n}
\end{aligned}$$

(*b*) From (*a*), we have $\sigma_{f,g} = q^{3n}$ if and only if

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{u})|^2 = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_g(\mathbf{u})|^2$$

That is, $\sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}_q^n\ \mathbf{u}\neq\mathbf{v}} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{v})|^2 = 0$ if and only if $|\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{v})|^2 = 0$ for any $\mathbf{u} \neq \mathbf{v}$.

If $|\mathcal{W}_f(\mathbf{u})|^2 = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$ then it contradicts the Parseval's identity. Therefore $|\mathcal{W}_f(\mathbf{u}_0)|^2 \neq 0$ for at least one $\mathbf{u}_0 \in \mathbb{Z}_q^n$. Consider the following cases:

(1) If there exist only one $\mathbf{u}_0 \in \mathbb{Z}_q^n$ such that $|\mathcal{W}_f(\mathbf{u}_0)|^2 \neq 0$ then $|\mathcal{W}_g(\mathbf{v})|^2 = 0$ for all $\mathbf{v} \in \mathbb{Z}_q^n$ except $\mathbf{v} \neq \mathbf{u}_0$. By Parseval identity, we have $|\mathcal{W}_f(\mathbf{u}_0)|^2 = q^n$ which implies that $f(x) = a - < \mathbf{u}_0, \mathbf{x} >$ for some $a \in \mathbb{Z}_q$. On the other hand, since $|\mathcal{W}_g(\mathbf{v})|^2 = 0$ for any $\mathbf{v} \neq \mathbf{u}_0$, implies $|\mathcal{W}_g(\mathbf{u}_0)|^2 = q^n$. That is $g(x) = b - < \mathbf{u}_0, \mathbf{x} >$ for some $b \in \mathbb{Z}_q$. Thus f and g are affine.
(2) If there exist only two $\mathbf{u}_1, \mathbf{u}_2 \in \mathbb{Z}_q^n$ $(\mathbf{u}_1 \neq \mathbf{u}_2)$ such that $|\mathcal{W}_f(\mathbf{u}_1)|^2 \neq 0$ and $|\mathcal{W}_f(\mathbf{u}_2)|^2 \neq 0$, then $|\mathcal{W}_g(\mathbf{u})|^2 = 0$ for any $\mathbf{u} \neq \mathbf{u}_1$ and $|\mathcal{W}_g(\mathbf{u})|^2 = 0$ for any $\mathbf{u} \neq \mathbf{u}_2$ accordingly. That is, $|\mathcal{W}_g(\mathbf{u})|^2 = 0$ for all $\mathbf{u} \in \mathbb{Z}_q^n$ which contradicts Parseval's identity. Similarly, there does not exist only $k (3 \le k \le 2^n)$ distinct $\mathbf{u}_i \in \mathbb{Z}_q^n (1 \le i \le k)$ such that $|\mathcal{W}_f(\mathbf{u}_i)|^2 \neq 0$.

(c) $\sigma_{f,g} = (\triangle_{f,g}(0))^2$ if and only if

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})|^2 |\mathcal{W}_g(\mathbf{u})|^2 \sum_{\mathbf{u}\in\mathbb{Z}_q^n} 1^2 = \left(\sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{W}_f(\mathbf{u})\overline{\mathcal{W}_g(\mathbf{u})}| \times 1 \right)^2,$$

if and only if, by Cauchy-Schwarz's inequality, for any $\mathbf{u} \in \mathbb{Z}_q^n$, $\frac{\mathcal{W}_f(\mathbf{u})\overline{\mathcal{W}_g(\mathbf{u})}}{1} = \phi(\mathbf{u})$ such that $|\phi(\mathbf{u})| = k$, a positive real number. There are two cases:

(1) If $k = 0$, then f and g are perfectly uncorrelated.
(2) If $k \neq 0$, then $|\mathcal{W}_f(\mathbf{u})\overline{\mathcal{W}_g(\mathbf{u})}| = |\mathcal{W}_f(\mathbf{v})||\overline{\mathcal{W}_g(\mathbf{v})}|$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$. This is equivalent to $\frac{|\mathcal{W}_f(\mathbf{u})|}{|\mathcal{W}_f(\mathbf{v})|} = \frac{|\mathcal{W}_g(\mathbf{v})|}{|\mathcal{W}_g(\mathbf{u})|} = t$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$, where t is positive real. That is, $|\mathcal{W}_f(\mathbf{u})| = t|\mathcal{W}_f(\mathbf{v})|$ and $|\mathcal{W}_g(\mathbf{v})| = t|\mathcal{W}_g(\mathbf{u})|$. Using Parseval's identity, we get $t^2 = 1$. Therefore, $|\mathcal{W}_f(\mathbf{u})|^2|$ and $|\mathcal{W}_g(\mathbf{u})|^2$ are constants for all $\mathbf{u} \in \mathbb{Z}_q^n$. Again by using Parseval's identity, we get $|\mathcal{W}_f(\mathbf{u})| = 1 = |\mathcal{W}_g(\mathbf{u})|$ for all $\mathbf{u} \in \mathbb{Z}_q^n$ which proves that f and g both are generalized bent.

4.1 Crosscorrelation of Maiorana-McFarland type q-ary bent functions

In this section we obtain crosscorrelation between two bent functions in a subclass of Maiorana-McFarland type q-ary bent functions.

Kumar et al. [6, Theorem 1] have given a natural generalization of the classical Maiorana McFarland construction. We provide here an alternative proof of this result.

Lemma 3. *[6, Theorem 1] Let $n = 2m$, where m is a positive integer. Then a function $f : \mathbb{Z}_q^m \times \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q$ expressed as*

$$f(\mathbf{x}, \mathbf{y}) =< \mathbf{x},\ \pi(\mathbf{y}) > + g(\mathbf{y}),$$

where $g : \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q$ is any q-ary function and $\pi : \mathbb{Z}_q^m \longrightarrow \mathbb{Z}_q^m$ be any permutation, is bent.

Proof. Let $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$. Using Lemma 1, we compute,

$$\begin{aligned}
\mathcal{W}_f(\mathbf{u}, \mathbf{v}) &= \frac{1}{q^m} \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \xi^{<\mathbf{x},\ \pi(\mathbf{y})>+g(\mathbf{y})+<\mathbf{u},\ \mathbf{x}>+<\mathbf{v},\ \mathbf{y}>} \\
&= \frac{1}{q^m} \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \xi^{g(\mathbf{y})+<\mathbf{v},\ \mathbf{y}>} \sum_{\mathbf{x}\ \in\mathbb{Z}_q^m} \xi^{<\pi(\mathbf{y})+\mathbf{u},\ \mathbf{x}>} \\
&= \xi^{g(\pi^{-1}(-u))+<\mathbf{v},\ \pi^{-1}(-u)>}
\end{aligned}$$

Thus $|\mathcal{W}_f(\mathbf{u}, \mathbf{v})| = 1$ for all $(\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$. This completes the proof.

Let $\mathcal{P}$ be the set of permutations on $\mathbb{Z}_q^m$ such that $\pi_1, \pi_2 \in \mathcal{P} \implies \pi_1^{-1} - \pi_2^{-1} \in \mathcal{P}$.

Theorem 7. *Let $n = 2m$, m a positive integer. Let f_1, f_2 be two q-ary Maiorana-McFarland type generalized bent function on $\mathbb{Z}_q^n$, i.e., $f_1(\mathbf{x}, \mathbf{y}) =< \mathbf{x},\ \pi_1(\mathbf{y}) > +g_1(\mathbf{y})$ and $f_2(\mathbf{x}, \mathbf{y}) =< \mathbf{x},\ \pi_2(\mathbf{y}) > +g_2(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^m$, where π_1, π_2 are permutations on $\mathbb{Z}_q^m$ and $g_1, g_2 \in \mathcal{B}_{m,q}$. If $\pi_1, \pi_2 \in \mathcal{P}$, then*

$$|\mathcal{C}_{f_1,f_2}(\mathbf{u}, \mathbf{v})| = q^m,\ \forall\ (\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m.$$

Proof. By Lemma 1 and Lemma 3, we have

$$\begin{aligned}
\mathcal{C}_{f_1,f_2}(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^m} \mathcal{W}_{f_1}(\mathbf{x},\mathbf{y})\overline{\mathcal{W}_{f_2}(\mathbf{x},\mathbf{y})}\xi^{<\mathbf{x},\ \mathbf{u}>+<\mathbf{y},\ \mathbf{v}>} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^m} (\xi^{g_1(\pi_1^{-1}(-\mathbf{x}))+<\mathbf{y},\ \pi_1^{-1}(-\mathbf{x})>})\overline{(\xi^{g_2(\pi_2^{-1}(-\mathbf{x}))+<\mathbf{y},\ \pi_2^{-1}(-\mathbf{x})>})}\xi^{<\mathbf{x},\ \mathbf{u}>+<\mathbf{y},\ \mathbf{v}>} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^m} \xi^{g_1(\pi_1^{-1}(-\mathbf{x}))+<\mathbf{y},\ \pi_1^{-1}(-\mathbf{x})>-g_2(\pi_2^{-1}(-\mathbf{x}))-<\mathbf{y},\ \pi_2^{-1}(-\mathbf{x})>+<\mathbf{x},\ \mathbf{u}>+<\mathbf{y},\ \mathbf{v}>} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \xi^{g_1(\pi_1^{-1}(-\mathbf{x}))-g_2(\pi_2^{-1}(-\mathbf{x}))+<\mathbf{x},\ \mathbf{u}>} \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \xi^{<\mathbf{y},\ \mathbf{v}+\pi_1^{-1}(-\mathbf{x})-\pi_2^{-1}(-\mathbf{x})>}. \\
&= q^m\xi^{g_1(\pi_1^{-1}(\pi_2^{-1}-\pi_1^{-1})^{-1}(\mathbf{v}))-g_2(\pi_2^{-1}(\pi_2^{-1}-\pi_1^{-1})^{-1}(\mathbf{v}))+<\mathbf{u},\ \mathbf{x}>}
\end{aligned}$$

This completes the proof.

It is to be noted that smaller values $\triangle_{f,g}$ and $\sigma_{f,g}$ correspond to low correlation between f and g. From Theorem 7 we have $\triangle_{f_1,f_2} = q^{2n}$ and $\sigma_{f_1,f_2} = q^m$. These bounds are much better than the trivial bounds obtained in Theorem 10 and 6.

4.2 Relationship among crosscorrelation of four q-ary functions

Zhuo [15] has established the relationship among crosscorrelation of four arbitrary Boolean functions. In the following results we provide an analogue of these results in the generalized setup.

Theorem 8. *Let $f, g, h, k \in \mathcal{B}_{n,q}$. Then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,k}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_{f,h}(\mathbf{a})\overline{\mathcal{C}_{g,k}(\mathbf{a}+\mathbf{e})},\ \forall \mathbf{e}\in\mathbb{Z}_q^n. \tag{13}$$

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

$$\begin{aligned}
&\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,k}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})}\overline{\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{h(\mathbf{y})-k(\mathbf{y}+\mathbf{u}+\mathbf{e})}} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-h(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \xi^{-g(\mathbf{x}+\mathbf{u})+k(\mathbf{y}+\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{x})-h(\mathbf{y})} \sum_{\lambda\in\mathbb{Z}_q^n} \xi^{-g(\lambda)+k(\mathbf{y}-\mathbf{x}+\lambda+\mathbf{e})} \\
&= \sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{y}-\mathbf{a})-h(\mathbf{y})} \sum_{\lambda\in\mathbb{Z}_q^n} \xi^{-g(\lambda)+k(\lambda+\mathbf{a}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{f(\mathbf{y})-h(\mathbf{y}+\mathbf{a})}\overline{\mathcal{C}_{g,k}(\mathbf{a}+\mathbf{e})} \\
&= \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_{f,h}(\mathbf{a})\overline{\mathcal{C}_{g,k}(\mathbf{a}+\mathbf{e})}
\end{aligned}$$

In particular, if we take $f = h$ and $g = k$, then we have the following result.

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

$$\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{f,g}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{a})\overline{\mathcal{C}_g(\mathbf{a}+\mathbf{e})}.$$

In particular, if $\mathbf{e} = \mathbf{0}$, then we have

$$\sigma_{f,g} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_f(\mathbf{a})\overline{\mathcal{C}_g(\mathbf{a})}. \tag{14}$$

Corollary 4. *Let $f, g \in \mathcal{B}_{n,q}$, then $\sigma_{f,g} \le q^{3n}$.*

Proof. The result follows from the fact that $\sigma_f \le q^{3n}$ and the Cauchy inequality in (14).

If $g = k$ in (13), then we have $\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,g}(\mathbf{u}+\mathbf{e})} = \sum_{\mathbf{a}\in\mathbb{Z}_q^n} \mathcal{C}_{f,h}(\mathbf{a})\overline{\mathcal{C}_g(\mathbf{a}+\mathbf{e})}$. Moreover, if g is q-ary bent, then we have the following proposition.

Proposition 4. *Let $f, g, h \in \mathcal{B}_{n,q}$ and g is q-ary bent, then*

(1) $\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,g}(\mathbf{u}+\mathbf{e})} = q^n\mathcal{C}_{f,h}(-\mathbf{e})\phi_{\{-\mathbf{e}\}}(\mathbf{a})$, *where* $\phi_{\{\mathbf{v}\}}(\mathbf{u}) = \begin{cases} 1, & \text{if } \mathbf{u} = \mathbf{v}, \\ 0, & \text{otherwise .} \end{cases}$
(2) $\sigma_{f,g} = q^{2n}$.
(3) *If $\mathbf{e} \neq 0$ and $f(\mathbf{x})$ is q-ary bent, then* $\sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,g}(\mathbf{u}+\mathbf{e})} = 0$.

Theorem 9. *Let $f, g \in \mathcal{B}_{n,q}$ such that g is q-ary bent, then*

$$\triangle_{f,g} \geq q^{n/2}, \text{ and}$$

$$\max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{\mathbf{0}\}} |\mathcal{C}_{f,g}(\mathbf{u})| \geq \sqrt{\frac{q^{2n} - |\mathcal{C}_{f,g}(0)|^2}{q^n - 1}}.$$

Proof. We have $\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{f,g}(\mathbf{u})|^2$. Thus, the absolute value of each $\mathcal{C}_{f,g}(\mathbf{u})$ will be minimum only when they all possess equal values. Therefore the minimum value of $\triangle_{f,g}$ is $\sqrt{\sigma_{f,g}/q^n}$. From property (2) of Proposition 4, we have $\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}^2(\mathbf{u}) = q^{2n}$. Since the sum on the left side has q^n non-negative terms, therefore $\triangle_{f,g} \geq \sqrt{q^{2n}/q^n} = q^{n/2}$.

Since $\sum_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{0\}} \mathcal{C}_{f,g}^2(\mathbf{u}) = q^{2n} - |\mathcal{C}_{f,g}(\mathbf{0})|^2$ and the sum on left side has $q^n - 1$ non-negative terms, therefore $\max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{0\}} |\mathcal{C}_{f,g}(\mathbf{u})| \geq \sqrt{\frac{q^{2n}-|\mathcal{C}_{f,g}(0)|^2}{q^n-1}}$.

Corollary 5. *Let $f, g \in \mathcal{B}_{n,q}$ such that g is q-ary bent. If $|\mathcal{C}_{f,g}(0)| < q^{n/2}$, then* $\max_{\mathbf{u}\in\mathbb{Z}_q^n\setminus\{0\}} |\mathcal{C}_{f,g}(\mathbf{u})| > q^{n/2}$.

5 Secondary constructions on quaternary balanced functions with five valued Walsh-Hadamard spectra

In this section, we construct some balanced quaternary functions with high nonlinearity under Lee metric.

Theorem 10. *Suppose $g \in \mathcal{B}_{n+1,4}$ is expressed as*

$$g(x_{n+1}, x_n, \ldots, x_1) = x_{n+1} + f(x_n, \ldots, x_1),$$

where $f \in \mathcal{B}_{n,4}$ be a quaternary bent. Then g is balanced and its nonlinearity under Lee metric is given by

$$nl_4^L(g) = 4^{n+1} - 2^{n+2}.$$

Proof. Let $\mathbf{x} = (x_n, \ldots, x_1) \in \mathbb{Z}_4^n$ and $j \in \mathbb{Z}_4$.

$$\begin{aligned} Supp_j(g) &= \{\mathbf{x}' = (x_{n+1}, \mathbf{x}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n | g(\mathbf{x}') = j\} \\ &= \{\mathbf{x} \in \mathbb{Z}_4^n, x_{n+1} \in \mathbb{Z}_4 | f(\mathbf{x}) + x_{n+1} = j\} \\ &= \cup_{l=0}^3 \{\mathbf{x} \in \mathbb{Z}_4^n | f(\mathbf{x}) = l = (j - x_{n+1}) \mod 4\} = \cup_{l=0}^3 Supp_l(f), \end{aligned}$$

implies that $\eta_j(g) = |\cup_{i=0}^3 Supp_i(f)| = \sum_{i=0}^3 \eta_i(f) = 4^n$ for all $j \in \mathbb{Z}_4$. Hence, g is balanced.

The Walsh-Hadamard transform of g at $(u_{n+1}, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$ is

$$\begin{aligned} \mathcal{W}_g(u_{n+1}, \mathbf{u}) &= \frac{1}{2^{n+1}} \sum_{(x_{n+1},\mathbf{x})\in\mathbb{Z}_4\times\mathbb{Z}_4^n} \imath^{g(x_{n+1},\mathbf{x})+<\mathbf{u},\mathbf{x}>+u_{n+1}x_{n+1}} \\ &= \frac{1}{2^{n+1}} \sum_{(x_{n+1},\mathbf{x})\in\mathbb{Z}_4\times\mathbb{Z}_4^n} \imath^{f(\mathbf{x})+<\mathbf{u},\mathbf{x}>+(u_{n+1}+1)x_{n+1}} \\ &= \frac{1}{2^{n+1}} \sum_{\mathbf{x}\in\mathbb{Z}_4^n} \imath^{f(\mathbf{x})+<\mathbf{u},\mathbf{x}>} \sum_{x_{n+1}\in\mathbb{Z}_4} \imath^{(u_{n+1}+1)x_{n+1}} \\ &= \begin{cases} 2\ \mathcal{W}_f(\mathbf{u}), & \text{if } u_{n+1} = 3, \\ 0, & \text{otherwise .} \end{cases} \end{aligned} \tag{15}$$

Since f is quaternary bent, therefore $\mathcal{W}_f(\mathbf{u}) \in \{\pm 1, \pm\imath\}$ for every $\mathbf{u} \in \mathbb{Z}_4^n$. Using (15), we have

$$\mathcal{W}_g(u_{n+1}, \mathbf{u}) = \begin{cases} \pm 2 \text{ or } \pm\imath\, 2, & \text{if } u_{n+1} = 3, \\ 0, & \text{otherwise .} \end{cases}$$

Thus the Walsh-Hadamard spectrum of g contains 5 distinct values from the set $\{\pm 2, \pm\imath 2, 0\}$ for every $(u_{n+1}, \mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n$. By Proposition 1, we have

$$\begin{aligned} nl_4^L(g) &= 4^{n+1} - 2^{n+1} \max_{(u_{n+1},\mathbf{u}) \in \mathbb{Z}_4 \times \mathbb{Z}_4^n} \{|Re[\mathcal{W}_g((u_{n+1}, \mathbf{u}))]|, |Im[\mathcal{W}_g((u_{n+1}, \mathbf{u}))]|\} \\ &= 4^{n+1} - 2^{n+2}. \end{aligned}$$

Remark 1. A function $g \in \mathcal{B}_{n+1,4}$ expressed as

$$g(x_{n+1}, x_n, \ldots, x_1) = x_{n+1} + f(x_n, \ldots, x_1),$$

where $f \in \mathcal{B}_{n,4}$, is balanced and its nonlinearity under Lee metric is

$$nl_4^L(g) = 4\ nl_4^L(f).$$

Proof. The proof is a direct consequence of (1) and Proposition 1.

Theorem 11. *Let $f_1 \in \mathcal{B}_{r,4}$ and $f_2 \in \mathcal{B}_{s,4}$. A function $g \in \mathcal{B}_{r+s,4}$ expressed as*

$$g(x_{r+s}, \ldots, x_{r+2}, x_{r+1}, \ldots, x_1) = f_1(x_r, \ldots, x_1) + f_2(x_{r+s}, \ldots, x_{r+2}, x_{r+1}),$$

is balanced if either f_1 or f_2 is balanced.

Proof. The proof follows from Proposition 3 and the fact that $\mathcal{W}_g(\mathbf{u}, \mathbf{v}) = \mathcal{W}_{f_1}(\mathbf{u})\mathcal{W}_{f_2}(\mathbf{v})$ and $\mathcal{W}_g^2(\mathbf{u}, \mathbf{v}) = \mathcal{W}_{f_1}^2(\mathbf{u})\mathcal{W}_{f_2}^2(\mathbf{v})$ for all $(\mathbf{u}, \mathbf{v})\mathbb{Z}_4^r \times \mathbb{Z}_4^s$.

References

1. C. Carlet and S. Dubuc, On generalized bent and q-ary perfect nonlinear functions, in: D. Jungnickel, H. Niederreiter (Eds.), Finite Fields and Applications, Proceedings of Fq5, Springer, Berlin, (2000), pp. 81-94.
2. X. Hou, q-ary bent functions constructed from chain rings. Finite Fields and Applications 4(1998), pp. 55-61.
3. X.-D. Hou, Bent functions, partial difference sets and quasi-Frobenius rings. Designs, Codes and Cryptography 20(2000), pp. 251-268.
4. X. Hou, p-ary and q-ary versions of certain results about bent functions and resilient functions. Finite Fields and Applications 10(2004), pp. 566-582.
5. Z. Jadda and P. Parraud, $\mathbb{Z}_4$-nonlinearity of a constructed quaternary cryptographic functions class. C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338(2010), pp. 270-283.
6. P.V. Kumar, R.A. Scholtz and L.R. Welch, Generalized bent functions and their properties. Journal of Combinatirial Theory, Ser. A 1(40) (1985), pp. 90-107.
7. P.V. Kumar, T. Hellesth, A.R. Calderbank and A.R Hammons, Large families of quaternary sequences with low correlation. IEEE Transactions on Information Theory 42(2)(1996), pp. 579–592.
8. O.S. Rothaus, On bent functions. Journal of Combinatorial Theory 20 (1976), pp. 300-305.
9. P. Sarkar and S. Maitra, Cross-correlation analysis of cryptographically useful Boolean functions. Theory of Computing Systems 35 (2002), pp. 39-57.
10. K-U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA. IEEE Transactions on Information Theory 55 (4) 2009, pp. 1824-1832.
11. C. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28 (1949), pp. 656-715.
12. P. Solé and N. Tokareva, Connections between quaternary and binary bent functions. Cryptology ePrint Archives (2009), http://www.eprint.iacr.org/2009/544.
13. N. Tokareva, Generalizations of bent functions: A survey. Journal of Applied and Industrial Mathematics 5(1) (2011), pp. 110-129.
14. Y. Zhou, M. Xie and G. Xiao, On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Information Sciences 180, pp. 256-265, 2010.
15. Z. Zhuo, On cross-correlation properties of Boolean functions, International Journal of Computer Mathematics 88(10) (2011), pp. 2035-2041.