Contemporary Mathematics
http://ojs.wiserpub.com/index.php/CM/

UNIVERSAL WISER PUBLISHER

Research Article

# Two Indicators of Cross-Correlation for the Functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$

**Deep Singh[1], Harsh Mishra[1], Vitsoto Luho[1], Amit Paul[2*]**

[1]Department of Mathematics and Statistics, Central University of Punjab, Bathinda, Punjab, India
[2]Department of Mathematics, Guru Nanak Dev University, Amritsar, Punjab, India
E-mail: amitpaulcuj@gmail.com

**Received:** 3 August 2023; **Revised:** 12 September 2023; **Accepted:** 19 September 2023

**Abstract:** Boolean functions play an important role in the design of secure cryptosystems and code division multiple access (CDMA) communication. Several possible generalizations of Boolean functions have been obtained in recent years. In this paper, we analyze the properties of functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$ in terms of their Walsh-Hadamard transform (WHT). We provide a relationship between cross-correlation and the WHT of these functions. Also, we present a necessary and sufficient condition for the functions to have complementary autocorrelation. The Parseval's identity for the current setup of these functions is obtained. Further, we obtained the modulus indicator (MI) and the sum-of-squares-modulus indicator (SSMI) of cross-correlation among two functions for the current setup.

***Keywords*:** WHT, cross-correlation, autocorrelation, MI, SSMI

**MSC:** 94A60, 94D10, 06E30

## 1. Introduction

Data security has become very important for society in the present digital age. Cryptography is the art of writing secure data. The main advancement in the field of cryptography marks with the introduction of Boolean functions [1-2]. Boolean bent functions were introduced by Rothaus [3] and have many applications in the fields of cryptography and coding theory. Bent functions are those Boolean functions which have the maximum distance from the set of all affine functions (equivalently, if they have a flat spectrum with respect to Walsh-Hadamard transform (WHT). In previous years, various authors [4-10] have presented many generalizations of Boolean functions and studied the effect of WHT on these functions. Here, in this article, we consider the generalized functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$ with $q \geq 2$ is a positive integer. The WHT is a crucial component in analyzing several properties of Boolean functions as well as their generalizations. The Hamming distance of Boolean functions and other coding and decoding axioms are investigated through WHT. We analyze some properties of functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$ with respect to the WHT. The results presented in this paper are useful in the design of secure coding and decoding algorithms.

Let $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ be the set of integers, real numbers, and complex numbers, respectively. Let $q \geq 2$ and $n$ be the positive integers. Let $\mathbb{Z}_2^n$ be the vector space of dimension $n$ over the field $\mathbb{Z}_2$, and $\mathbb{Z}_q$ be the ring of integers modulo $q$, respectively. A function $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is known as a Boolean function on $n$ variables. Let $\mathcal{B}_n$ denote the set of all Boolean functions on $n$ variables. Kumar et al. [4] have presented the concept of generalized bent functions which is defined as $g : \mathbb{Z}_q^n \to \mathbb{Z}_q$. The set of all such functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ is denoted by $\mathcal{B}_{n,q}$. Let + denote the addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$,


DOI: https://doi.org/10.37256/cm.5220243489

and $\oplus$ denote the addition over $\mathbb{Z}_q^n$. If $\mathbf{z}=(z_1,z_2,...,z_n)$ and $\mathbf{w}=(w_1,w_2,...,w_n)$ are two elements $\mathbb{Z}_q^n$, then the inner (scalar) product $\langle \mathbf{z},\mathbf{w}\rangle$ is defined by

$$<\mathbf{z},\mathbf{w}> = z_1w_1 \oplus z_2w_2 \oplus ... \oplus z_nw_n.$$

The WHT of $g \in \mathcal{B}_{n,q}$ is given by

$$\mathcal{T}_g^q(\mathbf{w}) = \frac{1}{q^{n/2}} \sum_{\mathbf{z}\in\mathbb{Z}_q^n} \zeta^{g(\mathbf{z})+\langle \mathbf{z},\mathbf{w}\rangle}.$$

The inverse WHT for the generalized bent function is given by [8]

$$\zeta^{g(\mathbf{z})} = q^{-n/2} \sum_{v\in\mathbb{Z}_q^n} \mathcal{T}_g^q(\mathbf{v})\zeta^{\langle \mathbf{v},\mathbf{z}\rangle}.$$

Further, Schmidt [11] has provided the construction of bent functions for the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Let $\mathcal{A}_{n,q}$ represent the collection of all functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Let $\xi$ be the primitive $2q$-th root of unity and $\zeta$ be the $q$-th root of unity, then the WHT of $g \in \mathcal{A}_{n,q}$ is given by [11]

$$\mathcal{T}_g(\mathbf{w}) = \frac{1}{q^{n/2}} \sum_{\mathbf{z}\in\mathbb{Z}_q^n} \xi^{g(\mathbf{x})}\zeta^{\langle \mathbf{z},\mathbf{w}\rangle},$$

where $\langle \mathbf{z},\mathbf{w}\rangle$ is the inner product of $\mathbf{z}$ and $\mathbf{w}$ in $\mathbb{Z}_q^n$.

Suppose $g,h \in \mathcal{A}_{n,q}$. Then, the cross-correlation [12] of $g$ and $h$ at any $\mathbf{v} \in \mathbb{Z}_q^n$ is defined as

$$\mathcal{C}_{g,h}(\mathbf{v}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{g(\mathbf{y})-h(\mathbf{y}+\mathbf{v})}.$$

If $g = h$, then the autocorrelation of $g$ at $\mathbf{v} \in \mathbb{Z}_q^n$ is defined as

$$\mathcal{C}_{g,g}(\mathbf{v}) = \mathcal{C}_g(\mathbf{v}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \xi^{g(\mathbf{y})-g(\mathbf{y}+\mathbf{v})}.$$

The two indicators: sum-of-squares indicator and the absolute indicator were introduced by Zhang et al. [13]. These indicators of Boolean functions are referred to as the global avalanche characteristics among them. Further, corresponding to these indicators, Singh et al. [14] have given two similar indicators: the *modulus indicator* (MI) and the *sum-of-squares-modulus indicator* (SSMI) of cross-correlation among two $q$-ary functions. They have investigated several properties of $q$-ary functions with respect to MI and SSMI. Also, they have obtained lower as well as upper bounds for these two indicators. Following a similar concept, we have defined two indicators in the present setup. For possible applications in cryptographic algorithms, the functions must possess a smaller correlation. The SSMI and MI bounds obtained for the functions in the current setup show that these functions have importance in communication algorithms and code division multiple access (CDMA) systems.

The SSMI of $g,h \in \mathcal{A}_{n,q}$ is given by

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

and the MI of $g,h \in \mathcal{A}_{n,q}$ is given by

$$\Delta_{g,h} = \max_{\mathbf{u}\in\mathbb{Z}_q^n} |\mathcal{C}_{g,h}(\mathbf{u})|^2.$$

The structure of the article is as follows: Section 2 presents the inverse WHT of the functions belonging to the present setup. Also, we present a link between the WHT and the cross-correlation of these functions. The Parseval's identity is obtained for these functions. Section 3 presents a result related to the complementary autocorrelation of these functions. It is also shown that $h \in \mathcal{A}_{s+t,\,q}$ is a bent function if and only if $g_1 \in \mathcal{A}_{s,\,q}$, $g_2 \in \mathcal{A}_{t,\,q}$ are bent for $h = g_1 + g_2$. In Section 4, two indicators of correlation, SSMI and MI, for the functions in the current setup are provided. Further, the lower and upper bounds for these indicators are also obtained. Section 5 presents the conclusion.

We recall the following preliminary results.

**Lemma 1** [15] Suppose $\mathbf{u} \in \mathbb{Z}_2^n$. Then, we have

$$\sum_{\mathbf{y}\in\mathbb{Z}_2^n}(-1)^{<\mathbf{u},\,\mathbf{y}>} = \begin{cases} 2^n, & \text{if } \mathbf{u} = 0, \\ 0, & \text{otherwise.} \end{cases}$$

**Lemma 2** [4] Suppose $\mathbf{u} \in \mathbb{Z}_q^n$, where $n$ is a positive integer. Then, we have

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n}\zeta^{\langle \mathbf{u},\mathbf{y}\rangle} = \begin{cases} q^n, & \text{if } \mathbf{u} = 0, \\ 0, & \text{otherwise.} \end{cases}$$

## 2. Properties of WHT from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$

In this section, we provide the inverse WHT and cross-correlation of the function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Next, we present a relationship among the cross-correlation and WHT of these functions.

**Theorem 1** Suppose $f$ is a function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$ and $\mathbf{y} \in \mathbb{Z}_q^n$. The inverse WHT is given by

$$\xi^{f(\mathbf{z})} = q^{-n/2}\sum_{\mathbf{v}\in\mathbb{Z}_q^n}\mathcal{T}_f(\mathbf{v})\zeta^{\langle \mathbf{v},\mathbf{z}\rangle}. \tag{1}$$

**Proof.** The WHT for the function $f$ is given by

$$\mathcal{T}_f(\mathbf{u}) = q^{-n/2}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})}\zeta^{\langle \mathbf{x},\,\mathbf{u}\rangle}.$$

Taking right hand side of Equation (1)

$$q^{-n/2}\sum_{\mathbf{v}\in\mathbb{Z}_q^n}\mathcal{T}_f(\mathbf{v})\zeta^{\langle \mathbf{v},\mathbf{z}\rangle} = q^{-n/2}\sum_{\mathbf{v}\in\mathbb{Z}_q^n}q^{-n/2}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})}\zeta^{\langle \mathbf{x},\mathbf{v}\rangle}\zeta^{\langle \mathbf{v},\mathbf{y}\rangle}$$

$$= q^{-n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})}\sum_{\mathbf{v}\in\mathbb{Z}_q^n}\zeta^{\langle \mathbf{v},\mathbf{x}+\mathbf{y}\rangle}$$

$$= q^{-n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})}q^n$$

$$= \xi^{f(\mathbf{y})}$$

**Theorem 2** Suppose $f$ and $g$ are the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$, $\mathbf{y} \in \mathbb{Z}_q^n$, and $\mathbf{v}, \mathbf{y} \in \mathbb{Z}_q^n$. Then

$$\mathcal{C}_{f,g}(\mathbf{v}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{T}_f(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{y})}\,\zeta^{\langle \mathbf{v},\mathbf{y}\rangle} \tag{2}$$

and

$$\sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{v})\zeta^{\langle -\mathbf{u},\mathbf{y}\rangle} = q^n \mathcal{T}_f(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{y})}. \tag{3}$$

**Proof.** Taking right hand side of Equation (2)

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{T}_f(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{y})}\zeta^{\langle \mathbf{v},\mathbf{y}\rangle} = \sum_{\mathbf{y}\in\mathbb{Z}_q^n}\left(q^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})}\zeta^{\langle \mathbf{x},\mathbf{y}\rangle}\right)\left(q^{-\frac{n}{2}}\sum_{\mathbf{u}\in\mathbb{Z}_q^n}\xi^{-g(\mathbf{u})}\zeta^{-\langle \mathbf{u},\mathbf{y}\rangle}\right)\zeta^{\langle \mathbf{v},\mathbf{y}\rangle}\right)$$

$$= \sum_{\mathbf{y}\in\mathbb{Z}_q^n} q^{-n}\sum_{\mathbf{x},\mathbf{u}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})-g((\mathbf{u})}\zeta^{\langle \mathbf{x}-\mathbf{u},\mathbf{y}\rangle}\zeta^{\langle \mathbf{v},\mathbf{y}\rangle}$$

$$= q^{-n}\sum_{\mathbf{y}\in\mathbb{Z}_q^n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})-g(\mathbf{u}+\mathbf{x})}\zeta^{\langle \mathbf{x}-\mathbf{u}+\mathbf{v},\mathbf{y}\rangle}$$

$$= q^{-n}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{x})-g(\mathbf{v}+\mathbf{x})}q^n \qquad \text{(by using Lemma 2)}$$

$$= \mathcal{C}_{f,g}(\mathbf{v})$$

Now, taking left hand side of the Equation (3)

$$\sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{f,g}(\mathbf{v})\zeta^{\langle -\mathbf{u},\mathbf{y}\rangle} = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{T}_f(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{y})}\zeta^{\langle \mathbf{v},\mathbf{y}\rangle}\zeta^{\langle -\mathbf{u},\mathbf{y}\rangle}$$

$$= \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{T}_f(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{y})}\zeta^{\langle \mathbf{v}-\mathbf{u},\mathbf{y}\rangle}$$

$$= q^n \mathcal{T}_f(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{y})}$$

Hence, the result.
We have the following corollary for $f = g$.
**Corollary 1** Let $f \in \mathcal{A}_{n,q}$, Then, we have

$$\mathcal{C}_f(\mathbf{v}) = \sum_{\mathbf{y}\in\mathbb{Z}_q^n} |\mathcal{T}_f(\mathbf{v})|^2\,\zeta^{\langle \mathbf{v},\mathbf{y}\rangle}$$

and

$$|\mathcal{T}_f(v)|^2 = q^{-n}\sum_{x\in\mathbb{Z}_q^n}\mathcal{C}_f(x)\zeta^{\langle -v,x\rangle}.$$

**Theorem 3** Suppose $f$ is a function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$ and $\mathbf{y}\in\mathbb{Z}_q^n$. Then, we have

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

where $q \geq 2$ is any positive integer.

**Proof.** Taking

$$\sum_{y\in\mathbb{Z}_q^n}\left|\mathcal{T}_f(y)\right|^2 = \sum_{y,z\in\mathbb{Z}_q^n}\mathcal{T}_f(y)\overline{\mathcal{T}_f(z)}$$

$$= \sum_{y,z\in\mathbb{Z}_q^n} q^{-n}\left(\sum_{u\in\mathbb{Z}_q^n}\xi^{f(u)}\zeta^{\langle u,y\rangle}\right)\left(\sum_{v\in\mathbb{Z}_q^n}\xi^{-f(v)}\zeta^{-\langle v,z\rangle}\right)$$

$$= q^{-n}\sum_{u,v\in\mathbb{Z}_q^n}\xi^{f(u)-f(v)}\sum_{y,z\in\mathbb{Z}_q^n}\zeta^{\langle u,y\rangle-\langle v,z\rangle}$$

Let $\mathbf{y} = \mathbf{z} + \mathbf{k}$

$$= q^{-n}\sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}_q^n}\xi^{f((\mathbf{u})-f(\mathbf{v})}\sum_{\mathbf{z}\in\mathbb{Z}_q^n}\zeta^{(\mathbf{u},\mathbf{z}+\mathbf{k})-(\mathbf{v},\mathbf{z})\rangle}$$

$$= q^{-n}\sum_{\mathbf{u},\mathbf{v}\in\mathbb{Z}_q^n}\xi^{f(\mathbf{u})-f(\mathbf{v})}\zeta^{\langle\mathbf{u},\mathbf{k}\rangle}\sum_{z\in\mathbb{Z}_q^n}\zeta^{\langle\mathbf{u}-\mathbf{v},\mathbf{z}\rangle}$$

$$= q^{-n}\sum_{\mathbf{u}\in\mathbb{Z}_q^n}\zeta^{\langle\mathbf{u},\mathbf{k}\rangle}q^n \qquad \text{(by using Lemma 2)}$$

In particular, for $\mathbf{y} = \mathbf{z}$, we have

$$\sum_{\mathbf{y}\in\mathbb{Z}_q^n}|\mathcal{T}_f(\mathbf{y})|^2 = q^n \tag{4}$$

which gives the Parseval's identity for the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$.

# 3. Complementary autocorrelation of functions

In this section, we present a result on complementary autocorrelation of the functions $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Also, it is shown that the function $h\in\mathcal{A}_{s+t,q}$ is bent if and only if $g_1\in\mathcal{A}_{s,q}$ and $g_2\in\mathcal{A}_{t,q}$, where $h = g_1 + g_2$, are bent functions.

Let $\mathbf{k} = (k_r, k_{r-1},..., k_1)$. Define

$$g_{\mathbf{k}}(y_{n-r},...,y_1) = g(y_n = k_r,...,y_{n-r+1} = k_1, y_{n-r},...,y_1).$$

For any $\mathbf{s} = (s_r,...,s_1) \in \mathbb{Z}_q^r$ and $\mathbf{m} = (m_{n-r},...,m_1) \in \mathbb{Z}_q^{n-r}$, the vector *concatenation* $\mathbf{sm}$ is defined as

$$\mathbf{sm} = (\mathbf{s},\mathbf{m}) = (s_r,...s_1, m_{n-r},...,m_1).$$

**Lemma 3** Let $\mathbf{s} \in \mathbb{Z}_q^r$, $\mathbf{m} \in \mathbb{Z}_q^{n-r}$ and $g$ be a function of $n$ variables on $\mathbb{Z}_q^n$. Then, the autocorrelation of $g$ will be

$$\mathcal{C}_g(\mathbf{sm}) = \sum_{\mathbf{k} \in \mathbb{Z}_q^r} \mathcal{C}_{g_{\mathbf{k}}, g_{\mathbf{k} \oplus \mathbf{s}}}(\mathbf{m}).$$

**Proof.** We compute

$$\begin{aligned}
\mathcal{C}_g(\mathbf{sm}) &= \sum_{y \in \mathbb{Z}_q^n} \xi^{g(\mathbf{y}) - g(\mathbf{sm}+\mathbf{y})} \\
&= \sum_{k \in \mathbb{Z}_q^r} \sum_{z \in \mathbb{Z}_q^{n-r}} \xi^{g(\mathbf{kz}) - g(\mathbf{kz}+\mathbf{sm})} \\
&= \sum_{k \in \mathbb{Z}_q^r} \sum_{z \in \mathbb{Z}_q^{n-r}} \xi^{g_k(\mathbf{z}) - g_{k+s}(\mathbf{z}+\mathbf{m})} \\
&= \sum_{k \in \mathbb{Z}_q^r} \mathcal{C}_{g_k, g_{k \oplus s}}(\mathbf{m}).
\end{aligned}$$

Any two functions $g$ and $h$ have complementary *autocorrelation* if $\mathcal{C}_g(\mathbf{v}) + \mathcal{C}_h(\mathbf{v}) = 0$ for any $\mathbf{v} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$.

**Theorem 4** Any functions $f$ and $g$ are considered to possess complementary autocorrelation if $|\mathcal{T}_f(\mathbf{v})|^2 + |\mathcal{T}_g(\mathbf{v})|^2 = 2, \forall\ \mathbf{v} \in \mathbb{Z}_q^n$.

**Proof.** Suppose that $f, g \in \mathcal{A}_{n,q}$. Let $f$ and $g$ on $\mathbb{Z}_q^n$ acquires complementary autocorrelation. Then

$$|\mathcal{T}_f(v)|^2 = q^{-n} \sum_{x \in \mathbb{Z}_q^n} \mathcal{C}_f(x) \zeta^{\langle -v, x \rangle} \tag{5}$$

$$|\mathcal{T}_g(v)|^2 = q^{-n} \sum_{x \in \mathbb{Z}_q^n} \mathcal{C}_g(x) \zeta^{\langle -v, x \rangle}. \tag{6}$$

Adding Equation (5) and Equation (6), we get

$$\begin{aligned}
\left|\mathcal{T}_f(\mathbf{v})\right|^2 + \left|\mathcal{T}_g(\mathbf{v})\right|^2 &= q^{-n} \sum_{\mathbf{x} \in \mathbb{Z}_q^n} \left(\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x})\right) \zeta^{\langle -\mathbf{v}, \mathbf{x} \rangle}, \\
&= q^{-n} \left(2q^n\right)
\end{aligned}$$

which gives that for all $\mathbf{v} \in \mathbb{Z}_q^n$, we have $|\mathcal{T}_f(\mathbf{v})|^2 + |\mathcal{T}_g(\mathbf{v})|^2 = 2$.

Conversely, assume that for all $\mathbf{v} \in \mathbb{Z}_q^n$, we have $|\mathcal{T}_f(\mathbf{v})|^2 + |\mathcal{T}_g(\mathbf{v})|^2 = 2$.

Then

$$\begin{aligned}\mathcal{C}_f(\mathbf{x}) + \mathcal{C}_g(\mathbf{x}) &= \sum_{\mathbf{v} \in \mathbb{Z}_q^n} \left( \left|\mathcal{T}_f(\mathbf{v})\right|^2 + \left|\mathcal{T}_g(\mathbf{v})\right|^2 \right) \zeta^{\langle \mathbf{v}, \mathbf{x} \rangle} \\ &= 2 \sum_{\mathbf{v} \in \mathbb{Z}_q^n} \zeta((\mathbf{x}\rangle \\ &= 2q^n \delta_0(\mathbf{x})\end{aligned}$$

where $\delta_{\mathbf{0}}(\mathbf{x}) = \begin{cases} 1, & \text{if } \mathbf{x} = \mathbf{0}, \\ 0, & \text{otherwise} \end{cases}$ and therefore, $\mathcal{C}_f(\mathbf{y}) + \mathcal{C}_g(\mathbf{y}) = 0$ for all $\mathbf{y} \in \mathbb{Z}_q^n \setminus \{\mathbf{0}\}$. Hence, $f$ and $g$ possess complementary autocorrelation.

**Theorem 5** Let $g_1 \in \mathcal{A}_{s,q}$ and $g_2 \in \mathcal{A}_{t,q}$. Then, the function $h \in \mathcal{A}_{s+t,q}$ expressed as

$$h(x_{s+t}, \ldots x_{s+1}, x_s, \ldots, x_1) = g_2(x_{s+t}, \ldots x_{s+1}) + g_1(x_s, \ldots, x_1)$$

will be bent if both $g_1$ and $g_2$ are bent.

**Proof.** Let $(\mathbf{v}, \mathbf{w}) \in \mathbb{Z}_q^s \times \mathbb{Z}_q^t$. We figure out

$$\begin{aligned}\mathcal{T}_h(\mathbf{v}, \mathbf{w}) &= q^{-(s+t)/2} \sum_{(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_q^s \times \mathbb{Z}_q^t} \xi^{h(\mathbf{x}, \mathbf{y})} \zeta^{\langle \mathbf{v}, \mathbf{x} \rangle + \langle \mathbf{w}, \mathbf{y} \rangle} \\ &= q^{-\frac{s}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_q^s} \xi^{g_1(x)} \zeta^{\langle \mathbf{v}, \mathbf{x} \rangle} q^{-\frac{t}{2}} \sum_{\mathbf{y} \in \mathbb{Z}_q^t} \xi^{g_2(\mathbf{y})} \zeta^{\langle \mathbf{w}, \mathbf{y} \rangle} \\ &= \mathcal{T}_{g_1}(\mathbf{v}) \mathcal{T}_{g_2}(\mathbf{w}).\end{aligned}$$

Now, if $g_1$ and $g_2$ both are bent functions, then $|\mathcal{T}_{g_1}(\mathbf{v})|$ and $|\mathcal{T}_{g_2}(\mathbf{w})|$ are both equal to 1, which implies that $|\mathcal{T}_h(\mathbf{v}, \mathbf{w})| = |\mathcal{T}_{g_1}(\mathbf{v})||\mathcal{T}_{g_2}(\mathbf{w})| = 1$ for any $(\mathbf{v}, \mathbf{w}) \in \mathbb{Z}_q^s \times \mathbb{Z}_q^t$. Hence, the function $h$ is a bent.

Conversely, suppose that $h$ is a bent. Our aim is to prove that $g_1$ and $g_2$ are also bent functions. Suppose that the function $g_1$ is not a bent. Then, there must exists $\mathbf{v} \in \mathbb{Z}_q^s$ in such a way $|\mathcal{T}_{g_1}(\mathbf{v})| > 1$. This means that $|\mathcal{T}_{g_2}(\mathbf{w})| > 1$ for all $\mathbf{w} \in \mathbb{Z}_q^t$. Since $|\mathcal{T}_{g_1}(\mathbf{v})||\mathcal{T}_{g_2}(\mathbf{w})| = 1$, which contradicts the fact that $\sum_{\mathbf{w} \in \mathbb{Z}_q^t} |\mathcal{T}_{g_2}(\mathbf{w})|^2 = q^t$.

# 4. Cross-correlation indicators for the functions $\mathbb{Z}_q^n \to \mathbb{Z}_{2q}$

Any function $g \in \mathcal{A}_{n,q}$ is called a balanced function if $|\{a : g(a) = k\}| = \frac{q^{n-1}}{2}$ for all $k \in \mathbb{Z}_{2q}$. We compute a lower bound and upper bound of $\Delta_{g,h}$, by using the definition of $\Delta_{g,h}$, in the following result.

**Theorem 6** Suppose $g, h \in \mathcal{A}_{n,q}$. Then, we have

1. $\Delta_{g,h} = 0$ if and only if $g(\mathbf{a}) - h(\mathbf{a} + \mathbf{v})$ is balanced for all $\mathbf{v} \in \mathbb{Z}_q^n$.

2. $\Delta_{g,h} = (2q)^n$ if and only if $g(\mathbf{a}) = h(\mathbf{a}+\mathbf{v}) + c$, $c \in \mathbb{Z}_{2q}$ for some $\mathbf{v} \in \mathbb{Z}_q^n$.
3. $0 \le \Delta_{g,h} \le (2q)^n$.

**Proof.**

1. Let $g(\mathbf{a}) - h(\mathbf{a}+\mathbf{v})$ is balanced for all $\mathbf{v} \in \mathbb{Z}_q^n$.Then

$$|\{\mathbf{a} : g(\mathbf{a}) - h(\mathbf{a}+\mathbf{v}) = k\}| = \frac{q^{n-1}}{2} \text{ for all } k \in \mathbb{Z}_{2q}.$$

The cross-correlation between $g, h \in \mathcal{A}_{n,q}$ at $\mathbf{v} \in \mathbb{Z}_q^n$ is

$$\begin{aligned} \mathcal{C}_{g,h}(\mathbf{v}) &= \sum_{a \in \mathbb{Z}_q^n} \xi^{g(\mathbf{a}) - h(\mathbf{a}+\mathbf{v})} \\ &= \frac{q^{n-1}}{2} \sum_{k \in \mathbb{Z}_{2q}} \xi^k \\ &= \frac{q^{n-1}}{2} \left( \frac{1-\xi^{2q}}{1-\xi} \right) \\ &= 0. \end{aligned}$$

Since $g(\mathbf{a}) - h(\mathbf{a}+\mathbf{v})$ is balanced for all $\mathbf{v} \in \mathbb{Z}_q^n$, then $\mathcal{C}_{g,h} = 0$ for all $\mathbf{v} \in \mathbb{Z}_q^n$. Thus, by definition, we have $\Delta_{g,h} = 0$.

2. Suppose that $g(\mathbf{a}) = h(\mathbf{a}+\mathbf{v}) + c$, $c \in \mathbb{Z}_{2q}$ for some $\mathbf{v} \in \mathbb{Z}_q^n$. Then

$$\begin{aligned} \Delta_{g,h} &= \max_{v \in \mathbb{Z}_q^n} \left| \mathcal{C}_{g,h}(v) \right| \\ &= \max_{v \in \mathbb{Z}_q^n} \left| \sum_{a \in \mathbb{Z}_q^n} \xi^{g(a) - h(a+v)} \right| \\ &= \max_{v \in \mathbb{Z}_q^n} | \sum_{a \in \mathbb{Z}_q^n} \xi^{h(a+v)+c-h(a+v)} \\ &= \max_{v \in \mathbb{Z}_q^n} \left| \sum_{a \in \mathbb{Z}_q^n} \xi^{c} \right| \\ &= (2q)^n. \end{aligned}$$

3. Since $|\mathcal{C}_{g,h}(\mathbf{v})| \ge 0$ and the upper bound of $\Delta_{g,h}$ is $(2q)^n$. Hence, we conclude that $0 \le \Delta_{g,h} \le (2q)^n$.

**Theorem 7** Suppose $g, h \in \mathcal{A}_{n,q}$. Then

1. $|\mathcal{C}_{g,h}(0)|^2 \le \sigma_{g,h} \le q^{3n}$.
2. $\sigma_{g,h} = q^{3n}$ if and only if $g$ and $h$ are affine.
3. $\sigma_{g,h} = |\mathcal{C}_{g,h}(0)|^2$ if and only if $g$ and $h$ are either perfectly uncorrelated or generalized bent.

**Proof.**

1. By using Cauchy inequality and Theorem 2, we have $(\sum_j x_j y_j)^2 \le \sum_j x_j^2 \sum_j y_j^2$ for all $x_j, y_j \in \mathbb{R}$, we have

$$\begin{aligned}
\sigma_{g,h} &= \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{g,h}(\mathbf{v})\overline{\mathcal{C}_{g,h}(\mathbf{v})} \\
&= \sum_{\mathbf{v}\in\mathbb{Z}_q^n}\sum_{\mathbf{y}\in\mathbb{Z}_q^n} \mathcal{T}_g(\mathbf{y})\overline{\mathcal{T}_h(\mathbf{y})}\zeta^{(-v,\mathbf{y})} \sum_{\overline{z}\in\mathbb{Z}_q^n} \overline{\mathcal{T}_g(\mathbf{z})\overline{\mathcal{T}_h(\mathbf{z})}\zeta^{\langle -\mathbf{v},\mathbf{z}}} \\
&= \sum_{\mathbf{y}\in\mathbb{Z}_q^n}\sum_{z\in\mathbb{Z}_q^n} \mathcal{T}_g(\mathbf{y})\overline{\mathcal{T}_g(\mathbf{z})}\mathcal{T}_h(\mathbf{z})\overline{\mathcal{T}_h(\mathbf{y})} \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \zeta^{\langle \mathbf{v},\mathbf{z}-\mathbf{y}\rangle} \\
&= q^n \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left|\mathcal{T}_g(\mathbf{y})\right|^2 \left|\mathcal{T}_h(\mathbf{y})\right|^2 \\
&\le q^n \left( \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left|\mathcal{T}_g(\mathbf{y})\mathcal{T}_h(\mathbf{y})\right| \right)^2 \\
&\le q^n \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left|\mathcal{T}_g(\mathbf{y})\right|^2 \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \left|\mathcal{T}_h(\mathbf{y})\right|^2 \\
&= q^{3n}.
\end{aligned}$$

Also,

$$\begin{aligned}
\sigma_{g,h} &= \sum_{\mathbf{v}\in\mathbb{Z}_q^n} \mathcal{C}_{g,h}(\mathbf{v})\overline{\mathcal{C}_{g,h}(\mathbf{v})} \\
&\ge \mathcal{C}_{g,h}(\mathbf{0})\overline{\mathcal{C}_{g,h}(\mathbf{0})} \\
&= \left|\mathcal{C}_{g,h}(0)\right|^2
\end{aligned}$$

Hence the result.

2. Using part 1, we have $\sigma_{g,h} = q^{3n}$ if and only if

$$\sum_{\mathbf{w}\in\mathbb{Z}_q^n} |\mathcal{T}_g(\mathbf{w})|^2 |\mathcal{T}_h(\mathbf{w})|^2 = \sum_{\mathbf{w}\in\mathbb{Z}_q^n} |\mathcal{T}_g(\mathbf{w})|^2 \sum_{\mathbf{w}\in\mathbb{Z}_q^n} |\mathcal{T}_h(\mathbf{w})|^2.$$

that is, $\sum_{\mathbf{v},\mathbf{w}\in\mathbb{Z}_q^n,\,\mathbf{v}\neq\mathbf{w}} |\mathcal{T}_g(\mathbf{v})|^2 |\mathcal{T}_h(\mathbf{w})|^2 = 0$ if $|\mathcal{T}_g(\mathbf{v})|^2 |\mathcal{T}_h(\mathbf{w})|^2 = 0$ for any $\mathbf{v} \neq \mathbf{w}$. If $|\mathcal{T}_g(\mathbf{v})|^2 = 0$ for all $\mathbf{v} \in \mathbb{Z}_q^n$, then it is a contradiction to Parseval's identity, (4). Therefore, for at least one $\mathbf{v}_0 \in \mathbb{Z}_q^n$, we must have $|\mathcal{T}_g(\mathbf{v}_0)|^2 \neq 0$. We consider the two cases:

(a) If there exists only one $\mathbf{v}_0 \in \mathbb{Z}_q^n$ for which $|\mathcal{T}_g(\mathbf{v}_0)|^2 \neq 0$, then $|\mathcal{T}_h(\mathbf{w})|^2 = 0$ for all $\mathbf{w} \in \mathbb{Z}_q^n$ except $\mathbf{w} \neq \mathbf{v}_0$. By using the identity (4), we get $|\mathcal{T}_g(\mathbf{u}_0)|^2 = q^n$, which gives $g(\mathbf{y}) = \mathbf{a} - 2\langle \mathbf{v}_0, \mathbf{y}\rangle$ for some $\mathbf{a} \in \mathbb{Z}_q^n$. Furthermore, $|\mathcal{T}_h(\mathbf{w})|^2 = 0$

for any $\mathbf{w} \neq \mathbf{v}_0$, implies that $|\mathcal{T}_g(\mathbf{v}_0)|^2 = q^n$. This means that for some $\mathbf{b} \in \mathbb{Z}_{2q}$, we have $h(\mathbf{y}) = \mathbf{b} - 2\langle \mathbf{v}_0, \mathbf{y} \rangle$. Therefore, the functions $f$ and $g$ are affine.

(b) If there is only two $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{Z}_q^n$ and $\mathbf{v}_1 \neq \mathbf{v}_2$ such that $|\mathcal{T}_g(\mathbf{v}_1)|^2 \neq 0$ and $|\mathcal{T}_g(\mathbf{v}_2)|^2 \neq 0$ then $|\mathcal{T}_h(\mathbf{v})|^2 = 0$ for any $\mathbf{v} \neq \mathbf{v}_1$ and accordingly $|\mathcal{T}_h(\mathbf{v})|^2 = 0$ for $\mathbf{v} \neq \mathbf{v}_2$. Thus, we get $|\mathcal{T}_h(\mathbf{v})|^2 = 0$ for all $\mathbf{v} \in \mathbb{Z}_q^n$, this is a contradiction to the identity (4). Equivalently, there is not only $r$, $(3 \leq r \leq 2^n)$ distinct $\mathbf{v}_i \in \mathbb{Z}_q^n (1 \leq i \leq r)$ with $|\mathcal{T}_g(\mathbf{v}_i)|^2 = 0$.

3. $\sigma_{g,h} = (\Delta_{g,h}(0))^2$ if and only if

$$\sum_{\mathbf{v} \in \mathbb{Z}_q^n} |\mathcal{T}_g(\mathbf{v})|^2 |\mathcal{T}_h(\mathbf{v})|^2 \sum_{\mathbf{v} \in \mathbb{Z}_q^n} 1^2 = \left( \sum_{\mathbf{v} \in \mathbb{Z}_q^n} |\mathcal{T}_g(\mathbf{v}) \overline{\mathcal{T}_h(\mathbf{v})}| \times 1 \right)^2$$

if and only if, for any $\mathbf{v} \in \mathbb{Z}_q^n$, $\dfrac{\mathcal{T}_g(\mathbf{v})\overline{\mathcal{T}_h(\mathbf{v})}}{1} = \phi(\mathbf{v})$, with $|\phi(\mathbf{v})| = r$, by Cauchy-Schwarz's inequality. There are the following cases:

(a) If $r = 0$, then the functions $g$ and $h$ are perfectly uncorrelated.

(b) If $r \neq 0$, then $|\mathcal{T}_g(\mathbf{v})\overline{\mathcal{T}_h(\mathbf{v})}| = \mathcal{T}_g(\mathbf{w})\overline{\mathcal{T}_h(\mathbf{w})}$ for any $\mathbf{v}, \mathbf{w} \in \mathbb{Z}_q^n$. Equivalently, $\dfrac{|\mathcal{T}_g(\mathbf{v})|}{|\mathcal{T}_g(\mathbf{w})|} = \dfrac{|\mathcal{T}_h(\mathbf{w})|}{|\mathcal{T}_h(\mathbf{v})|} = k$ for any $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$, where $k$ is a positive real number. Thus, $|\mathcal{T}_g(\mathbf{v})| = k|\mathcal{T}_g(\mathbf{w})|$ and $|\mathcal{T}_h(\mathbf{w})| = k|\mathcal{T}_h(\mathbf{v})|$. By using the identity (4), we have $k^2 = 1$. Hence, $|\mathcal{T}_g(\mathbf{v})|^2$ and $\mathcal{T}_h(\mathbf{v})|^2$ are constants for any $\mathbf{v} \in \mathbb{Z}_q^n$. Again, by using the identity (4), we have $|\mathcal{T}_g(\mathbf{v})| = |\mathcal{T}_h(\mathbf{v})| = 1$ for all $\mathbf{v} \in \mathbb{Z}_q^n$. This proves that both $g$ and $h$ are generalized bent.

# 5. Conclusion

Boolean functions and their various existing generalizations have numerous applications in the design of cryptosystems and coding theory. In this article, the cryptographic properties of the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. We have obtained the inverse WHT for the functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_{2q}$. Also, we provided a relationship between the WHT and the cross-correlation of these functions. The Parseval's identity is provided in the current setup. The complementary autocorrelation of these functions is studied. The concept of the indicators (SSMI and MI) is extended to the functions of the current setup. We analyzed these indicators and provided lower as well as upper bounds for them. The results of this article are useful for their applications in wireless communication systems.

# Acknowledgments

The first author is thankful to the Central University of Punjab for providing research seed money (grant no: CUPB/Acad./2022/1194) and to National Board for Higher Mathematics-Department of Atomic Energy (NBHM-DAE) for providing financial support under grant no.-02011/10/2020 NBHM(R.P.)/R\&D II/7025.

# Conflict of interest

There is no conflict of interest for this study.

# References

[1] Mitchell C. Enumerating Boolean functions of cryptographic significance. *Journal of Cryptology*. 1990; 2(3): 155-170. Available from: https://doi.org/10.1007/BF00190802.

[2] Shannon CE. *A mathematical theory of cryptography*. Bell Telephone Labs. Report Number: MM-45-110-92, 1945. Available from: https://www.iacr.org/museum/shannon/shannon45.pdf.
[3] Rothaus OS. On "bent" functions. *Journal of Combinatorial Theory, Series A*. 1976; 20(3): 300-305. Available from: https://doi.org/10.1016/0097-3165(76)90024-8.
[4] Kumar PV, Scholtz RA, Welch LR. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*. 1985; 40(1): 90-107. Available from: https://doi.org/10.1016/0097-3165(85)90049-4.
[5] Riera C, Parker MG. Generalized bent criteria for Boolean functions (I). *IEEE Transactions on Information Theory*. 2006; 52(9): 4142-4159. Available from: https://doi.org/10.1109/TIT.2006.880069.
[6] Schmidt KU. Quaternary constant-amplitude codes for multicode CDMA. *IEEE Transactions on Information Theory*. 2009; 55(4): 1824-1832. Available from: https://doi.org/10.1109/TIT.2009.2013041.
[7] Solé P, Tokareva N. Connections between quaternary and binary bent functions. *IACR Cryptology ePrint Archive*. 2009; 2009: 544. Available from: https://eprint.iacr.org/2009/544.pdf.
[8] Stănică P, Martinsen T, Gangopadhyay S, Singh BK. Bent and generalized bent Boolean functions. *Designs, Codes and Cryptography*. 2013; 69(1): 77-94. Available from: https://doi.org/10.1007/s10623-012-9622-5.
[9] Singh D, Paul A, Kumar N, Stoffová V, Verma C. Resiliency and nonlinearity profiles of some cryptographic functions. *Mathematics*. 2022; 10(23): 4473. Available from: https://doi.org/10.3390/math10234473.
[10] Singh D, Paul A. Some properties of cryptographic functions employed in wireless communication systems. *International Journal of Recent Technology and Engineering*. 2019; 8(3): 4154-4157. Available from: https://doi.org/10.35940/ijrte.C5490.098319.
[11] Schmidt KU. Highly nonlinear functions. *Designs, Codes and Cryptography*. 2015; 74(3): 665-672. Available from: https://doi.org/10.1007/s10623-013-9880-x.
[12] Sarkar P, Maitra S. Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes. *Theory of Computing Systems*. 2002; 35(1): 39-57. Available from: https://doi.org/10.1007/s00224-001-1019-1.
[13] Zhang XM, Zheng Y. GAC-the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*. 1995; 1(5): 320-337. Available from: https://doi.org/10.3217/jucs-001-05-0320.
[14] Singh D, Bhaintwal M, Singh BK. Some results on $q$-ary bent functions. *International Journal of Computer Mathematics*. 2013; 90(9): 1761-1773. Available from: https://doi.org/10.1080/00207160.2013.766330.
[15] Cusick TW, Stănică P. *Cryptographic Boolean Functions and Applications*. Amsterdam: Academic Press; 2009. Available from: https://doi.org/10.1016/B978-0-12-374890-4.X0001-8.