On generalized semi-bent (and partially bent) Boolean functions

Brajesh Kumar Singh[1]

Department of Mathematics, School of Allied Sciences,
Graphic Era Hill University, Dehradun-248002 (Uttarakhand) INDIA

Abstract

In this paper, we obtain a characterization of generalized Boolean functions based on spectral analysis. We investigate a relationship between the Walsh-Hadamard spectrum and σ_f, the sum-of-squares-modulus indicator (SSMI) of the generalized Boolean function. It is demonstrated that $\sigma_f = 2^{2n+s}$ for every s-plateaued generalized Boolean function in n variables. Two classes of generalized semi-bent Boolean functions are constructed.We have constructed a class of generalized semi-bent functions in $(n+1)$ variables from generalized semi-bent functions in n variables and identify a subclass of it for which σ_f and $\triangle_f$ both have optimal value. Finally, some construction on generalized partially bent Boolean functions are given.

Keywords: Boolean functions, generalized functions; Walsh-Hadamard spectrum; generalized bent Boolean functions; generalized semi-bent functions; sum-of-squares-modulus indicator (SSMI); modulus indicator (MI)

1. Introduction

Let $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_q$ respectively denotes the set of integers, real numbers, complex numbers, and the ring of integers modulo q. By '+' we denote the addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, whereas '$\oplus$' denotes the addition over an n-dimensional vector space $\mathbb{Z}_2^n$ over binary field $\mathbb{Z}_2$ with the standard operations. Addition modulo q is denoted by '+' and it is understood from the context. The scalar product of two vectors $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1)$ of $\mathbb{Z}_2^n$ is defined by $\mathbf{x} \cdot \mathbf{y} := x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. If $z = a + b\,\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\overline{z} = a - b\,\imath$ denotes the complex conjugate of z, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. $Re[z]$ denotes the real part of z.

In the recent years several authors have proposed generalizations of Boolean functions [6, 11, 14, 15] and studied the effect of Walsh–Hadamard transform on these classes. As in the Boolean case, in the generalized setup the functions which have flat spectra with respect to the Walsh–Hadamard transform are said to be generalized bent and are of special interest (the classical notion of bent was invented by Rothaus [8]) in cryptography and coding theory and have wide application in different type of cryptosystems [6, 11]. For example: the generalized bent Boolean functions are used for constructing the constant amplitude codes for the q valued version of multicode Code Division Multiple Access (MC-CDMA). The generalization of Boolean function due to Schmidt is a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$, $(q \geq 2)$, and he referred such function as *generalized Boolean function* on n variables [11], $\mathcal{GB}_n^q$ denotes the set of such functions. In particular, the set of classical Boolean functions on n variables is $\mathcal{B}_n := \mathcal{GB}_n^2$. For some problems concerning cyclic codes, Kerdock codes, and Delsarte-Goethals codes, the generalization of Boolean function [11] seems more natural than the generalization due to Kumar, Scholtz and Welch [6].

The (generalized) *Walsh–Hadamard transform* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is given by $\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}$, is complex valued function, where $\zeta = e^{2\pi\imath/q}$ is the complex q-primitive root of unity. The inverse of the Walsh-Hadamard transform [15, Thm.1] of $f \in \mathcal{GB}_n^q$ is given by $\zeta^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{y}}$. Moreover, the (generalized) Parseval's identity holds, that is,

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 = 2^n. \tag{1.1}$$

[*] corresponding author

Email address: bksingh0584@gmail.com (Brajesh Kumar Singh)

Preprint submitted to Elsevier *March 22, 2013*

A function $f \in \mathcal{GB}_n^q$ is a *generalized bent* function if $|\mathcal{H}_f(\mathbf{u})| = 1$, for all $\mathbf{u} \in \mathbb{Z}_2^n$. A function $f \in \mathcal{B}_n$ is bent if and only if $\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}} \in \{-1, 1\}$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. The classical bent Boolean functions exists only for even n [8] whereas the generalized bent functions exists for every positive integer. For $q = 4$, Schmidt [11] studied the relations between generalized bent functions, constant amplitude codes, and $\mathbb{Z}_4$-linear codes. The links between Boolean bent functions [8], generalized bent Boolean functions [11], and quaternary bent functions [6] is investigated systematically by Sol*é*-Tokareva [14]. Recently, several properties as well as constructions of generalized bent Boolean functions is presented by Stănică et al. [15].

A function $f \in \mathcal{B}_n^q$ is called *generalized semi-bent* if for any $\mathbf{u} \in \mathbb{Z}_q^n$ (*i*) $|\mathcal{H}_f(\mathbf{u})| \in \{0, \sqrt{2}\}$ for odd n, and (*ii*) $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2\}$ for even n. In particular, for $q = 2$ the semi-bent functions are also known as 3-valued almost optimal functions, plateaued functions and preferred functions [7, 16]. These functions have lowest Walsh-Hadamard spectrum values among the functions having 3-valued spectrum. It is not hard to show that the generalized bent Boolean functions can also be constructed from generalized semi-bent Boolean functions which is desirable in cryptosystem.

The *cross-correlation* between $f, g \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is defined as $C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-g(\mathbf{x}\oplus\mathbf{u})}$. The *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is $C_{f,f}(\mathbf{u})$ above, which we denote by $C_f(\mathbf{u})$. The *sum-of-squares-of-modulus indicator* (SSMI) [12] of f and g is defined as $\sigma_{f,g} = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} |C_{f,g}(\mathbf{x})|^2$. In particular, the SSMI of $f \in \mathcal{GB}_n^q$ is defined by $\sigma_f = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} |C_f(\mathbf{x})|^2$.

The modulus indicator (MI) [12] of $f, g \in \mathcal{GB}_n^q$ is defined as $\triangle_{f,g} = \max_{\mathbf{u}\in\mathbb{Z}_2^n} |C_{f,g}(\mathbf{u})|$. The MI of $f \in \mathcal{GB}_{n,q}$ is $\triangle_f = \max_{\mathbf{u}\in\mathbb{Z}_2^n,\mathbf{u}\neq\mathbf{0}} |C_f(\mathbf{u})|$.

In Boolean case, Gong and Khoo [19] have introduced the concept of dual of a Boolean function and provided a relationship between the autocorrelation of the s-plateaued functions and the Walsh-Hadamard Spectrum of the dual of the s-plateaued functions. Also, if the function $f \in \mathcal{B}_n$, for n odd, is a balanced semi-bent function such that $\tilde{f} \in \mathcal{B}_n$ also semi-bent, then $\triangle_f = 2^{\frac{n+1}{2}}$ and $C_f(a) = 0$ for $2^{n-1} - 1$ $a's$, that is, f has optimal additive autocorrelation [19, Thm. 2]. Several classes Boolean functions such as Dillon-Dobbertin, Kasami, Segre hyperoval and Welch-Gong Transformation functions for which the bounds are optimal is discussed in [19]. Several research papers are available in literature on these indicators, for details we refer [17, 19, 22, 23] and the references of these papers. Singh et al. [12, Thm. 4.4] obtained the optimal value of $\sigma_{f,g}$ and $\triangle_{f,g}$ for the functions in a subclass of Maiorana-McFarland class of q-ary bent functions, demonstrated that $\sigma_{f,g} = q^{2n}$ whenever one of the function f, g is q-ary bent.

2. Properties of Walsh-Hadamard transform on generalized Boolean functions

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. Several cryptographic properties of Boolean functions are discussed in terms spectral analysis of Boolean functions, for details we refer [9, 10, 17] and their references In this section, we provide the spectral analysis of the generalized Boolean functions. The following lemma is the generalization of Corollary 3.3 of Sarkar and Maitra [10] (obtained for $q = 2$).

Lemma 2.1. *Let $f, g, h \in \mathcal{GB}_n^q$ such that $h(\mathbf{x}) = f(\mathbf{x}) - g(\mathbf{x})$. Then*

$$\mathcal{H}_h(\mathbf{u}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})}, \textit{ for all } \mathbf{u} \in \mathbb{Z}_2^n. \tag{2.1}$$

Proof. Let $\mathbf{u} \in \mathbb{Z}_2^n$., we have

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})} = \frac{1}{2^n} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{y})}(-1)^{(\mathbf{x}+\mathbf{u})\cdot\mathbf{y}} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} \zeta^{-g(\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}}$$

$$= \frac{1}{2^n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{y})-g(\mathbf{z})}(-1)^{\mathbf{u}\cdot\mathbf{y}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{x}\cdot(\mathbf{y}+\mathbf{z})} = \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{h(\mathbf{y})}(-1)^{\mathbf{u}\cdot\mathbf{y}} = 2^{\frac{n}{2}}\mathcal{H}_h(\mathbf{u}).$$

□

The *derivative* of $f, g \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is defined as $D_{f,g}(\mathbf{u}) = f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})$. In particular for $f = g$, $D_f(\mathbf{u}) = f(\mathbf{x}) - f(\mathbf{x}+\mathbf{u})$ is defined as the derivative of f at $\mathbf{u}$. In Theorem 2.1 below we provide a relationship between $D_{f,g}(\mathbf{u})$-the derivative of $f, g \in \mathcal{GB}_n^q$ at every $\mathbf{u} \in \mathbb{Z}_2^n$ and their Walsh-Hadamard spectrums which is the generalization of [18, Theorem 1] (obtained for $q = 2$).

Theorem 2.1. *If $f, g \in \mathcal{GB}_n^q$ and $\mathbf{z} \in \mathbb{Z}_2^n$, then for any $\mathbf{u} \in \mathbb{Z}_2^n$*

$$\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u}) = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{x}\cdot\mathbf{z}} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})}, \quad \textit{and} \tag{2.2}$$

$$\mathcal{W}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{W}_g(\mathbf{x})} = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} (-1)^{\mathbf{x}\cdot\mathbf{z}} \mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u}). \tag{2.3}$$

Proof. Let $g_{\mathbf{z}}(\mathbf{x}) = g(\mathbf{z}+\mathbf{x})$. Then we have $\mathcal{H}_{g_{\mathbf{z}}}(\mathbf{u}) = (-1)^{\mathbf{u}\cdot\mathbf{z}}\mathcal{H}_g(\mathbf{u})$. On replacing g by $g_{\mathbf{z}}$ and h by $D_{f,g}(\mathbf{z})$ in (2.1), we have

$$\begin{aligned}\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u}) &= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{W}_{g_{\mathbf{z}}}(\mathbf{x})} \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{x}\cdot\mathbf{z}} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})}\end{aligned}$$

Further, using (2.2), we have

$$\begin{aligned}\sum_{\mathbf{z}\in\mathbb{Z}_2^n} \mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u})(-1)^{\mathbf{y}\cdot\mathbf{z}} &= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} (-1)^{\mathbf{y}\cdot\mathbf{z}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{x}\cdot\mathbf{z}} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})} \\ &= \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} (-1)^{(\mathbf{y}+\mathbf{x})\cdot\mathbf{z}} = 2^{\frac{n}{2}} \mathcal{H}_f(\mathbf{y}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{y})}.\end{aligned}$$

□

Since $D_{f,g}(\mathbf{z})(\mathbf{0}) = 2^{-\frac{n}{2}} C_{f,g}(\mathbf{z})$. The following corollary is Theorem 1 of [15], is obtained by putting $\mathbf{u} = \mathbf{0}$ in the above theorem.

Corollary 2.1. *[15, Thm.1] We have:*

(*i*) *If $f, g \in \mathcal{GB}_n^q$, then*

$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} C_{f,g}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}$, *and* $C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}$.

Further, $C_{f,g}(\mathbf{u}) = \overline{C_{g,f}(\mathbf{u})}$ *for all* $\mathbf{u} \in \mathbb{Z}_2^n$ *this implies that* $C_f(\mathbf{u})$ *is always real.*

(*ii*) *Taking the particular case $f = g$ we obtain* $\sum_{\mathbf{u}\in\mathbb{Z}_2^n} C_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n|\mathcal{H}_f(\mathbf{x})|^2$, *and* $C_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2(-1)^{\mathbf{u}\cdot\mathbf{x}}$.

(*iii*) *If $f \in \mathcal{GB}_n^q$, then f is a generalized bent function if and only if* $C_f(\mathbf{u}) = 2^n\delta_{\mathbf{0}}(\mathbf{u})$.

In Boolean case, the properties of these transform can be derived from the previous theorem, and for more results on Boolean functions, we refer [2–4].

The dual of a vector space V of $\mathbb{Z}_2^n$ is defined by $V^\perp = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x}\cdot\mathbf{y} = 0 \text{ for all } \mathbf{y} \in V\}$. The following two theorems is the generalization Zhou et. al [17, Lemma 3 and Theorem 6] results (obtained for $q = 2$)

Theorem 2.2. *Let V be a subspace of $\mathbb{Z}_2^n$ of dimension k, and $\mathbf{u} \in \mathbb{Z}_2^n$. Then for any $f, g \in \mathcal{GB}_n^q$, we have*

$$\sum_{\mathbf{x}\in V} \mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})} = 2^{\frac{2k-n}{2}} \sum_{\mathbf{z}\in V^\perp} \mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u}).$$

Proof. From Theorem 2.1, we have

$$\begin{aligned}\sum_{\mathbf{x}\in V}\mathcal{H}_f(\mathbf{x}+\mathbf{u})\overline{\mathcal{H}_g(\mathbf{x})} &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}\in V}\sum_{\mathbf{z}\in\mathbb{Z}_2^n}\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u})(-1)^{\mathbf{z}\cdot\mathbf{x}} = 2^{-\frac{n}{2}}\sum_{\mathbf{z}\in\mathbb{Z}_2^n}\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u})\sum_{\mathbf{x}\in V}(-1)^{\mathbf{z}\cdot\mathbf{x}}\\ &= 2^{\frac{2k-n}{2}}\sum_{\mathbf{z}\in\mathbb{Z}_2^n}\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u})\phi_{V^\perp}(\mathbf{z}) = 2^{\frac{2k-n}{2}}\sum_{\mathbf{z}\in V^\perp}\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{u}).\end{aligned}$$

□

Corollary 2.2. *Let $f, g \in \mathcal{GB}_n^q$. Then*

$$\sum_{\mathbf{x}\in V}\mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})} = 2^k\sum_{\mathbf{z}\in V^\perp}\mathcal{C}_{f,g}(\mathbf{z}),\ \textit{and} \tag{2.4}$$

$$\sum_{\mathbf{x}\in V}\left|\mathcal{H}_f(\mathbf{x}+\mathbf{u})\right|^2 = 2^{\frac{2k-n}{2}}\sum_{\mathbf{z}\in V^\perp}(-1)^{\mathbf{z}\cdot\mathbf{u}}\mathcal{H}_{D_f(\mathbf{z})}(\mathbf{0}) \tag{2.5}$$

Let V and W be a subspaces of $\mathbb{Z}_2^n$ such that $\dim(W) = k$ and $\mathbb{Z}_2^n = V \oplus W$. The decomposition of f with respect to W is the sequence $\{f_{\mathbf{z}} : \mathbf{z} \in V\}$ of generalized Boolean functions $f_{\mathbf{z}} \in \mathcal{GB}_k^q$ defined on W as $f_{\mathbf{z}}(\mathbf{x}) = f(\mathbf{z}+\mathbf{x})$ for all $\mathbf{x} \in W$. The relationship between the Walsh-Hadamard spectrums of $f, g \in \mathcal{GB}_n^q$ and the Walsh-Hadamard spectrums of the decompositions of f and g with respect to V is presented in the following

Theorem 2.3. *Let V and W be a subspaces of $\mathbb{Z}_2^n$ with* $\dim(W) = k$ *and $\mathbb{Z}_2^n = V \oplus W$. Let $\{f_{\mathbf{z}} : \mathbf{z} \in V\}$ and $\{g_{\mathbf{z}} : \mathbf{z} \in V\}$ be the decompositions of f and g with respect to W. Then*

$$\sum_{\mathbf{x}\in W^\perp}\mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})} = 2^{-n}\sum_{\mathbf{x}\in V}\mathcal{H}_{f_{\mathbf{x}}}(\mathbf{0})\overline{\mathcal{H}_{g_{\mathbf{x}}}(\mathbf{0})},\ \textit{and} \tag{2.6}$$

$$\sum_{\mathbf{x}\in W^\perp}\left|\mathcal{H}_f(\mathbf{x})\right|^2 = 2^{-n}\sum_{\mathbf{x}\in V}\left|\mathcal{H}_{f_{\mathbf{x}}}(\mathbf{0})\right|^2.$$

Proof. We have $\mathcal{C}_{f,g}(\lambda) = \sum_{\mathbf{w}\in\mathbb{Z}_2^n}\zeta^{f(\mathbf{w})-g(\mathbf{w}+\lambda)} = \sum_{\mathbf{x}\in V}\sum_{\mathbf{y}\in W}\zeta^{f_{\mathbf{x}}(\mathbf{y})-g_{\mathbf{x}}(\mathbf{y}+\lambda)} = \sum_{\mathbf{x}\in V}\sum_{\mathbf{y}\in W}\zeta^{f(\mathbf{x}+\mathbf{y})-g(\mathbf{x}+\mathbf{y}+\lambda)}$, for every $\lambda \in \mathbb{Z}_2^n$. Using Theorem 2.2 with $\mathbf{u} = \mathbf{0}$, we have

$$\begin{aligned}\sum_{\mathbf{x}\in W^\perp}\mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})} &= 2^{\frac{2k-n}{2}}\sum_{\mathbf{z}\in W}\mathcal{H}_{D_{f,g}(\mathbf{z})}(\mathbf{0}) = 2^{k-n}\sum_{\mathbf{z}\in W}\mathcal{C}_{f,g}(\mathbf{z})\\ &= 2^{k-n}\sum_{\mathbf{z}\in W}\sum_{\mathbf{x}\in V}\sum_{\mathbf{y}\in W}\zeta^{f(\mathbf{x}+\mathbf{y})-g(\mathbf{x}+\mathbf{y}+\mathbf{z})} = 2^{k-n}\sum_{\mathbf{x}\in V}\sum_{\mathbf{y}\in W}\zeta^{f(\mathbf{x}+\mathbf{y})}\sum_{\mathbf{z}\in W}\zeta^{-g(\mathbf{x}+\mathbf{y}+\mathbf{z})}\\ &= 2^{k-n}\sum_{\mathbf{x}\in V}\sum_{\mathbf{y}\in W}\zeta^{f_{\mathbf{x}}(\mathbf{y})}\sum_{\mathbf{u}\in W}\zeta^{-g_{\mathbf{x}}(\mathbf{u})} = 2^{-n}\sum_{\mathbf{x}\in V}\mathcal{H}_{f_{\mathbf{x}}}(\mathbf{0})\overline{\mathcal{H}_{g_{\mathbf{x}}}(\mathbf{0})}.\end{aligned} \tag{2.7}$$

The second part is obtained by putting $f = g$ in (2.6). □

2.1. Analysis of cross-correlation spectrum of generalized Boolean functions

The following results were shown in a different contexts in [12, 21]. One can straightforwardly infer, by modifying those proofs that these result hold under the current notions, as well.

Theorem 2.4. *Let $f, g, h, k \in \mathcal{GB}_n^q$, and $\mathbf{z} \in \mathbb{Z}_2^n$. Then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n}\mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{k,h}(\mathbf{u}+\mathbf{z}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^n}\mathcal{C}_{f,h}(\mathbf{v})\mathcal{C}_{k,g}(\mathbf{v}+\mathbf{z}). \tag{2.8}$$

Proof. Let $\mathbf{z} \in \mathbb{Z}_2^n$. Then

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{k,h}(\mathbf{u}+\mathbf{z}) = \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{h,k}(\mathbf{u}+\mathbf{z})} = \sum_{\mathbf{u}\in\mathbb{Z}_2^n}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{u})} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{k(\mathbf{y}+\mathbf{u}+\mathbf{z})-h(\mathbf{y})}$$
$$= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-h(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \zeta^{k(\mathbf{y}+\mathbf{u}+\mathbf{z})-g(\mathbf{x}+\mathbf{u})} = \sum_{\mathbf{x},\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-h(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \zeta^{k(\mathbf{y}+\mathbf{x}+\mathbf{u}+\mathbf{z})-g(\mathbf{u})}$$
$$= \sum_{\mathbf{v}\in\mathbb{Z}_2^n}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-h(\mathbf{x}+\mathbf{v})} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \zeta^{k(\mathbf{v}+\mathbf{u}+\mathbf{z})-g(\mathbf{u})} = \sum_{\mathbf{v}\in\mathbb{Z}_2^n} \mathcal{C}_{f,h}(\mathbf{v})\overline{\mathcal{C}_{g,k}(\mathbf{v}+\mathbf{z})} = \sum_{\mathbf{v}\in\mathbb{Z}_2^n} \mathcal{C}_{f,h}(\mathbf{v})\mathcal{C}_{k,g}(\mathbf{v}+\mathbf{z})$$

□

Taking $f = h$ and $g = k$ in (2.8) we have the following

Corollary 2.3. *Let $f, g \in \mathcal{GB}_n^q$, and $\mathbf{z} \in \mathbb{Z}_2^n$. then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{g,f}(\mathbf{u}+\mathbf{z}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^n} \mathcal{C}_{f}(\mathbf{v})\mathcal{C}_{g}(\mathbf{v}+\mathbf{z}), \tag{2.9}$$

and if $\mathbf{z} = \mathbf{0}$, then

$$\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\overline{\mathcal{C}_{f,g}(\mathbf{u})} = \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{g,f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{C}_{f}(\mathbf{x})\mathcal{C}_{g}(\mathbf{x}). \tag{2.10}$$

Further, if we take $g = k$ in (2.8), then $\sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{g,h}(\mathbf{u}+\mathbf{z}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^n} \mathcal{C}_{f,h}(\mathbf{v})\mathcal{C}_{g}(\mathbf{v}+\mathbf{z})$ for all $\mathbf{z} \in \mathbb{Z}_2^n$, and so using Corollary 2.3, we have

Proposition 1. *Let $f, h \in \mathcal{GB}_n^q$, and $g \in \mathcal{GB}_n^q$ be a generalized bent Boolean function, then*

(1) $\sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{g,h}(\mathbf{u}+\mathbf{z}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^n} \mathcal{C}_{f,h}(\mathbf{v})\mathcal{C}_{g}(\mathbf{v}+\mathbf{z}) = 2^n \sum_{\mathbf{v}\in\mathbb{Z}_2^n} \mathcal{C}_{f,h}(\mathbf{v})\delta_{\mathbf{0}}(\mathbf{v}+\mathbf{z}) = 2^n\mathcal{C}_{f,h}(\mathbf{z})$

(2) $\sigma_{f,g} = 2^{2n}$.

(3) *If f is generalized bent Boolean function, then $\sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})\mathcal{C}_{g,f}(\mathbf{u}+\mathbf{z}) = 0$ for all $\mathbf{z} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$*

Theorem 2.5. *Let $f, g \in \mathcal{GB}_n^q$, and if g is generalized bent Boolean function, then*

$$\triangle_{f,g} \geq 2^{\frac{n}{2}}, \text{ and } \max_{\mathbf{u}\in\mathbb{Z}_2^n\setminus\{\mathbf{0}\}} |\mathcal{C}_{f,g}(\mathbf{u})| \geq \sqrt{\frac{2^{2n} - |\mathcal{C}_{f,g}(0)|^2}{2^n - 1}}.$$

Proof. From property (2) of Proposition 1, we have $\sigma_{f,g} = \sum_{\mathbf{u}\in\mathbb{Z}_q^n} \left|\mathcal{C}_{f,g}(\mathbf{u})\right|^2 = 2^{2n}$. The values of $|\mathcal{C}_{f,g}(\mathbf{u})|$ will be minimum for every $\mathbf{u} \in \mathbb{Z}_2^n$ only when they all possess equal values in modulus. Further, $|\mathcal{C}_{f,g}(\mathbf{u})| \geq 0$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. Therefore the minimum value of $\triangle_{f,g}$ is $\sqrt{\sigma_{f,g}/2^n} = \sqrt{2^{2n}/2^n} = 2^{\frac{n}{2}}$, that is, $\triangle_{f,g} \geq 2^{\frac{n}{2}}$.

Further, the sum $\sum_{\mathbf{u}\in\mathbb{Z}_2^n\setminus\{0\}} \mathcal{C}_{f,g}^2(\mathbf{u}) = 2^{2n} - |\mathcal{C}_{f,g}(\mathbf{0})|^2$ has $2^n - 1$ non-negative terms on its left side, and therefore $\max_{\mathbf{u}\in\mathbb{Z}_2^n\setminus\{0\}} |\mathcal{C}_{f,g}(\mathbf{u})| \geq \sqrt{\frac{2^{2n}-|\mathcal{C}_{f,g}(0)|^2}{2^n-1}}$. □

Corollary 2.4. *If $g \in \mathcal{GB}_n^q$ is generalized bent and $|\mathcal{C}_{f,g}(0)| < 2^{\frac{n}{2}}$, then $\max_{\mathbf{u}\in\mathbb{Z}_2^n\setminus\{\mathbf{0}\}} |\mathcal{C}_{f,g}(\mathbf{u})| > 2^{\frac{n}{2}}$, for all $g \in \mathcal{GB}_n^q$.*

The relationship between the Walsh-Hadamard spectrum and the autocorrelation of any two generalized Boolean functions.

Theorem 2.6. *Let $f, g \in \mathcal{GB}_n^q$, and $\mathbf{u} \in \mathbb{Z}_2^n$, then we have*

$$2^n \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^2 \left|\mathcal{H}_g(\mathbf{x}+\mathbf{u})\right|^2 = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{C}_f(\mathbf{x})\mathcal{C}_g(\mathbf{x})(-1)^{<\mathbf{x},\mathbf{u}>} \tag{2.11}$$

Proof. Let $\mathbf{u} \in \mathbb{Z}_2^n$. Using (ii) of Corollary 2.1, we have

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^2 \left|\mathcal{H}_g(\mathbf{x}+\mathbf{u})\right|^2 &= 2^{-2n} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \mathcal{C}_f(\mathbf{y})(-1)^{\mathbf{y}\cdot\mathbf{x}} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} \mathcal{C}_g(\mathbf{z})(-1)^{\mathbf{z}\cdot(\mathbf{x}+\mathbf{u})} \\ &= 2^{-2n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} \mathcal{C}_f(\mathbf{y})\mathcal{C}_g(\mathbf{z})(-1)^{\mathbf{z}\cdot\mathbf{u}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{x}\cdot(\mathbf{y}+\mathbf{z})} \\ &= 2^{-n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \sum_{\mathbf{z}\in\mathbb{Z}_2^n} \mathcal{C}_f(\mathbf{y})\mathcal{C}_g(\mathbf{z})(-1)^{\mathbf{z}\cdot\mathbf{u}}\delta_{\mathbf{0}}(\mathbf{y}+\mathbf{z}) = 2^{-n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \mathcal{C}_f(\mathbf{y})\mathcal{C}_g(\mathbf{y})(-1)^{\mathbf{y}\cdot\mathbf{u}}\end{aligned}$$

□

Taking $f = g$ in the above theorem, we have the following

Corollary 2.5. *Let $f \in \mathcal{B}_{n,q}$. Then for any $\beta \in \mathbb{Z}_q^n$, we have*

$$2^n \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^2 \left|\mathcal{H}_f(\mathbf{x}+\mathbf{u})\right|^2 = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left(\mathcal{C}_f(\mathbf{x})\right)^2 (-1)^{\mathbf{x}\cdot\mathbf{u}}. \tag{2.12}$$

Further, if $\mathbf{u} = 0$, *then*

$$\sigma_f = 2^n \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^4. \tag{2.13}$$

The following corollary is shown in different context in [12, Theorem 4.2(a)] is obtained, in current notion, by putting $\mathbf{u} = 0$ in (2.11) and using (2.10).

Corollary 2.6. *For any $f, g \in \mathcal{GB}_n^q$, we have*

$$\sigma_{f,g} = 2^n \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^2 \left|\mathcal{H}_g(\mathbf{x})\right|^2. \tag{2.14}$$

Corollary 2.7. *Let $f, g \in \mathcal{GB}_n^q$, then $\sigma_{f,g} \le 2^{3n}$.*

Proof. Using (1.1) in the above corollary, we have

$$\sigma_{f,g} = 2^n \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^2 \left|\mathcal{H}_g(\mathbf{x})\right|^2 \le 2^n \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{x})\right|^2 \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left|\mathcal{H}_g(\mathbf{x})\right|^2 = 2^{3n}.$$

□

A generalized Boolean function $f \in \mathcal{GB}_n^q$ ($q = 2^h$, $h \le n$) is balanced if for every $k \in \mathbb{Z}_q$, the cardinality of the set $\{\mathbf{x} \in \mathbb{Z}_2^n : f(\mathbf{x}) = k\}$ is $\frac{2^n}{q}$. Generalized balanced Boolean function exists only if q divides 2^n. The two functions $f, g \in \mathcal{GB}_n^q$ are said to be *perfectly uncorrelated* if $\mathcal{H}_f(\mathbf{u})\mathcal{H}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. The following results were shown in different contexts in [12, 17]. One can straightforwardly infer by modifying those results hold under the current notion, as well.

Theorem 2.7. *Let $f, g \in \mathcal{GB}_n^q$, then*

(1) $\triangle_{f,g} = 0$ *if and only if* $f(\mathbf{x}) - g(\mathbf{x}+\mathbf{u})$ *is balanced for every* $\mathbf{u} \in \mathbb{Z}_2^n$.

(2) $\triangle_{f,g} = q^n$ *if and only if* $f(\mathbf{x}) = g(\mathbf{x}+\mathbf{u}) + a$, *where* $a \in \mathbb{Z}_q$ *for some* $\mathbf{u} \in \mathbb{Z}_2^n$.

(3) $0 \le \triangle_{f,g} \le q^n$.

Theorem 2.8. *Let $f, g \in \mathcal{GB}_n^q$, then*

(a) $|\mathcal{C}_{f,g}(0)|^2 \le \sigma_{f,g} \le 2^{3n}$

(*b*) $\sigma_{f,g} = 2^{3n}$ *if and only if* f *and* g *both are the functions of the form* $\psi_{\mathbf{u},d}(\mathbf{x}) = \left(\frac{q}{2}\right)\mathbf{u}\cdot\mathbf{x} + d, \mathbf{u} \in \mathbb{Z}_2^n, d \in \mathbb{Z}_q$.

(*c*) $\sigma_{f,g} = |C_{f,g}(0)|^2$ *if and only if* f *and* g *are either generalized bents or perfectly uncorrelated.*

In Theorem 2.9 below we proved that the four indicators $\sigma_{f,g}, \triangle_{f,g}, \sigma_f$ and $\triangle_g$ are invariant under the affine transformation as represented in (2.15).

Theorem 2.9. *The SSMI and MI both of a generalized Boolean function are invariant under the affine transformation*

$$g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) + \mathbf{b}\cdot\mathbf{x} + d, \textit{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{2.15}$$

where $A \in GL(2,n), \mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n, d \in \mathbb{Z}_q$.

Proof. Let $g_1(\mathbf{x}) = f_1(\mathbf{x}A \oplus \mathbf{a}) + \mathbf{b}\cdot\mathbf{x} + d$ and $g_2(\mathbf{x}) = f_2(\mathbf{x}A \oplus \mathbf{a}) + \mathbf{b}\cdot\mathbf{x} + d$. Then it is shown in [13] that $C_{g_1,g_2}(\mathbf{u}) = \overline{\zeta}^{-\mathbf{u}\cdot\mathbf{b}} C_{f_1,f_2}(\mathbf{u}A)$, for all $\mathbf{u} \in \mathbb{Z}_2^n$, which implies that $|C_{g_1,g_2}(\mathbf{u})| = |C_{f_1,f_2}(\mathbf{u}A)|$ for all $\mathbf{u} \in \mathbb{Z}_2^n$ and therefore, we have

$$\sigma_{g_1,g_2} = \sigma_{f_1,f_2}, \text{ and } \triangle_{g_1,g_2} = \triangle_{f_1,f_2}.$$

In particular for $g_1 = g_2 = g$ (i.e., $f_1 = f_2 = f$) we have $|C_g(\mathbf{u})| = |C_f(\mathbf{u}A)|$ for all $\mathbf{u} \in \mathbb{Z}_2^n$ implying that $\sigma_g = \sigma_f$. Further, $\mathbf{u}A \neq \mathbf{0}$ if $\mathbf{u} \neq \mathbf{0}$ as A is invertible. Thus, we have $\triangle_g = \triangle_f$. □

2.1.1. Generalized Boolean functions with optimal value of σ_f *and* δ_f

Let $\mathbf{v} = (v_r, \ldots, v_1)$. We define $f_\mathbf{v}(x_{n-r}, \ldots, x_1) = f(x_n = v_r, \ldots, x_{n-r+1} = v_1, x_{n-r}, \ldots, x_1)$. Define the vector concatenation of $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_2^r$ and $\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{Z}_2^{n-r}$ as $\mathbf{uw} = (\mathbf{u}, \mathbf{w}) = (u_r, \ldots, u_1, w_{n-r}, \ldots, w_1)$. The following lemma is [15, Lemma 3]

Lemma 2.2. *Let* $\mathbf{u} \in \mathbb{Z}_2^r$, $\mathbf{w} \in \mathbb{Z}_2^{n-r}$. *Then the autocorrelation of* $f \in \mathcal{GB}_n^q$ *is*

$$C_f(\mathbf{uw}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^r} C_{f_\mathbf{v}, f_{\mathbf{v}\oplus\mathbf{u}}}(\mathbf{w}),$$

In particular, $C_f(0,\mathbf{w}) = C_{f_0}(\mathbf{w}) + C_{f_1}(\mathbf{w})$, *and* $C_f(1,\mathbf{w}) = 2Re[C_{f_0,f_1}(\mathbf{w})]$.

The two functions $f, g \in \mathcal{GB}_n^q$ said to have complementary autocorrelation if and only if $C_f(\mathbf{u}) + C_g(\mathbf{u}) = 0$ for all $\mathbb{Z}_2^n \setminus \{\mathbf{0}\}$ [15]. The following result is direct consequence of the above lemma

Proposition 2. *Let* $f \in \mathcal{GB}_n^q$ *be expressed as*

$$f(x_n, \mathbf{x}) = (1 + x_n)f_0(\mathbf{x}) + x_n f_1(\mathbf{x}), \tag{2.16}$$

where $f_0, f_1 \in \mathcal{GB}_{n-1}$. *If* f_0 *and* f_1 *have complementary autocorrelation, then*

$$\triangle_f = 2 \max_{\mathbf{u}\in\mathbb{Z}_2^{n-1}} \left|Re[C_{f_0,f_1}(\mathbf{u})]\right|.$$

Corollary 2.8. *Let* $f \in \mathcal{GB}_n^q$ *as expressed in* (2.16), *then* $\triangle_f = 2\max_{\mathbf{u}\in\mathbb{Z}_2^{n-1}} \left|Re[C_{f_0,f_1}(\mathbf{u})]\right|$, *if the Boolean functions* f_0 *and* f_1 *both are generalized bent.*

Proof. Since $f_0, f_1 \in \mathcal{GB}_{n-1}$ are generalized bent Boolean function, therefore $C_{f_0}(\mathbf{u}) = C_{f_1}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_2^{n-1}\setminus\{\mathbf{0}\}$. Thus, by Lemma 2.2 we have $C_f(0,\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_2^{n-1} \setminus \{\mathbf{0}\}$. Further applying Lemma 2.2 we have

$$\triangle_f = \max_{(u_n,\mathbf{u})\in\mathbb{Z}_2\times\mathbb{Z}_2^{n-1}} \mid C_f(u_n,\mathbf{u}) \mid = \max_{\mathbf{u}\in\mathbb{Z}_2^{n-1}} \{\mid C_f(0,\mathbf{u}) \mid, \mid C_f(1,\mathbf{u}) \mid\} = \max_{\mathbf{u}\in\mathbb{Z}_2^{n-1}} \mid C_f(1,\mathbf{u}) \mid = 2 \max_{\mathbf{u}\in\mathbb{Z}_2^{n-1}} \mid C_{f_0,f_1}(\mathbf{u}) \mid.$$

□

Let $n = 2m$, where m be a positive integer. Suppose that E_i $(i = 1, 2, \ldots, 2^m + 1)$ are m-dimensional subspaces of $\mathbb{Z}_2^n$ with $E_i \cap E_j = \{0\}$, if $i \neq j$. Recently, Stănica et al. [15, Theorem 9] constructed a class of generalized bent Boolean function (and refer it as *generalized Dillon class* (GD)), is given in the following.

Lemma 2.3. *[15, Theorem 9] Let $n = 2m$ and $k, \ell_1, \dots, \ell_{2^m+1}$ be integers such that $\sum_{i=1}^{2^m+1} \zeta^{\ell_i} = \zeta^k$. Let $F : \mathbb{Z}_2^n \to \mathbb{C}$ be given by $F(\mathbf{x}) = \sum_{i=1}^{2^m+1} \zeta^{\ell_i} \phi_{E_i}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$. Then the function $f \in \mathcal{GB}_n^q$ defined by*

$$\zeta^{f(\mathbf{x})} = F(\mathbf{x}) \textit{ for all } \mathbf{x} \in \mathbb{Z}_2^n \tag{2.17}$$

is a generalized bent function.

They identify a subclass of GD in $\mathcal{GB}_n^4$ [15, Theorem 13] which have optimal (minimum) value the the cross-correlation spectrum, in absolute, is given in the following

Lemma 2.4. *[15, Theorem 13] Let $f, g \in \mathcal{GB}_n^4$ be two Dillon type generalized bent functions such that $\imath^{f(\mathbf{x})} = \sum_{i=1}^{2^m+1} \imath^{a_i} \phi_{E_i}(\mathbf{x})$ and $\imath^{g(\mathbf{x})} = \sum_{i=1}^{2^m+1} \imath^{b_i} \phi_{E_i}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$ and $\sum_{i=1}^{2^m+1} \imath^{a_i} = \imath^k$, $\sum_{i=1}^{2^m+1} \imath^{a_i} = \imath^\ell$. If $\sum_{i=1}^{2^m+1} \sum_{j=1, j \neq i}^{2^m+1} \imath^{a_i - b_j} = \imath^{k-\ell}$, then*

$$C_{f,g}(\mathbf{u}) = \begin{cases} 2^m \imath^{a_i - b_i}, & \textit{if } \mathbf{u} \neq 0 \\ 2^m \imath^{k-\ell}, & \textit{if } \mathbf{u} = 0. \end{cases} \tag{2.18}$$

Remark 2.1. The results of Lemma 2.4 can be extended to at least for any even q.

Further, they generalized a result of Schmidt [11, Thm. 5.3] (obtained for $q = 4$). The class of functions as represented in (2.19) below is referred to as the *generalized Maiorana–McFarland class* (GMMF).

Lemma 2.5. *[15, Thm. 8] Suppose that q is an even positive integer. Let σ be a permutation on $\mathbb{Z}_2^m$, and let $g \in \mathcal{GB}_m^q$. Then the function $f_{\sigma,g} : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_q$ expressed as*

$$f_{\sigma,g}(\mathbf{x}, \mathbf{y}) = g(\mathbf{y}) + \left(\frac{q}{2}\right) \mathbf{x} \cdot \sigma(\mathbf{y}) \textit{ for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m \tag{2.19}$$

is a generalized bent. The dual of $f_{\sigma,g}$ is $g(\sigma^{-1}(\mathbf{x})) + \left(\frac{q}{2}\right) \mathbf{y} \cdot (\sigma^{-1}(\mathbf{x}))$, that is, $\mathcal{H}_{f_{\sigma,g}}(\mathbf{x}, \mathbf{y}) = \zeta^{g(\sigma^{-1}(\mathbf{x})) + (\frac{q}{2}) \mathbf{y} \cdot (\sigma^{-1}(\mathbf{x}))}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$.

Let us denote $\mathrm{S}_m(\mathbb{Z}_2)$ be the set of all permutations on $\mathbb{Z}_2^m$. Define a set $\mathcal{P}_m$ as $\mathcal{P}_m = \{(\sigma_1, \sigma_2) \in \mathrm{S}_m(\mathbb{Z}_2) \times \mathrm{S}_m(\mathbb{Z}_2) : \sigma_1^{-1} \oplus \sigma_2^{-1} \in \mathrm{S}_m(\mathbb{Z}_2)\}$. Recently, another subclass of GMMF is identified in [13, Theorem 3.2] which have optimal (minimum) value the the cross-correlation spectrum, in absolute, is given in the following

Lemma 2.6. *[13, Theorem 3.2] Suppose that q be a positive even integer. Let $f_{\sigma_1,g_1}, f_{\sigma_2,g_2}$ be two functions in GMMF $\subseteq \mathcal{GB}_n^q$, that is, $f_{\sigma_1,g_1}(\mathbf{x}, \mathbf{y}) = g_1(\mathbf{y}) + \left(\frac{q}{2}\right) \mathbf{x} \cdot \sigma_1(\mathbf{y})$ and $f_{\sigma_2,g_2}(\mathbf{x}, \mathbf{y}) = g_2(\mathbf{y}) + \left(\frac{q}{2}\right) \mathbf{x} \cdot \sigma_2(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$, where σ_1, σ_2 are permutations on $\mathbb{Z}_2^m$ and $g_1, g_2 \in \mathcal{GB}_m^q$. If $\sigma_1, \sigma_2 \in \mathcal{P}_m$, then*

$$|C_{f_{\sigma_1,g_1}, f_{\sigma_2,g_2}}(\mathbf{u}, \mathbf{v})| = 2^m, \textit{ for all } (\mathbf{u}, \mathbf{v}) \in \mathbb{Z}_2^m \times \mathbb{Z}_2^m.$$

The following result follows from Corollary 2.8 and Lemma 2.6

Theorem 2.10. *Let $n = 2m + 1$, and let the function $f : \mathbb{Z}_2 \times \mathbb{Z}_2^{n-1} \to \mathbb{Z}_q$ is expressed as*

$$f(x_n, \mathbf{x}) = (1 + x_n) f_0(\mathbf{x}) + x_n f_1(\mathbf{x}),$$

where $f_0, f_1 \in \mathcal{GB}_{2m}^q$ are two GMMF type functions as represented in Lemma 2.6, that is, $f_0(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi_0(\mathbf{y}) + g_0(\mathbf{y})$ and $f_1(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi_1(\mathbf{y}) + \ g_1(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$, $g_0, g_1 \in \mathcal{GB}_m^q$ and $\pi_0, \pi_1 \in \mathcal{P}_m$, then $\triangle_f = 2^{\frac{n+1}{2}}$, and $\sigma_f = 2^{2n+1}$.

From Corollary 2.8 and Lemma 2.4, we have following

Theorem 2.11. *Let $n = 2m + 1$, and let the function $f : \mathbb{Z}_2 \times \mathbb{Z}_2^{n-1} \to \mathbb{Z}_4$ is expressed as*

$$f(x_n, \mathbf{x}) = (1 + x_n) f_0(\mathbf{x}) + x_n f_1(\mathbf{x}),$$

where $f_0, f_1 \in \mathcal{GB}_{2m}^4$ are two Dillon type generalizedfunctions such that $\imath^{f_0(\mathbf{x})} = \sum_{i=1}^{2^m+1} \imath^{a_i} \phi_{E_i}(\mathbf{x})$ and $\imath^{f_1(\mathbf{x})} = \sum_{i=1}^{2^m+1} \imath^{b_i} \phi_{E_i}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$ and $\sum_{i=1}^{2^m+1} \imath^{a_i} = \imath^k$, $\sum_{i=1}^{2^m+1} \imath^{a_i} = \imath^\ell$. If $\sum_{i=1}^{2^m+1} \sum_{j=1, j \neq i}^{2^m+1} \imath^{a_i - b_j} = \imath^{k-\ell}$, then $\triangle_f = 2^{\frac{n+1}{2}}$, and $\sigma_f = 2^{2n+1}$.

Remark 2.2. Let $g \in \mathcal{GB}_n^q$ is obtained by $f \in \mathcal{GB}_n^q$ under the transformation given below

$$g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{a}) + \epsilon\, \mathbf{b} \cdot \mathbf{x} + d, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{2.20}$$

where $A \in GL(2, n)$, $\mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n$, $d \in \mathbb{Z}_q$, and $\epsilon = \begin{cases} 0, \ q/2 & if\ q \text{ is even} \\ 0 & if\ q \text{ is odd} \end{cases}$. It is shown in [15, Theorem 5] that property the generalized bent of generalized Boolean functions is preserved under the affine transformation as represented in (2.20). The set of all the generalized Boolean functions as represented in (2.20) *a complete class*, specially, it is referred to as *generalized Maiorana–McFarland complete class* ($\widehat{GMMF}$) if $f \in$ GMMF . Similarly, $\widehat{GD}$ denotes the complete class GD. Thus, from Theorem 2.10 and Theorem 2.11 we conclude that there exists two large classes of generalized Boolean functions in odd variables for which the indicators σ_f, and δ_f have optimal value.

2.1.2. A class of semi-bent Boolean functions with optimal value of SSMI and MI

In binary case, the modulus indicator is additive autocorrelation and SSMI is the sum-of-squares indicators. In this section, we identify a class of semi-bent Boolean functions with optimal value of SSMI and MI in n variables constructed from bent functions in $n-1$ variables. Let n be an odd integer. Dillon [5] demonstrated that a function $f : \mathbb{Z}_2 \times \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$ expressed as

$$f(x_n, \mathbf{x}) = (1 + x_n)f_0(\mathbf{x}) + x_n f_1(\mathbf{x}), \tag{2.21}$$

where $f_0, f_1 \in \mathcal{B}_{n-1}$ are bent functions, is semi-bent, and therefore, by Corollary 3.1 $\sigma_f = 2^{2n+1}$. Thus, by Corollary 2.8 for $q = 2$, we have the following

Corollary 2.9. *The function f as constructed in* (2.21) *is semi-bent, and*

$$\triangle_f = 2 \max_{\mathbf{u} \in \mathbb{Z}_2^{n-1}} \mid C_{f_0, f_1}(\mathbf{u}) \mid, \textit{ and } \sigma_f = 2^{2n+1}.$$

The following proposition is direct consequence of the above corollary and Theorem 2.10.

Proposition 3. *Let $n = 2m+1$, and $f_0, f_1 \in \mathcal{B}_{2m}$ are two Maiorana-McFarland type bent functions as given in [12, Theorem 4.4], that is $f_0(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi_0(\mathbf{y}) + g_0(\mathbf{y})$ and $f_1(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \pi_1(\mathbf{y}) + g_1(\mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$, where $g_0, g_1 \in \mathcal{B}_m$ and π_0, π_1 are permutations on $\mathbb{Z}_2^m$ such that $\pi_0^{-1} \oplus \pi_1^{-1}$ is also a permutation, then the function $f : \mathbb{Z}_2 \times \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$ expressed as*

$$f(x_n, \mathbf{x}) = (1 + x_n)f_0(\mathbf{x}) + x_n f_1(\mathbf{x}),$$

f is semi-bent function with optimal values of SSMI and MI both, that is $\sigma_f = 2^{2n+1}$ and $\triangle_f = 2^{\frac{n+1}{2}}$.

3. Constructions of generalized s-plateaued Boolean functions

In this section, we obtain the SSMI for generalized s-plateaued functions (the function $f \in \mathcal{GB}_n^q$ for which $2^{\frac{n}{2}}|\mathcal{H}_f(\mathbf{u})|$ is either 0 or $2^{\frac{n+s}{2}}$ is called s-plateaued). Further, we constructed a class of generalized semi-bent Boolean functions for odd n (1-plateaued functions) and another class of generalized semi-bent Boolean functions for even n (2-plateaued functions), and obtained their SSMI.

Theorem 3.1. *The SSMI of a generalized s-plateaued ($s = 1, 2, \ldots, n$) function $f \in \mathcal{GB}_n, q$ is 2^{2n+s}.*

Proof. Since $f \in \mathcal{GB}_n, q$ be a s-plateaued generalized Boolean function. Therefore, $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{\frac{s}{2}}\}$ for every $\mathbf{u} \in \mathbb{Z}_2^n$. Suppose if k be the number of vectors $\mathbf{u}'s$ for which $\mathcal{H}_f(\mathbf{u}) \neq 0$. Then by Parseval's identity we have $k = 2^{n-s}$. Now, from (2.13) we have

$$\sigma_f = 2^n \sum_{\mathbf{u} \in \mathbb{Z}_2^n} \mid \mathcal{H}_f(\mathbf{u}) \mid^4 = 2^n \cdot 2^{n-s} \cdot (2^{\frac{s}{2}})^4 = 2^{2n+s}.$$

□

In particular for $s = 1, 2$, we have the following corollary

Corollary 3.1. *The SSMI of a generalized semi-bent Boolean function $f \in \mathcal{B}_{n,q}$ is 2^{2n+1} if n is odd, and q^{2n+2} if n is even.*

Theorem 3.2. *Let n, s be two integers such that $n + s$ is even. Let $g \in \mathcal{GB}_{\frac{n-s}{2}}$ and $\phi : \mathbb{Z}_2^{\frac{n-s}{2}} \to \mathbb{Z}_2^{\frac{n+s}{2}}$ be an injective function, then a functionf : $\mathbb{Z}_2^{\frac{n+s}{2}} \times \mathbb{Z}_2^{\frac{n-s}{2}} \to \mathbb{Z}_q$ (q is an even integer) expressed as*

$$f(\mathbf{x},\mathbf{y}) = \left(\frac{q}{2}\right)\mathbf{x}\cdot\phi(\mathbf{y}) + g(\mathbf{y}),\ \textit{for all}\ (\mathbf{x},\mathbf{y}) \in \mathbb{Z}_2^{\frac{n+s}{2}} \times \mathbb{Z}_2^{\frac{n-s}{2}} \tag{3.1}$$

is s-plateaued generalized Boolean function.

Proof. Let $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_2^{\frac{n+s}{2}} \times \mathbb{Z}_2^{\frac{n-s}{2}}$, then

$$\begin{aligned}\mathcal{H}_f(\mathbf{u},\mathbf{v}) &= 2^{-\frac{n}{2}} \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{Z}_2^{\frac{n+s}{2}}\times\mathbb{Z}_2^{\frac{n-s}{2}}} \zeta^{f(\mathbf{x},\mathbf{y})}(-1)^{\mathbf{u}\cdot\mathbf{x}+\mathbf{v}\cdot\mathbf{y}} = 2^{-\frac{n}{2}} \sum_{\mathbf{y}\in\mathbb{Z}_2^{\frac{n-s}{2}}} \zeta^{g(\mathbf{y})+(\frac{q}{2})\mathbf{v}\cdot\mathbf{y}} \sum_{\mathbf{x}\in\mathbb{Z}_2^{\frac{n+s}{2}}} (-1)^{\mathbf{x}\cdot(\phi(\mathbf{y})+\mathbf{u})}\\ &= 2^{\frac{s}{2}} \sum_{\mathbf{y}\in\mathbb{Z}_2^{\frac{n-s}{2}}} \zeta^{g(\mathbf{y})+(\frac{q}{2})\mathbf{v}\cdot\mathbf{y}}\delta_{\mathbf{0}}(\phi(\mathbf{y})+\mathbf{u}) = \begin{cases} 2^{\frac{s}{2}}\zeta^{g(\mathbf{y})+(\frac{q}{2})\mathbf{v}\cdot\mathbf{y}}, & if\ \ \mathbf{y} = \phi^{-1}(\mathbf{u}),\\ 0 & otherwise.\end{cases}\end{aligned} \tag{3.2}$$

which implies that f is s-plateaued generalized Boolean function.

□

Corollary 3.2. *Let n be an odd integer. Let $g \in \mathcal{GB}_{\frac{n-1}{2}}$, and $\phi : \mathbb{Z}_2^{\frac{n-1}{2}} \to \mathbb{Z}_2^{\frac{n+1}{2}}$ be an injective function, then a function $f : \mathbb{Z}_2^{\frac{n+1}{2}} \times \mathbb{Z}_2^{\frac{n-1}{2}} \to \mathbb{Z}_q$ (q is an even integer) expressed as*

$$f(\mathbf{x},\mathbf{y}) = \left(\frac{q}{2}\right)\mathbf{x}\cdot\phi(\mathbf{y}) + g(\mathbf{y}),\ \textit{for all}\ (\mathbf{x},\mathbf{y}) \in \mathbb{Z}_2^{\frac{n+1}{2}} \times \mathbb{Z}_2^{\frac{n-1}{2}}$$

is generalized semi-bent Boolean function.

Corollary 3.3. *Let n be an even integer. Let $g \in \mathcal{GB}_{\frac{n-2}{2}}$, and $\phi : \mathbb{Z}_2^{\frac{n-2}{2}} \to \mathbb{Z}_2^{\frac{n+2}{2}}$ be any injective function, then a function $f : \mathbb{Z}_2^{\frac{n+2}{2}} \times \mathbb{Z}_2^{\frac{n-2}{2}} \to \mathbb{Z}_q$ (q is an even integer) expressed as*

$$f(\mathbf{x},\mathbf{y}) = \left(\frac{q}{2}\right)\mathbf{x}\cdot\phi(\mathbf{y}) + g(\mathbf{y}),\ \textit{for all}\ (\mathbf{x},\mathbf{y}) \in \mathbb{Z}_2^{\frac{n+2}{2}} \times \mathbb{Z}_2^{\frac{n-2}{2}}$$

is generalized semi-bent Boolean function.

In Theorem 3.3 below we demonstrate that the direct sum of f, g- the two generalized semi-bent functions is generalized semi-bent if both f and g are defined on odd number of variables.

Theorem 3.3. *Let $f_1 \in \mathcal{GB}_r^q$ and $f_2 \in \mathcal{GB}_s^q$, where r and s are positive integers. Then a function $g : \mathbb{Z}_2^r \times \mathbb{Z}_2^s \to \mathbb{Z}_q$ expressed as*

$$g(\mathbf{x},\mathbf{y}) = f_1(\mathbf{x}) + f_2(\mathbf{y}),\ \textit{for all}\ \mathbf{x} \in \mathbb{Z}_2^r, \mathbf{y} \in \mathbb{Z}_2^s,$$

is generalized semi-bent if f_1 and f_2 both are generalized semi-bent Boolean functions.

Proof. Let f_1 and f_2 be generalized semi-bent Boolean functions on $\mathbb{Z}_2^r$ and $\mathbb{Z}_2^s$ respectively, then $|\mathcal{H}_{f_1}(\mathbf{u})|, |\mathcal{H}_{f_2}(\mathbf{v})| \in \{0, \sqrt{2}\}$ for all $\mathbf{u} \in \mathbb{Z}_2^r$, $\mathbf{v} \in \mathbb{Z}_2^s$, and therefore $|\mathcal{H}_g(\mathbf{u},\mathbf{v})| = |\mathcal{H}_{f_1}(\mathbf{u})||\mathcal{H}_{f_2}(\mathbf{v})| \in \{0, 2\}$ for all $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s$ which implies that g is generalized semi-bent Boolean function. □

4. Constructions of generalized partially bent Boolean functions

A function $f \in \mathcal{GB}_n^q$ is *generalized partially bent* Boolean function if $(2^n - N_{C_f})(2^n - N_{\mathcal{H}_f}) = 2^n$, where $N_{C_f} = |\{\mathbf{x} \in \mathbb{Z}_2^n : C_f(\mathbf{x}) = 0\}|$ and $N_{\mathcal{H}_f}(\mathbf{x}) = |\{\mathbf{x} \in \mathbb{Z}_2^n : \mathcal{H}_f(\mathbf{x}) = 0\}|$.

Theorem 4.1. *Let $f \in \mathcal{GB}_n^q$. Then*

(*i*) $(2^n - N_{C_f})(2^n - N_{\mathcal{H}_f}) \geq 2^n$, *and*

(*ii*) *f is generalized partially bent if and only if* $(*)$ *There exists* $\mathbf{a} \in \mathbb{Z}_2^n$ *such that* $C_f(\mathbf{u}) \in \{0, (-1)^{\mathbf{u}\cdot\mathbf{a}}\, 2^n\}$ *for all* $\mathbf{u} \in \mathbb{Z}_2^n$, *and* $(**)$ $|\mathcal{H}_f(\mathbf{x})|^2$ *is constant for all* $\mathbf{x} \in \mathbb{Z}_2^n$ *whenever* $\mathcal{H}_f(\mathbf{x}) \neq 0$.

Proof. (*i*) Since $\frac{|C_f(\mathbf{x})|}{2^n} \leq 1$ for all $\mathbf{x} \in \mathbb{Z}_2^n$. Using Triangle Inequality: $|z_1 + z_2| \leq |z_1| + |z_1|$ for all $z_1, z_2 \in \mathbb{C}$, we have

$$\begin{aligned} 2^n - N_{C_f} &= \left|\{\mathbf{x} \in \mathbb{Z}_2^n : C_f(\mathbf{x}) \neq 0\}\right| \geq 2^{-n} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} |C_f(\mathbf{x})| \\ &\geq 2^{-n} \left| \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{y})-f(\mathbf{y}\oplus\mathbf{x})} \right| = 2^{-n} \left| \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \zeta^{-f(\mathbf{u})} \right| = \left| \mathcal{H}_f(\mathbf{0})\overline{\mathcal{H}_f(\mathbf{0})} \right| = |\mathcal{H}_f(\mathbf{0})|^2. \end{aligned} \tag{4.1}$$

Let $f_1 \in \mathcal{GB}_n^q$ such that $f_1(\mathbf{x}) = f(\mathbf{x}) + \left(\frac{q}{2}\right)\mathbf{x}\cdot\mathbf{a}$, then we have,

$$C_{f_1}(\mathbf{x}) = (-1)^{\mathbf{a}\cdot\mathbf{x}} C_f(\mathbf{x}), \text{ and } \mathcal{H}_{f_1}(\mathbf{x}) = \mathcal{H}_f(\mathbf{x}\oplus\mathbf{a}) \tag{4.2}$$

Thus, for any $\mathbf{a} \in \mathbb{Z}_2^n$, using (4.1) and (4.2), we have $2^n - N_{C_f} = 2^n - N_{C_{f_1}} \geq |\mathcal{H}_{f_1}(\mathbf{0})|^2 = 2^n|\mathcal{H}_f(\mathbf{a})|^2$, this implies that

$$2^n - N_{C_f} \geq |\mathcal{H}_f(\mathbf{w})|^2, \tag{4.3}$$

where $|\mathcal{H}_f(\mathbf{w})|^2 = \max\{|\mathcal{H}_f(\mathbf{x})|^2 : \mathbf{x} \in \mathbb{Z}_2^n\}$, and so, $\frac{|\mathcal{H}_f(\mathbf{x})|^2}{|\mathcal{H}_f(\mathbf{w})|^2} \leq 1$ for all $\mathbf{x} \in \mathbb{Z}_2^n$. Using (1.1), we have

$$2^n - N_{\mathcal{H}_f} \geq \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \frac{|\mathcal{H}_f(\mathbf{x})|^2}{|\mathcal{H}_f(\mathbf{w})|^2} = \frac{1}{|\mathcal{H}_f(\mathbf{w})|^2} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 = \frac{2^n}{|\mathcal{H}_f(\mathbf{w})|^2}. \tag{4.4}$$

Combining (4.3) and (4.4), we have

$$(2^n - N_{\mathcal{H}_f})(2^n - N_{C_f}) \geq 2^n. \tag{4.5}$$

(*ii*) Suppose f is partially generalized bent, that is, $(2^n - N_{\mathcal{H}_f})(2^n - N_{C_f}) = 2^n$, then $(*)$ $2^n - N_{C_f} = \max\{|\mathcal{H}_f(\mathbf{x})| : \mathbf{x} \in \mathbb{Z}_2^n\}$ and $(**)$ $2^n - N_{\mathcal{H}_f} = \frac{2^n}{\max\{|\mathcal{H}_f(\mathbf{x})| : \mathbf{x}\in\mathbb{Z}_2^n\}}$. Let $\mathbf{a} \in \mathbb{Z}_2^n$ such that $|\mathcal{H}_f(\mathbf{a})| = \max\{|\mathcal{H}_f(\mathbf{x})| : \mathbf{x} \in \mathbb{Z}_2^n\}$, and let $f_1 \in \mathcal{GB}_n^q$ such that $f_1(\mathbf{x}) = f(\mathbf{x}) + \left(\frac{q}{2}\right)\mathbf{x}\cdot\mathbf{a}$. Then by $(*)$

$$\begin{aligned} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} C_{f_1}(\mathbf{x}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f_1(\mathbf{y})-f_1(\mathbf{y}\oplus\mathbf{x})} = \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{f_1(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \zeta^{-f_1(\mathbf{u})} = 2^n|\mathcal{H}_{f_1}(\mathbf{0})|^2 \\ &= 2^n|\mathcal{H}_f(\mathbf{a})|^2 = 2^n(2^n - N_{C_f}) = 2^n(2^n - N_{C_{f_1}}) = \sum_{x : C_{f_1}(\mathbf{x})\neq 0} 2^n, \end{aligned} \tag{4.6}$$

which implies that $C_{f_1}(\mathbf{x}) = 0$ or 2^n because of $|C_{f_1}(\mathbf{x})| \leq 2^n$. Now, using (4.2) we have $C_f(\mathbf{x}) = 0$ or $(-1)^{\mathbf{a}\cdot\mathbf{x}}2^n$.

Next, by assumption $(**)$ and (1.1), we have

$$2^n - N_{\mathcal{H}_f} = \sum_{\mathbf{x}:\mathcal{H}_f(\mathbf{x})\neq 0} 1 = \frac{2^n}{\max\{|\mathcal{H}_f(\mathbf{x})|^2 : \mathbf{x} \in \mathbb{Z}_2^n\}} = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left(\frac{|\mathcal{H}_f(\mathbf{x})|^2}{|\mathcal{H}_f(\mathbf{a})|^2} \right), \tag{4.7}$$

which implies that $|\mathcal{H}_f(\mathbf{x})|^2 = |\mathcal{H}_f(\mathbf{a})|^2$ for $\mathbf{x} \in \mathbb{Z}_2^n$ and $\mathcal{H}_f(\mathbf{x}) \neq 0$. This shows that $|\mathcal{H}_f(\mathbf{w})|^2$ is constant for $\mathbf{w} \in \mathbb{Z}_2^n$ and $\mathcal{H}_f(\mathbf{w}) \neq 0$.

Conversely, suppose that there exists $\mathbf{a} \in \mathbb{Z}_2^n$, such that for any $\mathbf{u} \in \mathbb{Z}_2^n$, $C_f(\mathbf{u})$ is either 0 or $(-1)^{\mathbf{u}\cdot\mathbf{a}}\, 2^n$, and $|\mathcal{H}_f(\mathbf{x})|^2$ is a constant for $\mathbf{x} \in \mathbb{Z}_2^n$ and $\mathcal{H}_f(\mathbf{x}) \neq 0$.

Assume that $E = \{\mathbf{x} \in \mathbb{Z}_2^n : C_f(\mathbf{x}) = 2^n(-1)^{\mathbf{a}\cdot\mathbf{x}}\}$, $f_1(\mathbf{x}) = f(\mathbf{x}) \oplus \mathbf{a}\cdot\mathbf{x}$, then from (4.2), $C_{f_1}(\mathbf{x}) = 0$ or 2^n. Thus, $E = \{\mathbf{x} \in \mathbb{Z}_2^n : C_{f_1}(\mathbf{x}) = 2^n\}$. First, we show that E is subspace of $\mathbb{Z}_2^n$. Suppose $\mathbf{u}, \mathbf{v} \in E$, then $C_f(\mathbf{u}) = 2^n(-1)^{\mathbf{u}\cdot\mathbf{a}}$ and

$C_f(\mathbf{v}) = 2^n(-1)^{\mathbf{v}\cdot\mathbf{a}}$, that is $f(\mathbf{x}\oplus\mathbf{u}) = f(\mathbf{x}) + \left(\frac{q}{2}\right)\mathbf{u}\cdot\mathbf{a}$ and $f(\mathbf{x}\oplus\mathbf{v}) = f(\mathbf{x}) + \left(\frac{q}{2}\right)\mathbf{v}\cdot\mathbf{a}$ for all $\mathbf{x}\in\mathbb{Z}_2^n$. Therefore,

$$\begin{aligned} C_f(\mathbf{u}\oplus\mathbf{v}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-f(\mathbf{x}\oplus\mathbf{u}\oplus\mathbf{v})} = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-f((\mathbf{x}\oplus\mathbf{u})\oplus\mathbf{v})} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})-(f(\mathbf{x}+\mathbf{u})+\left(\frac{q}{2}\right)\mathbf{v}\cdot\mathbf{a})} = (-1)^{\mathbf{v}\cdot\mathbf{a}}C_f(\mathbf{u}) = 2^n(-1)^{(\mathbf{u}\oplus\mathbf{v})\cdot\mathbf{x}}, \end{aligned} \tag{4.8}$$

implies that $\mathbf{u}\oplus\mathbf{v}\in E$. This proves that E is subspace of $\mathbb{Z}_2^n$. Using (*ii*) of Corollary 2.1, we have

$$|\mathcal{H}_{f_1}(\mathbf{z})|^2 = 2^{-n}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} C_{f_1}(\mathbf{x})(-1)^{\mathbf{z}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in E}(-1)^{\mathbf{z}\cdot\mathbf{x}} = |E|\phi_{E^\perp}(\mathbf{z}), \text{ for all } \mathbf{z}\in\mathbb{Z}_2^n, \tag{4.9}$$

which implies that $\mathcal{H}_{f_1}(\mathbf{z}) \neq 0$ whenever $\mathbf{z}\in E^\perp$, that is, $|E^\perp| = 2^n - N_{\mathcal{H}_{f_1}}$. From (4.2), it is clear that the Walsh-Hadamard spectrums of f and f_1 are same. This implies that $|E^\perp| = 2^n - N_{\mathcal{H}_f}$, and $|\mathcal{H}_f(\mathbf{x})|^2$ is a constant for $\mathbf{x}\in\mathbb{Z}_2^n$ and $\mathcal{H}_{f_1}(\mathbf{x})\neq 0$. Now, using (1.1) in (4.9), we have

$$2^n = |E|\sum_{\mathbf{z}\in\mathbb{Z}_2^n}\phi_{E^\perp}(\mathbf{z}) = |E|\sum_{\mathbf{z}\in E^\perp} 1 = |E||E^\perp| = (2^n - N_{C_f})(2^n - N_{\mathcal{H}_f}).$$

This completes the proof. □

It can be easily conclude that the Walsh-Hadamard spectrum as well as the autocorrelation spectrum of a generalized Boolean function is invariant, in absolute value, under the affine transformation as represented in (2.15) this implies that $(2^n - N_{C_g})(2^n - N_{\mathcal{H}_g}) = (2^n - N_{C_f})(2^n - N_{\mathcal{H}_f})$. Thus we have the following

Proposition 4. *The property of* generalized partially bent *of the generalized Boolean functions is invariant under the affine transformation as represented in* (2.15).

Proposition 5. *Let* $f\in\mathcal{GB}_n^q$ *be a* generalized partially bent *Boolean function.* $E_f = \{\mathbf{x}\in\mathbb{Z}_2^n : C_f(\mathbf{x}) = 2^n(-1)^{\mathbf{a}\cdot\mathbf{x}}\}$, $E_f\cap E_f^\perp = \{\mathbf{0}\}$, *and* $\mathbf{a}\in\mathbb{Z}_2^n$ *as defined in Theorem 4.1. Then* $f(\mathbf{x})$ *is equivalent to the addition of a generalized bent function* $g:\mathbb{Z}_2^{n-m}\to\mathbb{Z}_q$ *and an affine function* $\psi_{\mathbf{a}}:\mathbb{Z}_2^m\to\mathbb{Z}_q$ *of the form* $\psi_{\mathbf{a}}(\mathbf{x}) = \left(\frac{q}{2}\right)\mathbf{a}\cdot\mathbf{x}$, *for all* $\mathbf{x}\in\mathbb{Z}_2^m$, *where* m *in an integer such that* $|E| = 2^m$.

Proof. If $f\in\mathcal{GB}_n^q$ is generalized bent, that is, $E_f = \mathbf{0}$. In case the proof is trivial. Assume that f is not generalized bent, and hence $E_f\neq\mathbf{0}$. By (4.8) E_f is a subspace of $\mathbb{Z}_2^n$, and so, without loss of generality, assume that $E_f = \mathbb{Z}_2^m$, $1\leq m<n$. Since $\mathbb{Z}_2^n = \mathbb{Z}_2^m\oplus\mathbb{Z}_2^{n-m}$, therefore, there exists $\mathbf{a}_1\in\mathbb{Z}_2^m$ and $\mathbf{a}_2\in\mathbb{Z}_2^{n-m}$ such that $\mathbf{a} = \mathbf{a}_1 + \mathbf{a}_2$. Thus, by property of $E_f = \mathbb{Z}_2^m$, $f(\mathbf{y}+\mathbf{u}) = f(\mathbf{y}) + \left(\frac{q}{2}\right)\mathbf{u}\cdot\mathbf{a}_1$ for all $\mathbf{u}\in\mathbb{Z}_2^m$, and $y\in\mathbb{Z}_2^{n-m}$. Thus, $f(\mathbf{x}+\mathbf{u})$ is an affine function restricted in $\mathbb{Z}_2^m$.

Next, we show that f is generalized bent Boolean function restricted within $\mathbb{Z}_2^{n-m}$. Let $\mathbf{x},\mathbf{u}\in\mathbb{Z}_2^n$. Then there exists $\mathbf{x}_1,\mathbf{u}_1\in\mathbb{Z}_2^m$, and $\mathbf{x}_2,\mathbf{u}_2\in\mathbb{Z}_2^{n-m}$ such that $\mathbf{x} = \mathbf{x}_1+\mathbf{x}_2$, $\mathbf{u} = \mathbf{u}_1+\mathbf{u}_2$. Now, $f(\mathbf{x}) + \left(\frac{q}{2}\right)\mathbf{x}\cdot\mathbf{u} = f(\mathbf{x}_1+\mathbf{x}_2) + \left(\frac{q}{2}\right)((\mathbf{x}_1+\mathbf{x}_2)\cdot(\mathbf{u}_1+\mathbf{u}_2)) = f(\mathbf{x}_2) + \left(\frac{q}{2}\right)\mathbf{a}_1\cdot\mathbf{x}_1 + \left(\frac{q}{2}\right)(\mathbf{x}_1\cdot\mathbf{u}_1 + \mathbf{x}_2\cdot\mathbf{u}_2) = f(\mathbf{x}_2) + \left(\frac{q}{2}\right)(\mathbf{x}_2\cdot\mathbf{u}_2 + \mathbf{x}_1\cdot(\mathbf{a}_1+\mathbf{u}_1))$. The Walsh-Hadamard transform of f at $\mathbf{u}\in\mathbb{Z}_2^n$ is

$$\begin{aligned} |\mathcal{H}_f(\mathbf{u}) &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\zeta^{f(\mathbf{x})+\left(\frac{q}{2}\right)\mathbf{x}\cdot\mathbf{u}} = 2^{-\frac{n}{2}}\sum_{\mathbf{x}_1\in\mathbb{Z}_2^m}\sum_{\mathbf{x}_2\in\mathbb{Z}_2^{n-m}}\zeta^{f(\mathbf{x}_2)+\left(\frac{q}{2}\right)(\mathbf{x}_2\cdot\mathbf{u}_2+\mathbf{x}_1\cdot(\mathbf{a}_1+\mathbf{u}_1))} \\ &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}_2\in\mathbb{Z}_2^{n-m}}\zeta^{f(\mathbf{x}_2)}(-1)^{\mathbf{x}_2\cdot\mathbf{u}_2}\sum_{\mathbf{x}_1\in\mathbb{Z}_2^m}(-1)^{\mathbf{x}_1\cdot(\mathbf{a}_1+\mathbf{u}_1)} = 2^{\frac{2m-n}{2}}\sum_{\mathbf{x}_2\in\mathbb{Z}_2^{n-m}}\zeta^{f(\mathbf{x}_2)}(-1)^{\mathbf{x}_2\cdot\mathbf{u}_2}\phi_{\mathbb{Z}_2^{n-m}}(\mathbf{u}_1+\mathbf{a}_1) \\ &= 2^{\frac{m}{2}}\mathcal{H}_{f_{\mathbb{Z}_2^{n-m}}}(\mathbf{u}_2)\delta_{\mathbf{0}}(\mathbf{u}_1+\mathbf{a}_1), \end{aligned} \tag{4.10}$$

where $f_{\mathbb{Z}_2^{n-m}}$ denotes the restriction of f to $\mathbb{Z}_2^{n-m}$. Since f is generalized partially bent Boolean function. By Theorem 4.1, the value of $\left|\mathcal{H}_{f_{\mathbb{Z}_2^{n-m}}}(\mathbf{u}_2)\right|^2$ is constant and not equal to zero for all $\mathbf{u}_2\in\mathbb{Z}_2^{n-m}$, that is, $\left|\mathcal{H}_{f_{\mathbb{Z}_2^{n-m}}}(\mathbf{u}_2)\right| = \ell\neq 0$ for all

$\mathbf{u}_2 \in \mathbb{Z}_2^{n-m}$. Now, using (1.1), we have

$$2^n = \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \left|\mathcal{H}_f(\mathbf{u})\right|^2 = \sum_{(\mathbf{u}_1,\mathbf{u}_2)\in\mathbb{Z}_2^m\times\mathbb{Z}_2^{n-m}} \left|\mathcal{H}_f(\mathbf{u}_1,\mathbf{u}_2)\right|^2 = 2^m\ell^2 \sum_{\mathbf{u}_2\in\mathbb{Z}_2^{n-m},\mathbf{u}_1=\mathbf{a}_1} 1 = 2^m\ell^2 2^{n-m} = 2^n\ell^2, \tag{4.11}$$

implies that $\ell = \left|\mathcal{H}_{f_{\mathbb{Z}_2^{n-m}}}(\mathbf{u}_2)\right| = 1$ for all $\mathbf{u}_2 \in \mathbb{Z}_2^{n-m}$. Hence $f_{\mathbb{Z}_2^{n-m}} \in \mathcal{GB}_{n-m}^q$ is generalized bent Boolean function.

Finally, we conclude that g is the addition of the generalized bent functions restricted with in $\mathbb{Z}_2^{n-m}$, and an affine function of the form $\psi_{\mathbf{a}}$ restricted in $\mathbb{Z}_2^m$. □

Remark 4.1. Let f be a generalized partially bent Boolean function as constructed in Proposition 5, then $\delta_f = 2^n$, and $\sigma_f = 2^{m+2n}$.

References

[1] C. Carlet, *Partially bent functions*, Designs, Codes and Cryptography 4, pp. 135-145, 1993.

[2] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monograph “Boolean Models and Methods in Mathematics, Computer Science, and Engineering” published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 257–397, 2010.

[3] C. Carlet, *Vectorial Boolean Functions for Cryptography*, Chapter of the monograph “Boolean Models and Methods in Mathematics, Computer Science, and Engineering” published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 398–469, 2010.

[4] T. W. Cusick and P. Stănică, Cryptographic Boolean functions and applications, Elsevier – Academic Press, 2009.

[5] J. F. Dillon, *Elementary Hadamard difference sets*, PhD Thesis, University of Maryland, 1974.

[6] P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory (A) 40,, pp. 90–107, 1985.

[7] T. Helleseth, P. V. Kumar, Sequences with Low Correlation, In Handbook of Coding Theory, North-Holland, Amsterdam 1998, pp. 1765-1853.

[8] O. S. Rothaus, *On bent functions*, J. Combinatorial Theory Ser. A 20, pp. 300–305, 1976.

[9] P. Sarkar, S. Maitra, Constructions of nonlinear Boolean functions with important cryptographic properties, In Advances in Cryptology-Eurocrypt 2000, LNCS, vol. 1807, Springer, 2008, pp. 485-506.

[10] P. Sarkar and S. Maitra, Cross-correlation analysis of cryptographically useful Boolean functions, Theory of Computing Systems 35 (2002) 39-57.

[11] K-U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA, *IEEE Trans. Inform. Theory*, Vol. 55(4), pp. 1824-1832, 2009.

[12] D. Singh, M. Bhaintwal, B. K. Singh, Some results on q-ary bent functions, Internatinal Journal of Computer Mathematics, DOI:10.1080/00207160.2013.766330.

[13] B. K. Singh, On cross-correlation spectrum of generalized bent functions in generalized Maiorana-McFarland class, Manuscript submitted.

[14] P. Solé and N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, http://eprint.iacr.org/2009/544.pdf; see also, Prikl. Diskr. Mat. 1, pp. 16–18, 2009.

[15] P. Staniča, T. Martinsen, S. Gangopadhyay and B. K. Singh, *Bent and generalized bent Boolean functions*, Designs, Codes and Cryptography, DOI 10.1007/s10623-012-9622-5..

[16] Y. Zheng, X. M. Zhang, Relationship between bent functions and complementary plateaued functions, Lecture Notes in Computer Science, 1787 (1999) 60-75.

[17] Y. Zhou, M. Xie, G. Xiao, On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity, Information Sciences 180 (2010) 256-265.

[18] Z. Zhuo, J. Chong, H. Cao, G. Xiao, Spectral analysis of two Boolean functions and their derivatives, Chi. Jour. of Electr. 20 (4) (2011) 747-749.

[19] G. Gong and K. Khoo, Additive autocorrelation of resilient Boolean functions, In: Selected Areas in Cryptography 2003, LNCS, pp. 275-290, 2004.

[20] X. Wang and J. Zhou, Generalized Partially Bent Functions, Future Generation Communications and Networking-*FGCN 2007*, Vol. 1, pp. 16-21, 2007.

[21] Z. Zhuo, On cross-correlation properties of Boolean functions, International Journal of Computer Mathematics 88(10) (2011), pp. 2035-2041.

[22] X. M. Zhang and Y. Zheng, GAC-The criterion for global acalanche criteria of cryptographic functions, Journal for Universal Computer Science, 1(5), pp. 316-333, 1995.

[23] Y. Zhou , W. Zhang , S. Zhu and G. Xiao, The global avalanche characteristics of two Boolean functions and algebraic immunity, International Journal of Computer Mathematics, 89 (16), pp. 21652179, 2012.