Information Sciences Letters

Volume 2
Issue 3 *Sep. 2013*

Article 2

2013

# On cross-correlation spectrum of generalized bent functions in generalized Maiorana-McFarland class

Brajesh Kumar Singh
*Department of Mathematics, School of Allied Sciences, Graphic Era Hill University, Dehradun-248002 (Uttarakhand), India*, bksingh0584@gmail.com

Inf. Sci. Lett. **2**, No. 3, 139-145 (2013)



Information Sciences Letters
*An International Journal*

http://dx.doi.org/10.12785/isl/020302

# On cross-correlation spectrum of generalized bent functions in generalized Maiorana-McFarland class

*Brajesh Kumar Singh*[*]

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

Received: 23 Apr. 2013, Revised: 15 Jul. 2013, Accepted: 28 Jul. 2013
Published online: 1 Sep. 2013

**Abstract:** In this paper, we obtain the cross-correlation spectrum of generalized bent Boolean functions in a subclass of Maiorana-McFarland class (GMMF). An affine transformation which preserve the cross-correlation spectrum of two generalized Boolean functions, in absolute value is also presented. A construction of generalized bent Boolean functions in $(n+2)$ variables from four generalized Boolean functions in $n$ variables is presented. It is demonstrated that the direct sum of two generalized bent Boolean functions is also generalized bent. Finally, we identify a class of affine functions, in the generalized set up, each of its function is generalized bent.

**Keywords:** Generalized bent Boolean functions; GMMF; Walsh–Hadamard transform (WHT); cross-correlation

## 1 Introduction

In the recent years several authors have proposed generalizations of Boolean functions [3,5,9,10,11,12] and studied the effect of Walsh–Hadamard transform (WHT) on these classes. As in the Boolean case, in the generalized setup the functions which have flat spectra with respect to the WHT are said to be generalized bent and are of special interest (the classical notion of bent was invented by Rothaus [8]). 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).

For some problems concerning cyclic codes, Kerdock codes, and Delsarte-Goethals codes, the generalization of Boolean function due to Schmidt [9] seems more natural than the generalization due to Kumar, Scholtz and Welch [3]. For $q = 4$, Schmidt [9] studied the relations between generalized bent functions, constant amplitude codes, and $\mathbb{Z}_4$-linear codes. He also generalized the classical notion of Maiorana-McFarland class of bent functions, for $q = 4$. A necessary and sufficient condition concerning the bentness of quadratic form is given based on the theory of $\mathbb{Z}_4$-valued quadratic forms in [10]. Li et al. [5] constructed generalized bent Boolean functions in polynomial forms (in trace form) on $\mathbb{Z}_4$. Based on $\mathbb{Z}_4$ valued quadratic forms, a simple method provided in [5] to provide several new constructions of generalized boolean bent functions. The authors in [5] present a method to transform the constructed generalized boolean bent functions into binary bent and semi-bent functions. The links between Boolean bent functions [8], generalized bent Boolean functions [9], and quaternary bent functions [3] is investigated systematically by Solé-Tokareva [11].

Recently, Stănică et al. [12] studied several properties generalized bent Boolean functions, characterized generalized bent Boolean functions symmetric with respect to two variables. The authors [12] also introduced two classes of generalized bent Boolean functions. The first class is an analogous of well known Maiorana-McFarland class of classical bent Boolean functions and referred to as *generalized Maiorana-McFarland class* (GMMF). Another class is an analogous of Dillon type bent functions [2] which is referred to as *generalized Dillon class* (GD).

This paper is organized as follows. In Section 2 some basic definitions and notations are introduced. The cross-correlation spectrum of two generalized bent functions in a subclass of GMMF is characterized in Section 3. Some constructions of generalized bent functions in large number of variables by concatenation of generalized bent functions in smaller number of variables are presented in Section 4. We identify a class of

[*] Corresponding author e-mail: bksingh0584@gmail.com

affine functions, in the generalized set up, each of its function is generalized bent in Section 5.

## 2 Basic definitions and notations

Let us denote the set of integers, real numbers and complex numbers by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, respectively. Also $\mathbb{Z}_q$ denotes 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 $\mathbb{Z}_2^n = \{0,1\}^n$ $(n \geq 1)$ over binary field $\mathbb{Z}_2$ with the standard operations. Addition modulo $q$ is denoted by '$+$' and it is understood from the context. For any $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1)$ in $\mathbb{Z}_2^n$, the scalar (or inner) product is defined by $\mathbf{x} \cdot \mathbf{y} := x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. The conjugate of a bit $b$ denoted by $\bar{b}$. If $z = a + b\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2+b^2}$ denotes the absolute value of $z$, and $\bar{z} = a - b\imath$ denotes the complex conjugate of $z$, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. $Re[z]$ denotes the real part of $z$. $\mathbb{R}\imath = \{a\imath : a \in \mathbb{R}\}$, denotes the set of purely imaginary numbers. A function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$, $(q \geq 2)$ is called *generalized Boolean function* on $n$ variables [9]. The set of such functions is denoted by $\mathscr{GB}_n^q$. For $q = 2$, we obtain the set $\mathscr{GB}_n^2 = \mathscr{B}_n$ of classical Boolean functions on $n$ variables.

Let $\zeta = e^{2\pi\imath/q}$ be the complex $q$-primitive root of unity. The (generalized) *Walsh–Hadamard transform (WHT)* of $f \in \mathscr{GB}_n^q$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is

$$\mathscr{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

The inverse [12] of the WHT of $f \in \mathscr{GB}_n^q$ is given by $\zeta^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u} \in \mathbb{Z}_2^n} \mathscr{H}_f(\mathbf{u}) (-1)^{\mathbf{u}\cdot\mathbf{y}}$. A function $f \in \mathscr{GB}_n^q$ is a *generalized bent* function if $|\mathscr{H}_f(\mathbf{u})| = 1$ 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. Further, we have

**Theorem 1.***[12, Thm. 1] If $f, g \in \mathscr{GB}_n^q$, then*

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

*(ii)* *Taking $f = g$, $\mathscr{C}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathscr{H}_f(\mathbf{x})|^2 (-1)^{\mathbf{u}\cdot\mathbf{x}}$.*

*(iii)* *$f$ is generalized bent if and only if $\mathscr{C}_f(\mathbf{u}) = 2^n \delta_{\mathbf{0}}(\mathbf{u})$.*

*(iv)* *The (generalized) Parseval's identity holds: that is, $\sum_{\mathbf{x} \in \mathbb{Z}_2^n} |\mathscr{H}_f(\mathbf{x})|^2 = 2^n$.*

Let $f \in \mathscr{GB}_n^q$ is a generalized bent function such that $\mathscr{H}_f(\mathbf{u}) = \zeta^{k_u}$, for some $k_u \in \mathbb{Z}_q$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. Then, for such a generalized bent function $f$, there exists a function $\tilde{f} : \mathbb{Z}_2^n \to \mathbb{Z}_q$ such that $\zeta^{\tilde{f}} = \mathscr{H}_f$. The function $\tilde{f}$ is called the *dual* of $f$ [12], is also generalized bent.

The *cross-correlation* of $f, g \in \mathscr{GB}_n^q$ at $\mathbf{u}$ is

$$\mathscr{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x}) - g(\mathbf{x} \oplus \mathbf{u})}.$$

The *autocorrelation* of $f \in \mathscr{GB}_n^q$ at $\mathbf{u}$ is $\mathscr{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathscr{C}_f(\mathbf{u})$.

## 3 Cross-correlation spectrum of some generalized bent Boolean functions

Let $n = 2m$, where $m$ be a positive integer. Stănică et al. [12, Thm. 8] generalized a result of Schmidt [9, Thm. 5.3] (obtained for $q = 4$). The class of functions as represented in (1) below is referred to as the *generalized Maiorana–McFarland class* (GMMF). In Section 3.2, we obtain the cross-correlation spectrum of two generalized bent functions in a subclass of GMMF.

**Lemma 1.***[12, Thm. 8] Let $q > 0$ be an even integer, $\sigma$ be a permutation on $\mathbb{Z}_2^m$, and $g \in \mathscr{GB}_m^q$. Then the function $f_{\sigma,g} : \mathbb{Z}_2^m \times \mathbb{Z}_2^m \to \mathbb{Z}_q$ expressed as*

$$f_{\sigma,g}(\mathbf{x},\mathbf{y}) = g(\mathbf{y}) + \left(\frac{q}{2}\right) \mathbf{x} \cdot \sigma(\mathbf{y}) \text{ for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m \qquad (1)$$

*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, $\mathscr{H}_{f_{\sigma,g}}(\mathbf{x},\mathbf{y}) = \zeta^{g(\sigma^{-1}(\mathbf{x})) + \left(\frac{q}{2}\right)\mathbf{y}\cdot(\sigma^{-1}(\mathbf{x}))}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^m$.*

**Theorem 2.***[12, Thm. 5] Let $f, g \in \mathscr{GB}_n^q$ are defined as*

$$g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{a}) + \varepsilon\, \mathbf{b} \cdot \mathbf{x} + d, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \qquad (2)$$

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

$$\varepsilon = \begin{cases} 0, q/2 & if\ q\ is\ even \\ 0 & if\ q\ is\ odd \end{cases}.$$

*Then $g$ is generalized bent if and only if $f$ is generalized bent.*

The set of all the generalized Boolean functions as represented in (2) is referred to as *a complete class*. Specially, it is called *generalized Maiorana–McFarland complete class* if $f \in GMMF$.

Let us denote $\mathrm{S}_m(\mathbb{Z}_2)$ be the set of all permutations on $\mathbb{Z}_2^m$. Define a set $\mathscr{P}_m$ as

$$\mathscr{P}_m = \{(\sigma_1, \sigma_2) \in \mathrm{S}_m(\mathbb{Z}_2) \times \mathrm{S}_m(\mathbb{Z}_2) : \sigma_1^{-1} \oplus \sigma_2^{-1} \in \mathrm{S}_m(\mathbb{Z}_2)\}. \qquad (3)$$

### 3.1 *Existence of* $\sigma_1, \sigma_2$

Let $\mathbb{F}_{2^m}$ be the field extension of $\mathbb{Z}_2$ of degree $m$. Any finite field $\mathbb{F}_{2^m}$ is isomorphic to $\mathbb{Z}_2^m$ as a vector space over $\mathbb{Z}_2$. Every permutation on $\mathbb{F}_{2^m}$ can be identified with a permutation on $\mathbb{Z}_2^m$, and can be represented by a polynomial on $\mathbb{F}_{2^m}[x]$ of degree at most $2^m - 2$. The existence of mappings $\sigma : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ such that $\sigma(\mathbf{x})$ and $\sigma(\mathbf{x}) \oplus \mathbf{x}$ both are permutations for any $m \geq 2$ from the perspective of *complete mapping polynomials* over finite field $\mathbb{F}_{2^m}$. A polynomial $\pi(x)$ over $\mathbb{F}_{2^m}[x]$ is called *complete mapping polynomial* [4] if $\pi(x)$ and $\pi(x) + x$ both are permutation over $\mathbb{F}_{2^m}[x]$.

Inf. Sci. Lett. **2**, No. 3, 139-145 (2013) / www.naturalspublishing.com/Journals.asp 

Suppose $\sigma_\pi(\mathbf{x})$ denotes the permutation on $\mathbb{Z}_2^m$ induced by *complete mapping polynomial* $\pi(x) \in \mathbb{F}_{2^m}[x]$, then it satisfies $\sigma_\pi(\mathbf{x}) \oplus \mathbf{x}$ is also a permutation on $\mathbb{Z}_2^m$. Thus, the permutations $\sigma_1, \sigma_2$ are obtained by letting ${\sigma_1}^{-1}(\mathbf{x}) = \sigma_\pi(\mathbf{x})$ and ${\sigma_2}^{-1}(\mathbf{x}) = \sigma_\pi(\mathbf{x}) \oplus \mathbf{x}$. This implies that $\mathscr{P}_m \neq \Phi$.

In the sequel, Su et al. [13] introduced two methods to obtain linear permutation $\sigma : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ such that $\sigma(\mathbf{x}) \oplus \mathbf{x}$ also a permutation for $m \geq 2$. Define the mapping $\sigma : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ as $\sigma(\mathbf{x}) = \mathbf{x}M$ for all $\mathbf{x} = (x_m, x_{m-1}, \ldots, x_1) \in \mathbb{Z}_2^m$. The mapping $\sigma(\mathbf{x})$ on $\mathbb{Z}_2^m$ satisfying $\sigma(\mathbf{x})$ and $\sigma(\mathbf{x}) \oplus \mathbf{x}$ both are permutation is corresponding to the matrix $M$ such that $M$ and $M \oplus I_m$ both are non-singular, that is, $M$ and $M \oplus I_m$ both have full rank. For $m = 2$, only the two matrices as represented in (4), satisfy the conditions. In **Method I**, the authors used exhaustive computer search to construct the matrices satisfying the conditions. They found 48 matrices satisfying the conditions for $m = 3$, and for $m = 4$ there are 5824 matrices satisfying such conditions, for example, see (5). For any even $m \geq 4$, they refer Parkar and Pott's [6, Sect. 3] method to construct symmetric matrix $M$ of order $m$ such that $M$ and $M \oplus I_m$ both have rank $m$.

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}. \tag{4}$$

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \text{ and } \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \tag{5}$$

A square matrix $P$ of order $m$ is said to be block diagonal matrix if its main diagonal blocks are square matrices and the off-diagonal blocks are zero matrices, that is,

$$P = \mathrm{diag}(P_1, P_2, \ldots, P_t) = \begin{pmatrix} P_1 & 0 & \ldots & 0 \\ 0 & P_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & P_t \end{pmatrix},$$

where $P_j, 1 \leq j \leq t$ is a square matrix of order $k_j$, and $k_1 + k_2 + \ldots + k_t = m$. Also for any block diagonal matrix $\det(P) = \prod_{i=1}^{t} \det(P_i)$. In **Method II**, Su et al. [13] used this property of block diagonal matrix to develop a recursive technique to construct the matrices of order $n \geq 2$ satisfying the conditions, is given in the following

**Lemma 2.***[13, Lemma 4] Suppose that $t \geq 2$ and $M_j$ be a square matrix of order $k_j$ such that $M_j$ and $M_j \oplus I_{k_j}$ both have full rank for any $1 \leq j \leq t$. If $k_1 + k_2 + \ldots + k_t = m$, then the matrix $M = diag(M_1, M_2, \ldots, M_t)$ and $M \oplus I_m$ have rank m.*

The existence of a matrix $M$ of order $m \geq 2$ such that $M$ and $M \oplus I_m$ both have full rank, is guaranteed by Lemma 2, and equation (4) and (5). If we define the mappings $\sigma_1, \sigma_2 : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ as $\sigma_1(\mathbf{x}) = \mathbf{x}M^{-1}$ and $\sigma_2(\mathbf{x}) = \mathbf{x}I_m$, where $M$ be any square matrix of order $m$ obtained by Lemma 2, and $I_m$ be identity matrix of order $m$, then $\sigma_1, \sigma_2 \in \mathscr{P}_m$.

### 3.2 *Cross-correlation spectrum of generalized Boolean functions in GMMF*

The authors in [12, Thm. 13] obtained the cross-correlation spectrum of generalized bent functions belonging to a subclass of *generalized Dillon class*. In Theorem 3 below we obtain the cross-correlation spectrum between two generalized bent functions in a subclass of GMMF.

**Theorem 3.***Let $q > 0$ be an even integer, and $f_{\sigma_1,g_1}, f_{\sigma_2,g_2}$ be two functions in GMMF $\subseteq \mathscr{GB}_n^q$, 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 $\sigma_1, \sigma_2$ are permutations on $\mathbb{Z}_2^m$ and $g_1, g_2 \in \mathscr{GB}_m^q$. If $\sigma_1, \sigma_2 \in \mathscr{P}_m$, then*

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

*Proof.*By Theorem 1, we have

$$\begin{aligned}
\mathscr{C}_{f_{\sigma_1,g_1}, f_{\sigma_2,g_2}}(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x},\mathbf{y} \in \mathbb{Z}_2^m} \mathscr{H}_{f_{\sigma_1,g_1}}(\mathbf{x},\mathbf{y}) \overline{\mathscr{H}_{f_{\sigma_2,g_2}}(\mathbf{x},\mathbf{y})} (-1)^{\mathbf{u}\cdot\mathbf{x} \oplus \mathbf{v}\cdot\mathbf{y}} \\
&= \sum_{\mathbf{x},\mathbf{y}} \zeta^{g_1({\sigma_1}^{-1}(\mathbf{x})) + \left(\frac{q}{2}\right)\mathbf{y}\cdot({\sigma_1}^{-1}(\mathbf{x}))} \overline{\zeta^{g_2({\sigma_2}^{-1}(\mathbf{x})) + \left(\frac{q}{2}\right)\mathbf{y}\cdot({\sigma_2}^{-1}(\mathbf{x}))}} (-1)^{\mathbf{u}\cdot\mathbf{x} \oplus \mathbf{v}\cdot\mathbf{y}} \\
&= \sum_{\mathbf{x} \in \mathbb{Z}_2^m} \zeta^{g_1({\sigma_1}^{-1}(\mathbf{x})) - g_2({\sigma_2}^{-1}(\mathbf{x})) + \left(\frac{q}{2}\right)\mathbf{u}\cdot\mathbf{x}} \sum_{\mathbf{y} \in \mathbb{Z}_2^m} (-1)^{\mathbf{y}\cdot(\mathbf{v} \oplus ({\sigma_1}^{-1} \oplus {\sigma_2}^{-1})(\mathbf{x}))} \\
&= 2^m \zeta^{g_1({\sigma_1}^{-1}(\mathbf{x})) - g_2({\sigma_2}^{-1}(\mathbf{x})) + \left(\frac{q}{2}\right)\mathbf{u}\cdot\mathbf{x}}, \quad \mathbf{x} = ({\sigma_1}^{-1} \oplus {\sigma_2}^{-1})^{-1}(\mathbf{v}).
\end{aligned}$$

This completes the proof. □

In Theorem 4 below we introduce an affine transformation which preserve the cross-correlation spectrum of two generalized Boolean functions, in absolute value.

**Theorem 4.***The cross-correlation spectrum of two generalized Boolean functions, in absolute values, is invariant under the affine transformation*

$$g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{a}) + \mathbf{b}\cdot\mathbf{x} + d, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{6}$$

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

*Proof.*For any $\mathbf{u} \in \mathbb{Z}_2^n$, we compute

$$\begin{aligned}
\mathscr{C}_{g_1,g_2}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{g_1(\mathbf{x}) - g_2(\mathbf{x} \oplus \mathbf{u})} \\
&= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{(f_1(\mathbf{x}A \oplus \mathbf{a}) + \mathbf{x}\cdot\mathbf{b} + d) - (f_2((\mathbf{x} \oplus \mathbf{u})A \oplus \mathbf{a}) + (\mathbf{x} \oplus \mathbf{u})\cdot\mathbf{b} + d)} \\
&= \overline{\zeta}^{\mathbf{u}\cdot\mathbf{b}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f_1(\mathbf{x}A \oplus \mathbf{a}) - f_2((\mathbf{x} \oplus \mathbf{u})A \oplus \mathbf{a})} \\
&= \overline{\zeta}^{\mathbf{u}\cdot\mathbf{b}} \sum_{\mathbf{y} \in \mathbb{Z}_2^n} \zeta^{f_1(\mathbf{y}) - f_2(\mathbf{y} \oplus \mathbf{u}A)} = \overline{\zeta}^{\mathbf{u}\cdot\mathbf{b}} \mathscr{C}_{f_1,f_2}(\mathbf{u}A),
\end{aligned}$$

which completes the proof. □

It is demonstrated from Theorem 3 and 4 that there exists an infinite number of generalized bent functions *generalized Maiorana–McFarland complete class* whose cross-correlation spectrum, in absolute, is minimum.

### 3.3 *Examples of generalized bent functions in GMMF with optimal value of cross-correlation spectrum in absolute*

*Example 1.*Suppose that for $n=2m=6$, $M=\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$, and so $M^{-1}=\begin{pmatrix}0&1&1\\1&1&0\\1&0&0\end{pmatrix}$. Eqn. (5) implies that $M^{-1}$ and $M^{-1}\oplus I_3$ both have rank 3.

Now take $\sigma_1(\mathbf{y})=\mathbf{y}M=(y_1,y_1\oplus y_2,y_1\oplus y_2\oplus y_3)$, $g_1(\mathbf{y})=y_1y_2y_3$, and $\sigma_2(\mathbf{y})=\mathbf{y}I_3=(y_3,y_2,y_1)$ and $g_2(\mathbf{y})=ay_1y_2+by_1y_2y_3$ for any $a,b\in\mathbb{Z}_q$, that is, $f_{\sigma_1,g_1}(\mathbf{x},\mathbf{y})=y_1y_2y_3+\binom{q}{2}(x_3y_1\oplus x_2y_1\oplus x_2y_2\oplus x_1y_1\oplus x_1y_2\oplus x_1y_3)$ and $f_{\sigma_2,g_2}(\mathbf{x},\mathbf{y})=ay_1y_2+by_1y_2y_3+\binom{q}{2}(x_1y_1\oplus x_2y_2\oplus x_3y_3)$, then

$$|\mathscr{C}_{f_{\sigma_1,g_1},f_{\sigma_2,g_2}}(\mathbf{u},\mathbf{v})|=8 \text{ for all } (\mathbf{u},\mathbf{v})\in\mathbb{Z}_2^3\times\mathbb{Z}_2^3.$$

*Example 2.*For $n=2m=8$, let $M=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&1\\1&0&1&0\end{pmatrix}$, and so, $M^{-1}=\begin{pmatrix}0&1&0&1\\1&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$. Eqn. (5) implies that $M^{-1}$ and $M^{-1}\oplus I_4$ both have rank 4.

Now take $\sigma_1(\mathbf{y})=\mathbf{y}M=(y_1,y_2,y_1\oplus y_3,y_2\oplus y_4)$, $g_1(\mathbf{y})=y_1y_2y_3y_4+\alpha y_2y_3y_4+\beta y_1y_3y_4+\delta y_1y_2y_4$, where $\alpha,\beta,\delta\in\mathbb{Z}_q$, and $\sigma_2(\mathbf{y})=(y_4,y_3,y_2,y_1)$ and $g_2(\mathbf{y})=ay_1y_2y_4+by_1y_2y_3y_4$ for any $a,b\in\mathbb{Z}_q$, that is, $f_{\sigma_1,g_1}(\mathbf{x},\mathbf{y})=y_1y_2y_3y_4+\alpha y_2y_3y_4+\beta y_1y_3y_4+\delta y_1y_2y_4+\binom{q}{2}(x_4y_1\oplus x_3y_2\oplus x_2y_3\oplus x_2y_1\oplus x_1y_2\oplus x_1y_4)$ and $f_{\sigma_2,g_2}(\mathbf{x},\mathbf{y})=ay_1y_2y_4+by_1y_2y_3y_4+\binom{q}{2}(x_1y_1\oplus x_2y_2\oplus x_3y_3\oplus x_4y_4)$, then

$$|\mathscr{C}_{f_{\sigma_1,g_1},f_{\sigma_2,g_2}}(\mathbf{u},\mathbf{v})|=2^4 \text{ for all } (\mathbf{u},\mathbf{v})\in\mathbb{Z}_2^4\times\mathbb{Z}_2^4.$$

*Example 3.*For $n=2m=10$, let $M=\begin{pmatrix}M_1&0\\0&M_2\end{pmatrix}$, where $M_1=\begin{pmatrix}0&1\\1&1\end{pmatrix}$ and $M_2=\begin{pmatrix}0&0&1\\0&1&1\\1&1&1\end{pmatrix}$, then $M^{-1}=\begin{pmatrix}M_1'&0\\0&M_2'\end{pmatrix}$, where $M_1'=\begin{pmatrix}1&1\\1&0\end{pmatrix}$ and $M_2'=\begin{pmatrix}0&1&1\\1&1&0\\1&0&0\end{pmatrix}$. Therefore, by Lemma 2 and Eqn. (5) we have that $M^{-1}$ and $M^{-1}\oplus I_5$ both have rank 5.

Now take $\sigma_1(\mathbf{y})=\mathbf{y}M=(y_4,y_4\oplus y_5,y_1,y_1\oplus y_2,y_1\oplus y_2\oplus y_3)$, $g_1(\mathbf{y})=y_1y_2y_3y_4y_5+\alpha y_2y_3y_4y_5+\beta y_1y_3y_4y_5+\delta y_1y_2y_4y_5$, where $\alpha,\beta,\delta\in\mathbb{Z}_q$, and $\sigma_2(\mathbf{y})=(y_5,y_4,y_3,y_2,y_1)$ and $g_2(\mathbf{y})=ay_1y_2y_4y_5+by_1y_2y_3y_4y_5+cy_1y_4y_5$ for any $a,b,c\in\mathbb{Z}_q$. Thus, $f_{\sigma_1,g_1}(\mathbf{x},\mathbf{y})=y_1y_2y_3y_4y_5+\alpha y_2y_3y_4y_5+\beta y_1y_3y_4y_5+\delta y_1y_2y_4y_5+\binom{q}{2}(x_5y_4\oplus x_4y_4\oplus x_4y_5\oplus x_3y_1\oplus x_2y_1\oplus x_2y_2\oplus x_1y_1\oplus x_1y_2\oplus x_1y_3)$ and $f_{\sigma_2,g_2}(\mathbf{x},\mathbf{y})=ay_1y_2y_4y_5+by_1y_2y_3y_4y_5+cy_1y_4y_5+\binom{q}{2}(x_1y_1\oplus x_2y_2\oplus x_3y_3\oplus x_4y_4\oplus x_5y_5)$, then

$$|\mathscr{C}_{f_{\sigma_1,g_1},f_{\sigma_2,g_2}}(\mathbf{u},\mathbf{v})|=2^5 \text{ for all } (\mathbf{u},\mathbf{v})\in\mathbb{Z}_2^5\times\mathbb{Z}_2^5.$$

## 4 Constructions of generalized bent Boolean functions

In Proposition 1 below, we present the construction bent functions in $n+2$ variables from 4 bent functions in $n$ variables due to Preneel et al. [7].

**Proposition 1.***[7, Thm. 7] The concatenation $f\in\mathscr{B}_{n+2}$ of 4 bent functions $f_\ell\in\mathscr{B}_n$ ($\ell=0,1,2,3$) is bent if and only if*

$$\mathscr{H}_{f_0}(\mathbf{u})\mathscr{H}_{f_1}(\mathbf{u})\mathscr{H}_{f_2}(\mathbf{u})\mathscr{H}_{f_3}(\mathbf{u})=-1, \text{ for all } \mathbf{u}\in\mathbb{Z}_2^n,$$

*Further, the order of the $f_\ell$'s [7, Cor. 2] has no importance, that is, suppose $f=f_0||f_1||f_2||f_3$ with $f_\ell\in\mathscr{B}_n$, then (a) If $f,f_0,f_1$ and $f_2$ are bent, then $f_3$ is bent; (b) If $f_0=f_1$, then $f_2=1\oplus f_3$, and if $f_0=f_1=f_2$, then $f_3=1\oplus f_1$.*

In this Section , we construct generalized bent functions on $(n+2)$ variables obtained by concatenation of four generalized Boolean functions on $n$ variables.

For $\mathbf{v}=(v_r,\ldots,v_1)$ define $f_{\mathbf{v}}(x_{n-r},\ldots,x_1)=f(x_n=v_r,\ldots,x_{n-r+1}=v_1,x_{n-r},\ldots,x_1)$, and the vector concatenation of $\mathbf{u}=(u_r,\ldots,u_1)\in\mathbb{Z}_2^r$ and $\mathbf{w}=(w_{n-r},\ldots,w_1)\in\mathbb{Z}_2^{n-r}$ is defined by $\mathbf{uw}:=(u_r,\ldots,u_1,w_{n-r},\ldots,w_1)$.

**Lemma 3.***[12, Lemma 3] Let $\mathbf{u}\in\mathbb{Z}_2^r$, $\mathbf{w}\in\mathbb{Z}_2^{n-r}$ and $f$ be an $n$-variable generalized Boolean function. Then*

$$\mathscr{C}_f(\mathbf{uw})=\sum_{\mathbf{v}\in\mathbb{Z}_2^r}\mathscr{C}_{f_{\mathbf{v}},f_{\mathbf{v}\oplus\mathbf{u}}}(\mathbf{w}).$$

*In particular, for $r=1$, $\mathscr{C}_f(0\mathbf{w})=\mathscr{C}_{f_0}(\mathbf{w})+\mathscr{C}_{f_1}(\mathbf{w})$, and $\mathscr{C}_f(1\mathbf{w})=2Re[\mathscr{C}_{f_0,f_1}(\mathbf{w})]$.*

Inf. Sci. Lett. **2**, No. 3, 139-145 (2013) / www.naturalspublishing.com/Journals.asp 

**Theorem 5.***A function* $f \in \mathscr{GB}_{n+2}^q$ *expressed as*

$$f(z,y,\mathbf{x}) = f_0(\mathbf{x})(1\oplus z)(1\oplus y) + f_1(\mathbf{x})(1\oplus z)y + f_2(\mathbf{x})(1\oplus y)z + f_3(\mathbf{x})yz,$$

*where* $f_\ell \in \mathscr{GB}_n^q$, $(\ell = 0,1,2,3)$, *is generalized bent if and only if*

*(a)* $\sum_{\ell=0}^{3} \mathscr{C}_{f_\ell}(\mathbf{u}) = 0$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{0\}$, *and*

*(b)* $\mathscr{C}_{f_0,f_1}(\mathbf{u}) + \mathscr{C}_{f_2,f_3}(\mathbf{u}), \mathscr{C}_{f_0,f_2}(\mathbf{u}) + \mathscr{C}_{f_1,f_3}(\mathbf{u}), \mathscr{C}_{f_0,f_3}(\mathbf{u}) + \mathscr{C}_{f_1,f_2}(\mathbf{u}) \in \mathbb{R}\imath$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n$.

*Proof.*Let $F_\ell$ $(\ell \in \mathbb{Z}_2)$ be the restriction of $f$ on the hyperplane $\{\ell\} \times \mathbb{Z}_2 \times \mathbb{Z}_2^n \equiv \mathbb{Z}_2^{n+1}$. Then $F_0(y,\mathbf{x}) = f(0,y,\mathbf{x}) = f_0(\mathbf{x})(1\oplus y) + f_1(\mathbf{x})y$ and $F_1(y,\mathbf{x}) = f(1,y,\mathbf{x}) = f_2(\mathbf{x})(1\oplus y) + f_3(\mathbf{x})y$. Now,

$$\begin{aligned}\mathscr{C}_{F_0,F_1}(0,\mathbf{u}) &= \sum_{(y,\mathbf{x})\in\mathbb{Z}_2\times\mathbb{Z}_2^n} \zeta^{F_0(y,\mathbf{x})-F_1((y,\mathbf{x})\oplus(0,\mathbf{u}))} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{F_0(0,\mathbf{x})-F_1((0,\mathbf{x}\oplus\mathbf{u}))} + \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{F_0(1,\mathbf{x})-F_1((1,\mathbf{x}\oplus\mathbf{u}))} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f_0(\mathbf{x})-f_2(\mathbf{x}\oplus\mathbf{u})} + \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f_1(\mathbf{x})-f_3(\mathbf{x}\oplus\mathbf{u})} \\ &= \mathscr{C}_{f_0,f_2}(\mathbf{u}) + \mathscr{C}_{f_1,f_3}(\mathbf{u}).\end{aligned} \tag{7}$$

Similarly

$$\mathscr{C}_{F_0,F_1}(1,\mathbf{u}) = \mathscr{C}_{f_0,f_3}(\mathbf{u}) + \mathscr{C}_{f_1,f_2}(\mathbf{u}). \tag{8}$$

Let $a \in \mathbb{Z}_2, \mathbf{u} \in \mathbb{Z}_2^n$, using Lemma 3 for $r = 1$, we have

$$\mathscr{C}_f(0,a,\mathbf{u}) = \mathscr{C}_{F_0}(a,\mathbf{u}) + \mathscr{C}_{F_1}(a,\mathbf{u}), \text{ and} \tag{9}$$

$$\mathscr{C}_f(1,a,\mathbf{u}) = \mathscr{C}_{F_0,F_1}(a,\mathbf{u}) + \overline{\mathscr{C}_{F_0,F_1}(a,\mathbf{u})}. \tag{10}$$

Further, using Lemma 3 in (9), we have

$$\mathscr{C}_f(0,0,\mathbf{u}) = \mathscr{C}_{f_0}(\mathbf{u}) + \mathscr{C}_{f_1}(\mathbf{u}) + \mathscr{C}_{f_2}(\mathbf{u}) + \mathscr{C}_{f_3}(\mathbf{u}), \text{ and} \tag{11}$$

$$\begin{aligned}\mathscr{C}_f(0,1,\mathbf{u}) &= \mathscr{C}_{F_0}(1,\mathbf{u}) + \mathscr{C}_{F_1}(1,\mathbf{u}) = \mathscr{C}_{f_0,f_1}(\mathbf{u}) + \overline{\mathscr{C}_{f_0,f_1}(\mathbf{u})} \\ &+ \mathscr{C}_{f_2,f_3}(\mathbf{u}) + \overline{\mathscr{C}_{f_2,f_3}(\mathbf{u})} = 2Re\left[\mathscr{C}_{f_0,f_1}(\mathbf{u}) + \mathscr{C}_{f_2,f_3}(\mathbf{u})\right].\end{aligned} \tag{12}$$

Using (7) and (10), we have

$$\begin{aligned}\mathscr{C}_f(1,0,\mathbf{u}) &= \mathscr{C}_{f_0,f_2}(\mathbf{u}) + \mathscr{C}_{f_1,f_3}(\mathbf{u}) + \overline{\mathscr{C}_{f_0,f_2}(\mathbf{u}) + \mathscr{C}_{f_1,f_3}(\mathbf{u})} \\ &= 2Re\left[\mathscr{C}_{f_0,f_2}(\mathbf{u}) + \mathscr{C}_{f_1,f_3}(\mathbf{u})\right].\end{aligned} \tag{13}$$

Similarly, by (8) and (10), we have

$$\mathscr{C}_f(1,1,\mathbf{u}) = 2Re\left[\mathscr{C}_{f_0,f_3}(\mathbf{u}) + \mathscr{C}_{f_1,f_2}(\mathbf{u})\right]. \tag{14}$$

Suppose $f \in \mathscr{GB}_{n+2}^q$ such that conditions $(a)$ and $(b)$ holds, then from (11), (12), (13) and (14) we have $\mathscr{C}_f(b,a,\mathbf{u}) = 0$, for all $(b,a,\mathbf{u}) \neq (0,0,\mathbf{0})$ and $\mathscr{C}_f(0,0,\mathbf{0}) = 2^{n+2}$. Therefore $f$ is generalized bent.

Conversely, if $f$ is generalized bent, then $\mathscr{C}_f(b,a,\mathbf{u}) = 0$ for all $(b,a,\mathbf{u}) \neq (0,0,\mathbf{0})$ and $\mathscr{C}_f(0,0,\mathbf{0}) = 2^{n+2}$. Using (11), (12), (13) and (14) with the above conditions we have $(a)$ and $(b)$. □

**Corollary 1.***Suppose* $f \in \mathscr{GB}_{n+2}^q$ *is expressed as*

$$f(z,y,\mathbf{x}) = f_{y\oplus 1}(\mathbf{x}) + \left(\frac{q}{2}\right)yz, \text{ for all } y,z, \in \mathbb{Z}_2, \mathbf{x} \in \mathbb{Z}_2^n, \tag{15}$$

*where* $f_{y\oplus 1} \in \mathscr{GB}_n^q$ $(y \in \mathbb{Z}_2)$. *Then* $f$ *is generalized bent if and only if* $f_0$, $f_1$ *both are generalized bent.*

*Proof.*Equation (15) can be rewritten as $f \equiv f_1||f_1||f_0||f_0 + \left(\frac{q}{2}\right)$. Using $\mathscr{C}_{f,g+\frac{q}{2}}(\mathbf{u}) + \mathscr{C}_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_2^n$ in Theorem 5, we have $(*)$ : $\mathscr{C}_f(0,0,\mathbf{u}) = 2\left(\mathscr{C}_{f_0}(\mathbf{u}) + \mathscr{C}_{f_1}(\mathbf{u})\right)$; $(**)$: $\mathscr{C}_f(1,0,\mathbf{u}) = 0 = \mathscr{C}_f(1,1,\mathbf{u})$; and $(***)$: $\mathscr{C}_f(0,1,\mathbf{u}) = 2(\mathscr{C}_{f_1}(\mathbf{u}) - \mathscr{C}_{f_0}(\mathbf{u}))$. Suppose $f$ is generalized bent, that is, $\mathscr{C}_f(b,a,\mathbf{u}) = 0$ for all $(b,a,\mathbf{u}) \neq 0$ and $\mathscr{C}_f(0,0,\mathbf{0}) = 2^{n+2}$, therefore from condition $(*)$ and $(***)$, we have $\mathscr{C}_{f_0}(\mathbf{u}) = 0$ and $\mathscr{C}_{f_1}(\mathbf{u}) = 0$ for all $\mathbf{u} \neq \mathbf{0}$, and $\mathscr{C}_{f_0}(\mathbf{0}) = \mathscr{C}_{f_1}(\mathbf{0}) = 2^n$.

Conversely, if $f_0$ and $f_1$ are generalized bent, then from above conditions $(*)$, $(**)$ and $(***)$, we have $\mathscr{C}_f(b,a,\mathbf{u}) = 0$ for all $(b,a,\mathbf{u}) \neq 0$ and $\mathscr{C}_f(0,0,\mathbf{0}) = 2^{n+2}$. □

*Remark.*For any $(b,a,\mathbf{u}) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^n$, one can observe that the WHT of $f$ as defined in Equation (15) is $\mathscr{H}_f(b,a,\mathbf{u}) = (-1)^{ab}\mathscr{H}_{f_{b\oplus 1}}(\mathbf{u})$, that is, $|\mathscr{H}_f(b,a,\mathbf{u})| = |\mathscr{H}_{f_{b\oplus 1}}(\mathbf{u})|$ for all $\mathbf{u} \in \mathbb{Z}_2^n, a,b \in \mathbb{Z}_2$. This implies that for any $(b,a,\mathbf{u}) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^n$, $|\mathscr{H}_f(b,a,\mathbf{u})| = 1$ if and only if $|\mathscr{H}_{f_0}(\mathbf{u})| = |\mathscr{H}_{f_1}(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. This completes the proof of Corollary 1.

Since the functions constructed in Corollary 1 are not symmetric with respect to the variables $y$ and $z$ if $f_0 \neq f_1$ as $f(1,0,\mathbf{x}) = f_1(\mathbf{x})$ and $f(0,1,\mathbf{x}) = f_0(\mathbf{x})$. Thus, the generalized bent functions constructed in Corollary 1 are distinct from the functions constructed in [12, Thm. 6].

In Theorem 6 below we demonstrate that as in the Boolean case [1, pp. 81], in the generalized setup, the direct sum of two generalized bent functions is also generalized bent.

**Theorem 6.***A function* $g \in \mathscr{GB}_{r+s}^q$ *expressed as*

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

*where* $f_1 \in \mathscr{GB}_r^q$, $f_2 \in \mathscr{GB}_s^q$, *is generalized bent if and only if* $f_1$ *and* $f_2$ *both are generalized bents.*

*Proof.*For any $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s$,

$$\mathscr{H}_g(\mathbf{u},\mathbf{v}) = \mathscr{H}_{f_1}(\mathbf{u})\mathscr{H}_{f_2}(\mathbf{v}). \tag{16}$$

Now, if $f_1 \in \mathscr{GB}_r^q$ and $f_2 \in \mathscr{GB}_s^q$ be generalized bent Boolean functions, then from (16) we have $|\mathscr{H}_g(\mathbf{u},\mathbf{v})| = |\mathscr{H}_{f_1}(\mathbf{u})||\mathscr{H}_{f_2}(\mathbf{v})| = 1$ for all $(\mathbf{u},\mathbf{v}) \in \mathbb{Z}_2^r \times \mathbb{Z}_2^s$ which implies that $g$ is generalized bent Boolean function.

Conversely, we assume $g$ is generalized bent Boolean function, our aim is to show that the functions $f_1$ and $f_2$ are generalized bent. Suppose that $f_1$ is not generalized bent, then there exists $\mathbf{u} \in \mathbb{Z}_2^r$ such that $|\mathscr{H}_{f_1}(\mathbf{u})| = \ell \neq 1$. Using (16), $|\mathscr{H}_{f_2}(\mathbf{v})| = \frac{1}{\ell}$ for every $\mathbf{v} \in \mathbb{Z}_2^s$. Now,

$$\sum_{\mathbf{v}\in\mathbb{Z}_2^s} |\mathscr{H}_{f_2}(\mathbf{v})|^2 = \frac{2^s}{\ell^2} \neq 2^s,$$

which is a contradiction. This completes the proof. □

## 5 Existence of generalized bent functions in the class of affine functions

In classical notion ($q = 2$) and $q$-ary functions [3] both all the affine functions are either balanced or constant and therefore, they are not bent. In Thm. 7 below we identify a class of affine functions, in the generalized set up due to Schmidt [9], each of its function is generalized bent.

**Theorem 7.** *Let $q$ be a positive integer such that $q = 0 \mod 4$. Then an affine function $f_\lambda \in \mathscr{GB}_n^q$ is generalized bent if and only if*

$$\prod_{i=1}^{n}\left(1+(-1)^{u_i}\cos\left(\frac{2\pi\lambda_i}{q}\right)\right) = 1, \forall \mathbf{u} \in \mathbb{Z}_2^n. \qquad (17)$$

*Proof.* Let $q$ be a positive integer such that $q = 0 \mod 4$, and $f_\lambda \in \mathscr{GB}_n^q$ be an affine function [9]. Then it is expressed as $f_\lambda(\mathbf{x}) = \lambda_0 + \sum_{i=1}^n \lambda_i x_i, \lambda_i \in \mathbb{Z}_q$, and for $\mathbf{u} \in \mathbb{Z}_2^n$,

$$2^{\frac{n}{2}}\mathscr{H}_{f_\lambda}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f_\lambda(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \zeta^{\lambda_0}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\sum_{i=1}^n(\lambda_i x_i + \left(\frac{q}{2}\right)u_i x_i)}$$

$$= \zeta^{\lambda_0}\prod_{i=1}^{n}\sum_{x_i\in\mathbb{Z}_2} \zeta^{(\lambda_i+\left(\frac{q}{2}\right)u_i)x_i} = \zeta^{\lambda_0}\prod_{i=1}^{n}(1+(-1)^{u_i}\zeta^{\lambda_i})$$

$$= \zeta^{\lambda_0}\prod_{i=1}^{n}\left(1+(-1)^{u_i}\cos\left(\frac{2\pi\lambda_i}{q}\right)+\imath(-1)^{u_i}\sin\left(\frac{2\pi\lambda_i}{q}\right)\right),$$

which implies that

$$2^n|\mathscr{H}_{f_\lambda}(\mathbf{u})|^2 = \prod_{i=1}^{n} 2\left(1+(-1)^{u_i}\cos\left(\frac{2\pi\lambda_i}{q}\right)\right)$$

$$= 2^n\prod_{i=1}^{n}\left(1+(-1)^{u_i}\cos\left(\frac{2\pi\lambda_i}{q}\right)\right).$$

Therefore, $f_\lambda$ is generalized bent if and only if

$$\prod_{i=1}^{n}\left(1+(-1)^{u_i}\cos\left(\frac{2\pi\lambda_i}{q}\right)\right) = 1, \forall \mathbf{u} \in \mathbb{Z}_2^n.$$

□

It is to be noted that for any $i \in \{1,2,\ldots,n\}$, $\lambda_i = \frac{q}{4}$, $\frac{3q}{4}$ are solutions of (17). Thus we have the following

**Proposition 2.** *Let $q$ be a positive integer such that $q = 0 \mod 4$. Then affine functions $f \in \mathscr{GB}_n^q$ of the form $f(\mathbf{x}) = \lambda_0 + \sum_{\ell=1}^n \lambda_\ell \mathbf{x}_\ell$, where for any $\ell \in \{1,2,\ldots,n\}$, $\lambda_\ell$ is either $\frac{q}{4}$ or $\frac{3q}{4}$ and $\lambda_0 \in \mathbb{Z}_q$, are always generalized bent.*

## 6 Conclusion

In this paper, a subclass of generalized bent Boolean functions in generalized Maiorana-McFarland class (GMMF) having minimum (optimal) cross-correlation spectrum, is identified. An affine transformation which preserve the cross-correlation spectrum of two generalized Boolean functions, in absolute value is also presented. Thus, for a given pair of generalized bent Boolean functions having optimal cross-correlation spectrum, one can construct large number of generalized bent Boolean functions having optimal value of the cross-correlation spectrum.

A construction of generalized bent Boolean functions in $(n+2)$ variables from four generalized Boolean functions in $n$ variables is presented. It is demonstrated that the direct sum of two generalized bent Boolean functions is also generalized bent. Finally, we identify a class of affine functions, in the generalized set up, each of its function is generalized bent.

## References

[1] T. W. Cusick and P. Stănică, Cryptographic Boolean functions and applications, Elsevier-Academic Press, (2009).

[2] J. F. Dillon, Elementary Hadamard difference sets, Proceedings of Sixth S.E. Conference of Combinatorics, Graph Theory, and Computing, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, 237-249 (1975).

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

[4] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields and Their Applications, **13**, 58-70 (2007).

[5] N. Li, X. Tang and T. Helleseth, New classes of generalized boolean bent functions over $\mathbb{Z}_4$, Proceedings of IEEE International Symposium on Information Theory ISIT 2012, 841-45 (2012).

[6] M. G. Parker, and A. Pott, On Boolean functions which are bent and negabent, Proceedings of Sequences, Subsequences, and Consequences, LNCS, **4893**, 9-23 (2007).

[7] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandewalle, Propagation characteristics of Boolean functions, Adv. in Crypt.-Eurocrypt'90. LNCS, **473**, 161-73 (1991).

[8] O. S. Rothaus, On bent functions, J. Combinatorial Theory Ser., **A 20**, 300-305 (1976).
[9] K-U. Schmidt, Quaternary constant-amplitude codes for multicode CDMA, IEEE Trans. Inform. Theory, **55**, 1824-1832 (2009).
[10] K-U. Schmidt, $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families, IEEE Trans. Inf. Theory, **55**, 5803-5810 (2009).
[11] P. Solé and N. Tokareva, Connections between Quaternary and Binary Bent Functions, IACR Cryptology ePrint Archive, **2009**, 544 (2009), see also, Prikl. Diskr. Mat., **1**, 16-18 (2009).
[12] P. Staniča, T. Martinsen, S. Gangopadhyay and B. K. Singh, Bent and generalized bent Boolean functions, Designs, Codes and Cryptography, **69**, 77-94 (2013).
[13] W. Su, A. Pott and X. Tang, Charecterization of negabent functions and constructions of bent-negabent functions with maximum algebraic degree, available at http://arxiv.org/pdf/1205.6568v1.pdf.