Some Results Concerning Generalized Bent Functions

Pantelimon Stănică[1], Sugata Gangopadhyay[2] and Brajesh Kumar Singh[2]

[1] Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943–5216, USA
pstanica@nps.edu
[2] Department of Mathematics***
Indian Institute of Technology Roorkee
Roorkee–247667, INDIA,
{gsugata, singh.brajesho584}@gmail.com

Abstract. In this paper we investigate the properties of generalized bent functions defined on $\mathbb{Z}_2^n$ with values in $\mathbb{Z}_q$ where $q \geq 2$ is any positive integer. We characterize the class of generalized bent functions symmetric with respect to two variables, provide an analogue of Maiorana–McFarland type bent functions in the generalized set up. A class of bent functions called generalized spreads type is introduced and it is demonstrated that recently introduced Dillon type generalized bent functions and Maiorana–McFarland type generalized bent functions can be described as generalized spreads type functions. Thus unification of two different types of generalized bent functions is achieved.

Keywords: Generalized Boolean functions; generalized bent functions; spreads.

1 Introduction

The Walsh–Hadamard transform on generalizations of Boolean functions have been studied for some time [11, 15–17]. Particular interest are analogues of bent functions in different generalized scenarios. In this paper we investigate the properties of generalized bent functions defined on $\mathbb{Z}_2^n$ with values in $\mathbb{Z}_q$ where $q \geq 2$ is any positive integer.

Suppose $\mathbb{Z}$ is the set of integers and $\mathbb{Z}_r$ is the ring of integers modulo r. A function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ is said to be a Boolean function on n variables and the set of all such functions is denoted by $\mathcal{B}_n$. A function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ (q a positive integer) is said to be a *generalized Boolean function* on n variables [16]. The set of all such functions is denoted by $\mathcal{GB}_n^q$. Let the set of real numbers and complex numbers be denoted by $\mathbb{R}$ and $\mathbb{C}$.

*** B.K.S. is a Ph.D. student in Mathematics at the Indian Institute of Technology Roorkee.

Any element $\mathbf{x} \in \mathbb{Z}_2^n$ can be written as an n-tuple $(x_n, \ldots, x_1)$, where $x_i \in \mathbb{Z}_2$ for all $i = 1, \ldots, n$. The addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ is denoted by '+'. The addition over $\mathbb{Z}_2^n$ for all $n \geq 1$, is denoted by $\oplus$. Addition modulo q is denoted by '+' and is understood from the context. If $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1)$ are two elements of $\mathbb{Z}_2^n$, we define the scalar (or inner) product, by $\mathbf{x} \cdot \mathbf{y} = x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. The cardinality of the set S is denoted by $|S|$. 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 $a, b \in \mathbb{R}$. The conjugate of a bit b will also be denoted by $\bar{b}$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is defined by

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

A function $f \in \mathcal{B}_n$, where n is even, is a *bent function* if $|W_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. If n is odd, a function $f \in \mathcal{B}_n$ is said to be *semibent* if and only if $|W_f(\mathbf{u})| \in \{0, \sqrt{2}\}$, for all $\mathbf{u} \in \mathbb{Z}_2^n$.

The sum

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})}$$

is the *crosscorrelation* of f and g at $\mathbf{z}$. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is $C_{f,f}(\mathbf{u})$ above, which we denote by $C_f(\mathbf{u})$.

The (generalized) *Walsh–Hadamard transform* of $f \in \mathcal{GB}_n^q$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is the complex valued function defined by

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

where $\zeta = e^{2\pi\imath/q}$ is a complex q-primitive root of unity. A function $f \in \mathcal{GB}_n^q$ is a *generalized bent function* (*gbent*, for short) if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. If f is gbent then $|\mathcal{H}_f(\mathbf{u})| = 1$, for all $\mathbf{u}$. Assume that for every such $\mathbf{u}$, we have $\mathcal{H}_f(\mathbf{u}) = \zeta^{k_u}$, for some $0 \leq k_u < q$. That is, for such a gbent function f, there is a function $F : \mathbb{Z}_2^n \to \mathbb{Z}_q$ such that $\zeta^F = \mathcal{H}_f$. We call such a function F the *dual* of f (*Caution*: only some gbent functions admit duals).

The sum

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

is the *crosscorrelation* of f and g at $\mathbf{z}$. The *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$.

2 Properties of Walsh–Hadamard transform on generalized Boolean functions

Several properties of Walsh–Hadamard transform and their generalized analogues are presented below [9, 16, 17].

Theorem 1 *We have:*

(*i*) *The inverse of the Walsh–Hadamard transform is*

$$(-1)^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} W_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{y}}, \text{ for all } f \in \mathcal{B}_n.$$

(*ii*) *If* $f, g \in \mathcal{B}_n$, *then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} C_{f,g}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n W_f(\mathbf{x})W_g(\mathbf{x}),$$
$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} W_f(\mathbf{x})W_g(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

(*iii*) *Taking the particular case* $f = g$ *we obtain* $C_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} W_f(\mathbf{x})^2(-1)^{\mathbf{u}\cdot\mathbf{x}}$.

(*iv*) *A Boolean function* f *is bent if and only if* $C_f(\mathbf{u}) = 0$ *for* $\mathbf{0} \neq \mathbf{u} \in \mathbb{Z}_2^n$.

(*v*) *For any* $f \in \mathcal{B}_n$, *the Parseval's identity holds* $\sum_{\mathbf{x}\in\mathbb{Z}_2^n} W_f(\mathbf{x})^2 = 2^n$.

For more details we refer to [5–7]. Analogues properties for generalized Boolean functions is as follows:

Theorem 2 *We have:*

(*i*) *Let* $f \in \mathcal{GB}_n^q$. *The inverse of the Walsh–Hadamard transform is given by*

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

Further, $\mathcal{C}_{f,g}(\mathbf{u}) = \overline{\mathcal{C}_{g,f}(\mathbf{u})}$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n$, *which implies that* $\mathcal{C}_f(\mathbf{u})$ *is always real.*

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

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

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

(*iv*) *If* $f \in \mathcal{GB}_n^q$, *then* f *is gbent if and only if*

$$\mathcal{C}_f(\mathbf{u}) = \begin{cases} 2^n & \text{if } \mathbf{u} = 0, \\ 0 & \text{if } \mathbf{u} \neq 0. \end{cases} \tag{1}$$

(*v*) *Moreover, the (generalized) Parseval's identity holds* $\sum_{\mathbf{x}\in\mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 = 2^n$.

3 Characterization and affine transformations of generalized bent functions

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

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

Let $\mathbf{u} = (u_r, \ldots, u_1) \in \mathbb{Z}_2^r$ and $\mathbf{w} = (w_{n-r}, \ldots, w_1) \in \mathbb{Z}_2^{n-r}$. We define the vector concatenation by

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

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*

$$\mathcal{C}_f(\mathbf{uw}) = \sum_{\mathbf{v} \in \mathbb{Z}_2^r} \mathcal{C}_{f_{\mathbf{v}}, f_{\mathbf{v} \oplus \mathbf{u}}}(\mathbf{w}). \tag{2}$$

In particular, for $r = 1$,

(i) $\mathcal{C}_f(0\mathbf{w}) = \mathcal{C}_{f_0}(\mathbf{w}) + \mathcal{C}_{f_1}(\mathbf{w})$,
(ii) $\mathcal{C}_f(1\mathbf{w}) = 2Re[\mathcal{C}_{f_0, f_1}(\mathbf{w})]$.

Proof. Certainly,

$$\begin{aligned}
\mathcal{C}_f(\mathbf{uw}) &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x}) - f(\mathbf{x} \oplus \mathbf{uw})} \\
&= \sum_{\mathbf{v} \in \mathbb{Z}_2^r} \sum_{\mathbf{z} \in \mathbb{Z}_2^{n-r}} \zeta^{f(\mathbf{vz}) - f(\mathbf{vz} \oplus \mathbf{uw})} \\
&= \sum_{\mathbf{v} \in \mathbb{Z}_2^r} \sum_{\mathbf{z} \in \mathbb{Z}_2^{n-r}} \zeta^{f_{\mathbf{v}}(\mathbf{z}) - f_{\mathbf{v} \oplus \mathbf{u}}(\mathbf{z} \oplus \mathbf{w})} \\
&= \sum_{\mathbf{v} \in \mathbb{Z}_2^r} \mathcal{C}_{f_{\mathbf{v}}, f_{\mathbf{v} \oplus \mathbf{u}}}(\mathbf{w}).
\end{aligned}$$

□

Two functions $f, g \in \mathcal{GB}_n^q$ are said to have *complementary autocorrelation* if and only if $\mathcal{C}_f(\mathbf{u}) + \mathcal{C}_g(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{Z}_2^n \setminus \{\mathbf{0}\}$.

Lemma 4 *Two functions $f, g \in \mathcal{GB}_n^q$ have complementary autocorrelation if and only if*

$$|\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 = 2, \text{ for all } \mathbf{u} \in \mathbb{Z}_2^n. \tag{3}$$

Proof. If f and g have complementary autocorrelation then

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

Thus, $|\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 = 2$, for all $\mathbf{u} \in \mathbb{Z}_2^n$.

Conversely, suppose that

$$|\mathcal{H}_f(\mathbf{x})|^2 + |\mathcal{H}_g(\mathbf{x})|^2 = 2, \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

Then,

$$\begin{aligned}\mathcal{C}_f(\mathbf{u}) + \mathcal{C}_g(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (|\mathcal{H}_f(\mathbf{x})|^2 + |\mathcal{H}_g(\mathbf{x})|^2)(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= 2\sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^{n+1}\delta_0(\mathbf{u}),\end{aligned}$$

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

Theorem 5 *If n is a positive integer and h is an $(n+1)$-variable generalized Boolean function, we write*

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

Then the following statements are equivalent:

(*a*) *h is gbent.*
(*b*) *f and g have complementary autocorrelation and $Re[\mathcal{C}_{f,g}(\mathbf{w})] = 0$.*
(*c*) *$|\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 = 2$, for all $\mathbf{u} \in \mathbb{Z}_2^n$ and $\frac{\mathcal{H}_g(\mathbf{u})}{\mathcal{H}_f(\mathbf{u})}$ is purely imaginary whenever $|\mathcal{H}_f(\mathbf{u})||\mathcal{H}_g(\mathbf{u})| \neq 0$.*

Proof. The equivalence of the first two statements is immediate from equation (1) and Lemma 3.

Let us identify $(x_{n+1}, x_n, \ldots, x_1) \in \mathbb{Z}_2^{n+1}$ with $(x_{n+1}, \mathbf{x}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^n$. Suppose that the function

$$h(x_{n+1}, \mathbf{x}) = (1 \oplus x_{n+1})f(\mathbf{x}) + x_{n+1}g(\mathbf{x}) \tag{4}$$

is gbent. The Walsh–Hadamard transform of h at $(a, \mathbf{u}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^n$ is

$$\begin{aligned}\mathcal{H}_h(a, \mathbf{u}) &= 2^{-\frac{n+1}{2}} \sum_{(x_{n+1},\mathbf{x})\in\mathbb{Z}_2\times\mathbb{Z}_2^n} \zeta^{h(x_{n+1},\mathbf{x})}(-1)^{x_{n+1}a+\mathbf{u}\cdot\mathbf{x}} \\ &= 2^{-\frac{n+1}{2}} \left(\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} + (-1)^a \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{g(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \right) \qquad (5) \\ &= \frac{1}{\sqrt{2}} \left(\mathcal{H}_f(\mathbf{u}) + (-1)^a \mathcal{H}_g(\mathbf{u})\right)\end{aligned}$$

Since the function h is gbent, then $|\mathcal{H}_h(a, \mathbf{u})| = 1$ for all $(a, \mathbf{u}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^n$. Therefore $\mathcal{H}_f(\mathbf{u})$ and $\mathcal{H}_g(\mathbf{u})$ cannot be zero simultaneously. Suppose that $|\mathcal{H}_f(\mathbf{u})||\mathcal{H}_g(\mathbf{u})| \neq 0$, for $\mathbf{u} \in \mathbb{Z}_2^n$. From (5) we have $|\mathcal{H}_f(\mathbf{u}) + \mathcal{H}_g(\mathbf{u})| = |\mathcal{H}_f(\mathbf{u}) - \mathcal{H}_g(\mathbf{u})|$ which implies

$$\mathcal{H}_f(\mathbf{u})\overline{\mathcal{H}_g(\mathbf{u})} = -\overline{\mathcal{H}_f(\mathbf{u})}\mathcal{H}_g(\mathbf{u}). \tag{6}$$

Since $\mathcal{H}_f(\mathbf{u}) \neq 0$ we obtain

$$\frac{\mathcal{H}_g(\mathbf{u})}{\mathcal{H}_f(\mathbf{u})} = -\overline{\left(\frac{\mathcal{H}_g(\mathbf{u})}{\mathcal{H}_f(\mathbf{u})}\right)}. \tag{7}$$

Therefore $\frac{\mathcal{H}_g(\mathbf{u})}{\mathcal{H}_f(\mathbf{u})}$ is purely imaginary. Since h is generalized bent, f and g have complementary autocorrelation and therefore by Lemma 4, we have $|\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. This proves that (a) implies (c). Conversely, suppose (c) is true. Suppose $\mathcal{H}_f(\mathbf{u}) = 0$. Then we obtain $|\mathcal{H}_g(\mathbf{u})| = \sqrt{2}$. This implies that $|\mathcal{H}_h(a, \mathbf{u})| = 1$ for all $a \in \mathbb{Z}_2$. Now, suppose $|\mathcal{H}_f(\mathbf{u})||\mathcal{H}_g(\mathbf{u})| \neq 0$ for $\mathbf{u} \in \mathbb{Z}_2^n$. Let $\frac{\mathcal{H}_g(\mathbf{u})}{\mathcal{H}_f(\mathbf{u})} = \imath\phi(\mathbf{u})$, where $\phi(\mathbf{u})$ is real. Then

$$\begin{aligned} |\mathcal{H}_h(a, \mathbf{u})|^2 &= \frac{1}{2}|\mathcal{H}_f(\mathbf{u})|^2|1 + \imath(-1)^a\phi(\mathbf{u})|^2 \\ &= \frac{1}{2}|\mathcal{H}_f(\mathbf{u})|^2(1 + \phi(\mathbf{u})^2) \\ &= \frac{1}{2}|\mathcal{H}_f(\mathbf{u})|^2\left(1 + \frac{|\mathcal{H}_g(\mathbf{u})|^2}{|\mathcal{H}_f(\mathbf{u})|^2}\right) \\ &= \frac{1}{2}(|\mathcal{H}_f(\mathbf{u})|^2 + |\mathcal{H}_g(\mathbf{u})|^2) = 1. \end{aligned} \tag{8}$$

Therefore (c) implies (a), and the theorem is proved. □

Theorem 6 *Let f, g be two generalized Boolean functions in n variables, where*

$$g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{a}) + \epsilon\ \mathbf{b} \cdot \mathbf{x} + d,\ \text{where } A \in GL(2, n), \mathbf{a}, \mathbf{b} \in \mathbb{Z}_2^n, d \in \mathbb{Z}_q,$$

and $\epsilon = \begin{cases} 0,\ q/2 & if\ q = even \\ 0 & if\ q = odd \end{cases}$. *Then f is gbent if and only if g is gbent.*

Proof. Let $B = A^{-1}$. We show the theorem when q is even and $\epsilon = q/2$, since the other cases are absolutely similar. Using $\zeta^{\frac{q}{2}} = -1$, we compute the Walsh–Hadamard transform of g at $\mathbf{z} \in \mathbb{Z}_2^n$,

$$\begin{aligned} \mathcal{H}_g(\mathbf{z}) &= 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(A\mathbf{x} \oplus \mathbf{a}) + \frac{q}{2}\mathbf{b}\cdot\mathbf{x} + d}(-1)^{\mathbf{z}\cdot\mathbf{x}} \\ &= 2^{-\frac{n}{2}}\zeta^d \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(A\mathbf{x} \oplus \mathbf{a})}(-1)^{(\mathbf{z} \oplus \mathbf{b})\cdot\mathbf{x}} \\ &= 2^{-\frac{n}{2}}\zeta^d(-1)^{B^T(\mathbf{b} \oplus \mathbf{z})\cdot\mathbf{a}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})}(-1)^{B^T(\mathbf{b} \oplus \mathbf{z})\cdot\mathbf{x}} \\ &= \zeta^d(-1)^{B^T(\mathbf{b} \oplus \mathbf{z})\cdot\mathbf{a}}\mathcal{H}_f(B^T(\mathbf{b} \oplus \mathbf{z})), \end{aligned}$$

which concludes our proof. □

4 Generalized bent functions symmetric about two variables

A generalized Boolean function $h \in \mathcal{GB}_{n+2}^q$ is symmetric with respect to two variables y and z if and only if there exist $f, g \in \mathcal{GB}_n^q$ such that

$$h(z, y, \mathbf{x}) = f(\mathbf{x}) + (y \oplus z)g(\mathbf{x}) + yzs(\mathbf{x}) \tag{9}$$

where $y, z \in \mathbb{Z}_2$ and $\mathbf{x} \in \mathbb{Z}_2^n$ and $\mathbb{Z}_2^{n+2}$ is identified with $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^n$.

Theorem 7 *Suppose q is a positive integer. Let h be a generalized Boolean function symmetric about two variables, as in (9). Then h is gbent if and only if $f, f+g$ are gbent and $s(\mathbf{x}) = \frac{q}{2}$ (and consequently, q must be even).*

Proof. Let $\Delta(F) = F(\mathbf{x}) - F(\mathbf{x} \oplus \mathbf{u})$. Now, for a function h as in (9),

$$\begin{aligned} h(z, y, \mathbf{x}) - h((z, y, \mathbf{x}) \oplus (a, b, \mathbf{u})) \\ &= f(\mathbf{x}) + (y \oplus z)g(\mathbf{x}) + yz\, s(\mathbf{x}) - f(\mathbf{x} \oplus \mathbf{u}) \\ &\quad -(y \oplus z \oplus a \oplus b)g(\mathbf{x} \oplus \mathbf{u}) - (z \oplus a)(y \oplus b)s(\mathbf{x} \oplus \mathbf{u}) \\ &= \Delta(f) + (y \oplus z)\Delta(g) + yz\, \Delta(s) \\ &\quad -(a \oplus b)g(\mathbf{x} \oplus \mathbf{u}) - (ay \oplus bz \oplus ab)s(\mathbf{x} \oplus \mathbf{u}), \end{aligned}$$

and the autocorrelation

$$\mathcal{C}_h(a, b, \mathbf{u}) = \sum_{(y,z,\mathbf{x}) \in \mathbb{Z}_2^{n+2}} \zeta^{\Delta(f)+(y\oplus z)\Delta(g)-(a\oplus b)g(\mathbf{x}\oplus\mathbf{u})+yz\, s(\mathbf{x})-(z\oplus a)(y\oplus b)s(\mathbf{x}\oplus\mathbf{u})}. \tag{10}$$

Assume that h is gbent on $\mathbb{Z}_2^{n+2}$, and so, in particular $\mathcal{C}_f(1, 1, \mathbf{0}) = 0$. Replace $a = b = 1$ and $\mathbf{u} = \mathbf{0}$ in equation (10), and since $\Delta(F) = 0$ if $\mathbf{u} = \mathbf{0}$, we get

$$\begin{aligned} \mathcal{C}_h(1, 1, \mathbf{0}) &= \sum_{(y,z,\mathbf{x}) \in \mathbb{Z}_2^{n+2}} \zeta^{(yz-\bar{y}\bar{z})s(\mathbf{x})} \\ &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \sum_{y,z} \zeta^{(yz-\bar{y}\bar{z})s(\mathbf{x})} \\ &= \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \left(\zeta^{-s(\mathbf{x})} + \zeta^{s(\mathbf{x})} + 2 \right) \\ &= \sum_{\mathbf{x}: s(\mathbf{x}) = \frac{q}{2}} 0 + \sum_{\mathbf{x}: s(\mathbf{x}) = l, l \neq \frac{q}{2}} k, \text{ for all } l \in \mathbb{Z}_q \setminus \left\{ \frac{q}{2} \right\}, 0 < k \leq 4. \end{aligned}$$

which follows from the following relations, (since $\zeta = e^{\frac{2\pi\imath}{q}}$)

$$\zeta^r + \zeta^{-r} + 2 = 0 \Leftrightarrow \zeta^r = -1 \Leftrightarrow r = \frac{q}{2}, \text{ and}$$

$$\zeta^r + \zeta^{-r} + 2 = 2\left(1 + \cos\frac{2\pi r}{q}\right) > 0, \text{ if } r \neq \frac{q}{2}.$$

Since $\mathcal{C}_h(1,1,\mathbf{0}) = 0$ this implies that $s(\mathbf{x}) = \frac{q}{2}$ for every $\mathbf{x} \in \mathbb{Z}_2^n$. Further, using $s(\mathbf{x}) = \frac{q}{2}$ in (10), we obtain

$$\begin{aligned}
\mathcal{C}_h(a,b,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)-(a\oplus b)g(\mathbf{x}\oplus\mathbf{u})} \sum_{(y,z)\in\mathbb{Z}_2^2} \zeta^{(y\oplus z)\Delta(g)+yz\, s(\mathbf{x})-(z\oplus a)(y\oplus b)s(\mathbf{x}\oplus\mathbf{u})} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)-(a\oplus b)g(\mathbf{x}\oplus\mathbf{u})} \Big(\zeta^{-ab\, s(\mathbf{x}\oplus\mathbf{u})} + \zeta^{\Delta(g)-\bar{b}a\, s(\mathbf{x}\oplus\mathbf{u})} \\
&\qquad\qquad + \zeta^{\Delta(g)-\bar{a}b\, s(\mathbf{x}\oplus\mathbf{u})} + \zeta^{s(\mathbf{x})-\bar{b}\bar{a}\, s(\mathbf{x}\oplus\mathbf{u})}\Big) \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)-(a\oplus b)g(\mathbf{x}\oplus\mathbf{u})} \left(\zeta^{-2ab} + \zeta^{\Delta(g)-2\bar{b}a} + \zeta^{\Delta(g)-2\bar{a}b} + \zeta^{2-2\bar{b}\bar{a}}\right).
\end{aligned}$$

Moreover,

$$\begin{aligned}
\mathcal{C}_h(0,0,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(2+2\zeta^{\Delta(g)}) = 2\mathcal{C}_f(\mathbf{u}) + 2\mathcal{C}_{f+g}(\mathbf{u}); \\
\mathcal{C}_h(0,1,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(\zeta^{\Delta(g)} + \zeta^{\Delta(g)-\frac{q}{2}}) = 0; \\
\mathcal{C}_h(1,0,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(\zeta^{\Delta(g)} + \zeta^{\Delta(g)-\frac{q}{2}}) = 0; \\
\mathcal{C}_h(1,1,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(-2+2\zeta^{\Delta(g)}) = -2\mathcal{C}_f(\mathbf{u}) + 2\mathcal{C}_{f+g}(\mathbf{u}).
\end{aligned} \tag{11}$$

Now, since h is gbent, then $\mathcal{C}_h(0,0,\mathbf{u}) = \mathcal{C}_h(1,1,\mathbf{u}) = 0$, from which we derive that $\mathcal{C}_f(\mathbf{u}) = \mathcal{C}_{f+g}(\mathbf{u}) = 0$ (if $\mathbf{u} \neq 0$) and so, both $f, f+g$ are gbent.

Conversely, we assume that both $f, f+g$ are gbent and $s(\mathbf{x}) = \frac{q}{2}$. From equations (11), we obtain that $\mathcal{C}_h(0,0,\mathbf{0}) = 2\mathcal{C}_f(\mathbf{0}) + 2\mathcal{C}_{f+g}(\mathbf{0}) = 2\cdot 2^n + 2\cdot 2^n = 2^{n+2}$, and $\mathcal{C}_h(z,y,\mathbf{u}) = 0$, when $(z,y,\mathbf{u}) \neq (0,0,\mathbf{0})$. The theorem is proved. □

For $g = 0$, we have the following corollary. We provide an alternative proof in this case.

Corollary 8 *Let $h : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^n \to \mathbb{Z}_q$ (n even) be the generalized Boolean function (symmetric with respect to two variables y, z) given by*

$$h(z,y,\mathbf{x}) = f(\mathbf{x}) + \frac{q}{2}\, yz \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, y, z \in \mathbb{Z}_2,$$

where $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ is an arbitrary generalized Boolean function. Then h is gbent if and only if f is gbent.

Proof. Since $\zeta = e^{\frac{2\pi i}{q}}$, therefore $\zeta^{\frac{q}{2}} = -1$. The Walsh transform of h at $(a,b,\mathbf{u}) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^n$ is

$$\mathcal{H}_h(a,b,\mathbf{u}) = 2^{-\frac{n+2}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{(y,z)\in\mathbb{Z}_2\times\mathbb{Z}_2} \zeta^{f(\mathbf{x})+\frac{q}{2}yz}(-1)^{\mathbf{u}\cdot\mathbf{x}+ay+bz}$$
$$= 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \left(\frac{1}{2} \sum_{(y,z)\in\mathbb{Z}_2\times\mathbb{Z}_2} (-1)^{yz}(-1)^{ay+bz} \right).$$

But it is easy to show that the function $k : \mathbb{Z}_2^2 \to \mathbb{Z}_2$ such that $k(z,y) = yz$ is bent, and so,

$$|\mathcal{H}_h(a,b,\mathbf{u})| = |\mathcal{H}_f(\mathbf{u})|, \text{ for all } a,b \in \mathbb{Z}_2 \text{ and } \mathbf{u} \in \mathbb{Z}_2^n,$$

which concludes our proof. □

5 Generalized Maiorana–McFarland and Dillon functions are contained in the generalized spreads class

Let ϕ_S denote the indicator function of any subset S of $\mathbb{Z}_2^n$.

Schmidt [15] proved that for any permutation σ on $\mathbb{Z}_2^t$ and $g \in \mathcal{GB}_t^4$, a function $f \in \mathcal{GB}_n^4$ defined by

$$f(\mathbf{x},\mathbf{y}) = 2\mathbf{x}\cdot\sigma(\mathbf{y}) + g(\mathbf{y}) \text{ for all } \mathbf{x},\mathbf{y} \in \mathbb{Z}_2^t, \tag{12}$$

is a generalized bent function. In Theorem 9 below we generalize this to functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$, for any even positive integer q, as follows

$$f(\mathbf{x},\mathbf{y}) = g(\mathbf{y}) + \frac{q}{2}\mathbf{x}\cdot\sigma(\mathbf{y}), \text{ for all } \mathbf{x},\mathbf{y} \in \mathbb{Z}_2^n, \tag{13}$$

for all $\mathbf{x},\mathbf{y} \in \mathbb{Z}_2^t$, where $g \in \mathcal{GB}_t^q$, σ is a permutation on $\mathbb{Z}_2^t$. The class of such functions is referred to as the *generalized Maiorana–McFarland class* $(GMMF)$.

Theorem 9 *Suppose q is an even positive integer. Let σ be a permutation on $\mathbb{Z}_2^n$, let $g : \mathbb{Z}_2^n \to \mathbb{Z}_q$ be an arbitrary function, then the function $f : \mathbb{Z}_2^{2n} \to \mathbb{Z}_q$ defined as*

$$f(\mathbf{x},\mathbf{y}) = g(\mathbf{y}) + \frac{q}{2}\mathbf{x}\cdot\sigma(\mathbf{y}) \text{ for all } \mathbf{x},\mathbf{y} \in \mathbb{Z}_2^n \tag{14}$$

is a gbent function and its dual is $g(\sigma^{-1}(\mathbf{x})) + \frac{q}{2}\mathbf{y}\cdot(\sigma^{-1}(\mathbf{x}))$.

Proof. Compute

$$\begin{aligned}\mathcal{H}_f(\mathbf{u},\mathbf{v}) &= 2^{-n} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{g(\mathbf{y})+\frac{q}{2}\mathbf{x}\cdot\sigma(\mathbf{y})}(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus\mathbf{v}\cdot\mathbf{y}} \\ &= 2^{-n} \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{g(\mathbf{y})}(-1)^{\mathbf{v}\cdot\mathbf{y}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{(\mathbf{u}\oplus\pi(\mathbf{y}))\cdot\mathbf{x}} \\ &= \sum_{\mathbf{y}\in\mathbb{Z}_2^n} \zeta^{g(\mathbf{y})}(-1)^{\mathbf{v}\cdot\mathbf{y}} \phi_{\{0\}}(\mathbf{u}\oplus\pi(\mathbf{y})). \\ &= \zeta^{g(\sigma^{-1}(\mathbf{u}))+\frac{q}{2}\mathbf{v}\cdot\sigma^{-1}(\mathbf{u})},\end{aligned}$$

and the theorem is proved. □

The following corollary is Theorem 5.3 of Schmidt [15].

Corollary 10 *Let σ be a permutation on $\mathbb{Z}_2^k$, $g : \mathbb{Z}_2^k \to \mathbb{Z}_4$ arbitrary, and let $f : \mathbb{Z}_2^{2k} \to \mathbb{Z}_4$ be given by*

$$f(\mathbf{x}, \mathbf{y}) = 2\sigma(\mathbf{x}) \cdot \mathbf{y} + g(\mathbf{x}).$$

Then f is a gbent function.

Carlet [2] introduced the generalized partial spreads class (GPS) of bent functions and conjectured that any bent function belongs to GPS. This conjecture was proved in affirmative by Carlet and Guillot [3]. A similar representation which provides a unique representation of bent functions were proposed by Carlet and Guillot [4]. Below we introduce a class for generalized bent functions which we refer to as the *generalized spreads class* (GS). We demonstrate that the Dillon type generalized bent functions as well as generalized Maiorana–McFarland type bent functions belong to GS. The question whether any generalized bent is in GS remains open.

Let $n = 2t$. Suppose $E_1, \ldots, E_k$ are t-dimensional subspaces of $\mathbb{Z}_2^n$ such that

$$\cup_{i=1}^k E_i = \cup_{i=1}^k E_i^\perp = \mathbb{Z}_2^n. \tag{15}$$

For each $\mathbf{x} \in \mathbb{Z}_2^n$ we define the following two sets

$$\mathcal{E}_\mathbf{x} = \{E_i : \mathbf{x} \in E_i\} \text{ and } \mathcal{E}_\mathbf{x}^\perp = \{E_i^\perp : \mathbf{x} \in E_i^\perp\}. \tag{16}$$

Theorem 11 *Let $m_1, \ldots, m_k \in \mathbb{Z}$ and $F : \mathbb{Z}_2^n \to \mathbb{C}$ is defined by*

$$F(\mathbf{x}) = \sum_{i=1}^k \zeta^{m_i} \phi_{E_i}(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{17}$$

Suppose

$$\sum_{\{i : E_i \in \mathcal{E}_\mathbf{x}\}} \zeta^{m_i}, \sum_{\{i : E_i^\perp \in \mathcal{E}_\mathbf{x}^\perp\}} \zeta^{m_i} \in \{\zeta^j : j = 0, 1, \ldots, q-1\}. \tag{18}$$

Then the function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ defined by

$$\zeta^{f(\mathbf{x})} = F(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{19}$$

is a generalized bent function. The class of such functions is referred to as the generalized spreads class (GS).

Proof. Suppose $f \in \mathcal{GB}_n^q$ satisfies (19). Then

$$\begin{aligned}
\mathcal{H}_f(\mathbf{u}) &= 2^{-t} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} = 2^{-t} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} F(\mathbf{x}) (-1)^{\mathbf{u} \cdot \mathbf{x}} \\
&= 2^{-t} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \sum_{i=1}^k \zeta^{m_i} \phi_{E_i}(\mathbf{x}) (-1)^{\mathbf{u} \cdot \mathbf{x}} = 2^{-t} \sum_{i=1}^k \zeta^{m_i} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \phi_{E_i}(\mathbf{x}) (-1)^{\mathbf{u} \cdot \mathbf{x}} \\
&= 2^{-t} \sum_{i=1}^k \zeta^{m_i} \sum_{\mathbf{x} \in E_i} (-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{i=1}^k \zeta^{m_i} \phi_{E_i^\perp}(\mathbf{u}) = \sum_{\{i : E_i^\perp \in \mathcal{E}_\mathbf{u}^\perp\}} \zeta^{m_i}.
\end{aligned} \tag{20}$$

Therefore any the function $f \in \mathcal{GB}_n^q$ satisfying (17) is generalized bent if the condition (18) is satisfied. □

Since the only units in the ring of Gaussian integers are $\pm 1, \pm\imath$, we have the next corollary, for the case $q = 4$.

Corollary 12 *Let $m_1, \ldots, m_k \in \mathbb{Z}$ and $F : \mathbb{Z}_2^n \to \mathbb{C}$ is defined by*

$$F(\mathbf{x}) = \sum_{i=1}^{k} \imath^{m_i} \phi_{E_i}(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{21}$$

The function $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$ defined by

$$\imath^{f(\mathbf{x})} = F(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{22}$$

is a generalized bent function if and only if $\sum_{\{i:E_i^\perp \in \mathcal{E}_{\mathbf{x}}^\perp\}} \imath^{m_i} \in \{\pm 1, \pm\imath\}$.

The analogue of Dillon type functions is introduced in [9]. Suppose that E_i $(i = 1, \ldots, 2^t + 1)$ are t-dimensional subspaces of $\mathbb{Z}_2^n$ with $E_i \cap E_j = \{0\}$, if $i \neq j$. It can be checked that this implies $E_i^\perp \cap E_j^\perp = \{0\}$, if $i \neq j$. It is also noted that in this case $\cup_{i=1}^{2^t+1} E_i = \cup_{i=1}^{2^t+1} E_i^\perp = \mathbb{Z}_2^n$. Thus (15) is satisfied. A natural generalization of [9, Theorem 10] leads us to a class of generalized bent functions which we refer to the *the generalized Dillon class* (GD).

Theorem 13 *Let $k, m_1, \ldots, m_{2^t+1}$ be integers such that $\sum_{i=1}^{2^t+1} \zeta^{m_i} = \zeta^k$. Let $F : \mathbb{Z}_2^n \to \mathbb{C}$ be given by*

$$F(\mathbf{x}) = \sum_{i=1}^{2^t+1} \zeta^{m_i} \phi_{E_i}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{23}$$

Then the function $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ defined by

$$\zeta^{f(\mathbf{x})} = F(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n \tag{24}$$

is a generalized bent function.

Below we demonstrate that GD and $GMMF$ both are contained in GS. Our proof is similar to the proof by Carlet [2] in the Boolean case.

Theorem 14 *The generalized Dillon and generalized Maiorana–McFarland classes are both contained in the generalized spreads class (i.e., $GD \cup GMMF \subseteq GS$).*

Proof. First, it can be directly checked that, for generalized Dillon type generalized bent functions with $m_1, \ldots, m_{2^t+1}, k \in \mathbb{Z}$ such that $\sum_{i=1}^{2^t+1} \zeta^{m_i} = \zeta^k$, $E_i \cap E_j = \{0\}$ and $E_i^\perp \cap E_j^\perp = \{0\}$ if $i \neq j$, the equations (18) are satisfied by the subspaces E_i's and $E_i^\perp$'s. Therefore, $GD \subseteq GS$.

Next, we concentrate on the $GMMF$ and assume q to be an even positive integer. Without loss of generality, we assume $\sigma(0) = 0$. Consider the following t-dimensional subspaces,

$$\begin{aligned} E_{\mathbf{z}} &= \sigma(\mathbf{z})^{\perp} \times \{0, \mathbf{z}\}, \\ K_{\mathbf{z}} &= (\sigma(\mathbf{z})^{\perp} \times \{0\}) \cup ((\mathbb{Z}_2^t \setminus (\sigma(\mathbf{z})^{\perp})) \times \{\mathbf{z}\}), \end{aligned} \tag{25}$$

for all $\mathbf{z} \in \mathbb{Z}_2^t \setminus \{0\}$. The duals of the above subspaces are as follows:

$$\begin{aligned} E_{\mathbf{z}}^{\perp} &= \{0, \sigma(\mathbf{z})\} \times \mathbf{z}^{\perp}, \\ K_{\mathbf{z}}^{\perp} &= (\{0\} \times \mathbf{z}^{\perp}) \cup (\{\sigma(\mathbf{z})\} \times (\mathbb{Z}_2^t \setminus \mathbf{z}^{\perp})). \end{aligned} \tag{26}$$

for all $\mathbf{z} \in \mathbb{Z}_2^t \setminus \{0\}$. Let

$$\begin{aligned} F(\mathbf{x}, \mathbf{y}) = &\sum_{\mathbf{z} \in \mathbb{Z}_2^t \setminus \{0\}} \zeta^{g(\mathbf{z})} \phi_{E_{\mathbf{z}}}(\mathbf{x}, \mathbf{y}) + \sum_{\mathbf{z} \in \mathbb{Z}_2^t \setminus \{0\}} (-\zeta^{g(\mathbf{z})}) \phi_{K_{\mathbf{z}}}(\mathbf{x}, \mathbf{y}) \\ &+ \zeta^{g(0)} \phi_{\mathbb{Z}_2^t \times \{0\}}(\mathbf{x}, \mathbf{y}), \end{aligned} \tag{27}$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^t$. We observe that in case $\mathbf{y} \neq 0$

$$F(\mathbf{x}, \mathbf{y}) = \begin{cases} \zeta^{g(\mathbf{y})}, \text{ if } \mathbf{x} \in \sigma(y)^{\perp} \\ \zeta^{\frac{q}{2} + g(\mathbf{y})}, \text{ if } \mathbf{x} \in \mathbb{Z}_2^t \setminus \sigma(y)^{\perp}. \end{cases}$$

In case $\mathbf{y} = 0$ we observe that $(\mathbf{x}, 0) \in E_{\mathbf{z}}$ if and only if $(\mathbf{x}, 0) \in K_{\mathbf{z}}$. Therefore for all $\mathbf{x} \in \mathbb{Z}_2^t$, $F(\mathbf{x}, 0) = \zeta^{g(0)}$. Thus, the function

$$f(\mathbf{x}, \mathbf{y}) = \frac{q}{2} \mathbf{x} \cdot \sigma(\mathbf{y}) + g(\mathbf{y})$$

satisfies $F(\mathbf{x}, \mathbf{y}) = \zeta^{f(\mathbf{x}, \mathbf{y})}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_2^t$. This proves that $GMMF \subseteq GS$. □

References

1. C.Bey, G.M. Kyureghyan, *On Boolean functions with the sum of every two of them being bent*, Des. Codes Cryptogr. 49 (2008), 341–346.
2. C. Carlet, *Generalized partial spreads*, IEEE Trans. Inform. Theory 41(5) (1995), 1482–1487.
3. C. Carlet, P. Guillot *A characterization of binary bent functions*, J. Combin. Theory (A) 76(2) (1996), 328–335.
4. C. Carlet, P. Guillot, *An alternate characterization of the bentness of binary functions, with uniqueness* Des. Codes Cryptography 14(2) (1998), 133–140.
5. C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
6. C. Carlet, *Vectorial Boolean functions for cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.

7. T. W. Cusick, P. Stănică, Cryptographic Boolean functions and applications, Elsevier – Academic Press, 2009.
8. J. F. Dillon, *Elementary Hadamard difference sets*, Proc. of Sixth S.E. Conference of Combinatorics, Graph Theory, and Computing, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg 1975, 237–249.
9. S. Gangopadhyay, B. K. Singh and P. Stănică, *On Generalized Bent Functions*, preprint.
10. M. D. Hirschhorn, *A simple proof of Jacobis four-square theorem*, Proc. Amer. Math. Soc., 101 (1987), 436–438.
11. P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory (A) 40 (1985), 90–107.
12. F. J. MacWilliams, N. J. A. Sloane, The theory of error–correcting codes, North-Holland, Amsterdam, 1977.
13. O. S. Rothaus, *On bent functions*, J. Combinatorial Theory Ser. A 20 (1976), 300–305.
14. P. Sarkar, S. Maitra, *Cross–Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes*, Theory Comput. Systems 35 (2002), 39–57.
15. K-U. Schmidt, *Quaternary Constant-Amplitude Codes for Multicode CDMA*, IEEE International Symposium on Information Theory, ISIT'2007 (Nice, France, June 24–29, 2007), 2781–2785; available at http://arxiv.org/abs/cs.IT/0611162.
16. P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, http://eprint.iacr.org/2009/544.pdf.
17. P. Stanica, T. Martinsen, *Octal Bent Generalized Boolean Functions*, http://eprint.iacr.org/2011/089.pdf.