Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9622-5

Bent and generalized bent Boolean functions

Pantelimon Stănică · Thor Martinsen · Sugata Gangopadhyay · Brajesh Kumar Singh

Received: 6 July 2011 / Revised: 4 November 2011 / Accepted: 24 January 2012

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 analogues of Maiorana–McFarland type bent functions and Dillon's functions in the generalized set up. A class of bent functions called generalized spreads is introduced and we show that it contains all Dillon type generalized bent functions and Maiorana–McFarland type generalized bent functions. Thus, unification of two different types of generalized bent functions is achieved. The crosscorrelation spectrum of generalized Dillon type bent functions is also characterized. We further characterize generalized bent Boolean functions defined on $\mathbb{Z}_2^n$ with values in $\mathbb{Z}_4$ and $\mathbb{Z}_8$. Moreover, we propose several constructions of such generalized bent functions for both n even and n odd.

Keywords Generalized Boolean functions · Generalized bent functions · Walsh–Hadamard transform

Mathematics Subject Classification (2000) 94A60 · 94C10 · 06E30

Communicated by C. Carlet.

P. Stănică · T. Martinsen
Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA
e-mail: pstanica@nps.edu

T. Martinsen
e-mail: tmartins@nps.edu

S. Gangopadhyay (✉) · B. K. Singh
Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667, India
e-mail: gsugata@gmail.com

B. K. Singh
e-mail: singh.brajesho584@gmail.com

Published online: 12 February 2012

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
12 FEB 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Bent and generalized bent Boolean functions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School (NPS),Department of Applied Mathematics,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In this paper, we investigate the properties of generalized bent functions defined on Zn2 with values in Zq, where q ≥ 2 is any positive integer. We characterize the class of generalized bent functions symmetric with respect to two variables, provide analogues of Maiorana?McFarland type bent functions and Dillon?s functions in the generalized set up. A class of bent functions called generalized spreads is introduced and we show that it contains all Dillon type generalized bent functions and Maiorana?McFarland type generalized bent functions. Thus, unification of two different types of generalized bent functions is achieved. The crosscorrelation spectrum of generalized Dillon type bent functions is also characterized. We further characterize generalized bent Boolean functions defined on Zn2 with values in Z4 and Z8. Moreover, we propose several constructions of such generalized bent functions for both n even and n odd.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

1 Introduction

In the recent years several authors have proposed generalizations of Boolean functions [10, 15,16,18,19] 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 was invented by Rothaus [13]).

Let us denote the set of integers, real numbers and complex numbers by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, respectively and let the ring of integers modulo r be denoted by $\mathbb{Z}_r$. The vector space $\mathbb{Z}_2^n$ is the space of all n-tuples $\mathbf{x} = (x_n, \ldots, x_1)$ of elements from $\mathbb{Z}_2$ with the standard operations. By '$+$' we denote the addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, whereas '$\oplus$' denotes the addition over $\mathbb{Z}_2^n$ for all $n \geq 1$. Addition modulo q is denoted by '$+$' and it is understood from the context. If $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1)$ are in $\mathbb{Z}_2^n$, 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 $|S|$, and the conjugate of a bit b will also be 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 $\overline{z} = a - b\,\imath$ denotes the complex conjugate of z, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$.

We call a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ ($q \geq 2$ a positive integer) a *generalized Boolean function* on n variables [16]. We denote the set of such functions by $\mathcal{GB}_n^q$. If $q = 2$, we obtain the classical Boolean functions on n variables, whose set will be denoted by $\mathcal{B}_n$.

Let $\zeta = e^{2\pi\imath/q}$ be the complex q-primitive root of unity. 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

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

If $q = 2$, we obtain the (normalized) *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$, which will be denoted by W_f. A function $f \in \mathcal{GB}_n^q$ is a *generalized bent* (*gbent*) function if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. When $q = 2$, then f is bent (these exist for n even, only). 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 $\mathbf{u} \in \mathbb{Z}_2^n$. Suppose $f \in \mathcal{GB}_n^q$ is a gbent function such that for every such $\mathbf{u}$, we have $\mathcal{H}_f(\mathbf{u}) = \zeta^{k_u}$, for some $0 \leq k_u < q$. Then, 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). By applying Theorem 1 below, one can easily see that the dual of a gbent function is also gbent, since the Walsh–Hadamard transform of the dual F is $\mathcal{H}_F(\mathbf{u}) = \zeta^{f(\mathbf{u})}$. 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 $\mathcal{C}_f(\mathbf{u})$.

If $2^{h-1} < q \leq 2^h$, for any $f \in \mathcal{GB}_n^q$ we associate a unique sequence of Boolean functions $a_i \in \mathcal{B}_n (i = 0, 1, \ldots, h-1)$ such that

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{h-1} a_{h-1}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{1}$$

If $q = 4$, then for $f \in \mathcal{GB}_n^4$ as in (1) we define the Gray map $\psi(f) : \mathcal{GB}_n^4 \to \mathcal{B}_{n+1}$ by

$$\psi(f)(z, \mathbf{x}) = a_0(\mathbf{x}) z + a_1(\mathbf{x}), \text{ for all } (z, \mathbf{x}) \in \mathbb{Z}_2 \times \mathbb{Z}_2^n. \tag{2}$$

The function $\psi(f)$ is referred to as the Gray image of f.

2 Properties of Walsh–Hadamard transform on generalized Boolean functions

The following properties of the Walsh–Hadamard transform on generalized Boolean functions are similar to the Boolean function case.

Theorem 1 *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 a gbent function if and only if* $\mathcal{C}_f(\mathbf{u}) = \begin{cases} 2^n & \text{if } \mathbf{u} = 0, \\ 0 & \text{if } \mathbf{u} \neq 0. \end{cases}$

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

The properties of these transforms for $q = 2$ can be derived from the previous theorem (for more on Boolean functions, the interested reader can consult [5–7]).

Let $\zeta = \mathbf{e}^{2\pi\imath/q}$ be the q-primitive root of unity, and $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$ as in (1). It turns out that the generalized Walsh–Hadamard spectrum of f can be described (albeit, in a complicated manner) in terms of the Walsh–Hadamard spectrum of its Boolean components a_i.

Theorem 2 *The Walsh–Hadamard transform of* $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$, $2^{h-1} < q \leq 2^h$, *where* $f(\mathbf{x}) = \sum_{i=0}^{h-1} a_i(\mathbf{x})2^i$, $a_i \in \mathcal{B}_n$ *is given by*

$$\mathcal{H}_f(\mathbf{u}) = 2^{-h} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \sum_{J\subseteq I, K\subseteq\bar{I}} (-1)^{|J|} W_{\sum_{\ell\in J\cup K} a_\ell(\mathbf{x})}(\mathbf{u}).$$

Proof For brevity, we use the notations $\zeta_i := \zeta^{2^i}$. It is easy to see that, for $s \in \mathbb{Z}_2$, we have

$$z^s = \frac{1+(-1)^s}{2} + \frac{1-(-1)^s}{2} z, \tag{3}$$

and so, we have the identities $\zeta_i^{a_i(\mathbf{x})} = \frac{1}{2}\left(A_i + A_i'\zeta_i\right)$, where $A_i = 1 + (-1)^{a_i(\mathbf{x})}$, $A_i' = 1 - (-1)^{a_i(\mathbf{x})}$, and the complement $\bar{I} := \{0, 1, \ldots, h-1\}\backslash I$, for some subset I of $\{0, 1, \ldots, h-1\}$. The Walsh–Hadamard coefficients of f are

$$
\begin{aligned}
2^{n/2}\mathcal{H}_f(\mathbf{u}) &= \sum_{\mathbf{x}} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}} \zeta^{\sum_{i=0}^{h-1} a_i(\mathbf{x})2^i}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \prod_{i=0}^{h-1} \left(\zeta^{2^i}\right)^{a_i(\mathbf{x})} \\
&= \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \prod_{i=0}^{h-1} \frac{1}{2}\left(1 + (-1)^{a_i(\mathbf{x})} + (1 - (-1)^{a_i(\mathbf{x})})\zeta_i\right) \\
&= 2^{-h} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{I\subseteq\{0,\ldots,h-1\}} \prod_{i\in I, j\in\bar{I}} \zeta_i A_i' A_j \\
&= 2^{-h} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \prod_{i\in I, j\in\bar{I}} A_i' A_j \\
&= 2^{-h} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \sum_{J\subseteq I, K\subseteq\bar{I}} (-1)^{|J|}(-1)^{\sum_{j\in J} a_j(\mathbf{x})\oplus\sum_{k\in K} a_k(\mathbf{x})} \\
&= 2^{-h} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \sum_{J\subseteq I, K\subseteq\bar{I}} (-1)^{|J|} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}}(-1)^{\sum_{\ell\in J\cup K} a_\ell(\mathbf{x})},
\end{aligned}
$$

and so, we obtain our result. □

In Sect. 7 we will use this result, for the particular case $q = 8$, which will allow us to completely describe the gbent Boolean functions in that case.

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

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

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 $\mathbf{u} \in \mathbb{Z}_2^n \backslash \{\mathbf{0}\}$.

The next two results were shown in a different context in [17]. One can straightforwardly infer, by modifying those proofs that these result hold under the current notions, as well.

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*

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

In particular, for $r = 1$, $\mathcal{C}_f(0\mathbf{w}) = \mathcal{C}_{f_0}(\mathbf{w}) + \mathcal{C}_{f_1}(\mathbf{w})$, and $\mathcal{C}_f(1\mathbf{w}) = 2Re[\mathcal{C}_{f_0,f_1}(\mathbf{w})]$. Further, $f, g \in \mathcal{GB}_n^q$ have complementary autocorrelation if and only if

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

Theorem 4 *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 $\frac{\mathcal{H}_g(\mathbf{u})}{\mathcal{H}_f(\mathbf{u})} \in \mathbb{R}\imath$ whenever $|\mathcal{H}_f(\mathbf{u})||\mathcal{H}_g(\mathbf{u})| \neq 0$.*

Theorem 5 *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 $\epsilon = \begin{cases} 0, q/2 & if\ q\ is\ even \\ 0 & if\ q\ is\ odd \end{cases}$. *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 $f, g, s \in \mathcal{GB}_n^q$ such that

$$h(z, y, \mathbf{x}) = f(\mathbf{x}) + (y \oplus z) g(\mathbf{x}) + yz s(\mathbf{x}) \tag{4}$$

where $y, z \in \mathbb{Z}_2$ and $\mathbf{x} \in \mathbb{Z}_2^n$ and $\mathbb{Z}_2^{n+2}$ is identified with $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2^n$. The binary case, that is, $q = 2$, is investigated by Zhao and Li [20]. In the following theorem we obtain a generalization of their main result.

Theorem 6 *Suppose that q is a positive integer. Let h be a generalized Boolean function symmetric about two variables, as in (4). 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 (4),

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

and the autocorrelation

$$\mathcal{C}_h(a, b, \mathbf{u}) = \sum_{(y,z,\mathbf{x}) \in \mathbb{Z}_2^{n+2}} \zeta^{\Delta(f)+(y\oplus z)\Delta(g)-(a\oplus b)g(\mathbf{x}\oplus\mathbf{u})+yz\, s(\mathbf{x})-(z\oplus a)(y\oplus b)s(\mathbf{x}\oplus\mathbf{u})}. \tag{5}$$

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 Eq. 5, and since $\Delta(f) = 0$ if $\mathbf{u} = \mathbf{0}$, we get

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

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

$$\begin{aligned} k_l &= \zeta^l + \zeta^{-l} + 2 = 0 \Leftrightarrow \zeta^l = -1 \Leftrightarrow l = \frac{q}{2}, \text{ and} \\ k_l &= \zeta^l + \zeta^{-l} + 2 = 2\left(1 + \cos\frac{2\pi l}{q}\right) \in (0, 4], \text{ if } l \neq \frac{q}{2}. \end{aligned}$$

Since $\mathcal{C}_h(1, 1, \mathbf{0}) = 0$ it follows 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 (5), we obtain

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

Moreover,

$$\begin{aligned}
\mathcal{C}_h(0,0,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(2+2\zeta^{\Delta(g)}) = 2\mathcal{C}_f(\mathbf{u}) + 2\mathcal{C}_{f+g}(\mathbf{u});\\
\mathcal{C}_h(0,1,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(\zeta^{\Delta(g)} + \zeta^{\Delta(g)-\frac{q}{2}}) = 0;\\
\mathcal{C}_h(1,0,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(\zeta^{\Delta(g)} + \zeta^{\Delta(g)-\frac{q}{2}}) = 0;\\
\mathcal{C}_h(1,1,\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{\Delta(f)}(-2+2\zeta^{\Delta(g)}) = -2\mathcal{C}_f(\mathbf{u}) + 2\mathcal{C}_{f+g}(\mathbf{u}).
\end{aligned} \tag{6}$$

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 Eq. 6, 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.

Corollary 7 *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 $h(z,y,\mathbf{x}) = f(\mathbf{x}) + \frac{q}{2}yz$ 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.*

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 $\mathbb{Z}_2^n$.

In Theorem 8 below we generalize a result of Schmidt [15, Theorem 5.3] (obtained for $q = 4$). The class of functions (7) below is referred to as the *generalized Maiorana–McFarland class* ($GMMF$).

Theorem 8 *Suppose that q is an even positive integer. Let σ be a permutation on $\mathbb{Z}_2^n$, and 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*

$$f(\mathbf{x},\mathbf{y}) = g(\mathbf{y}) + \frac{q}{2}\mathbf{x}\cdot\sigma(\mathbf{y}) \text{ for all } \mathbf{x},\mathbf{y} \in \mathbb{Z}_2^n \tag{7}$$

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

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

and the theorem is proved. □

In Sect. 7 (Conclusion and open problems) of [16], Solé and Tokareva mentioned that although there are analogues of Maiorana–MacFarland type construction in the context of quaternary Boolean functions and generalized Boolean functions [10,15], no construction has been proposed, which would generalize Dillon's partial–spreads type bent functions [8]. We propose such a construction, thus answering the challenge by Solé and Tokareva [16].

Let $n = 2t$. 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 also follows that $E_i^\perp \cap E_j^\perp = \{0\}$, if $i \neq j$). It is also noted that in this case $\cup_{i=1}^{2^t+1} E_i = \cup_{i=1}^{2^t+1} E_i^\perp = \mathbb{Z}_2^n$. In the following theorem we propose a class of gbent functions which we refer to as *the generalized Dillon class* (GD).

Theorem 9 *Let $n = 2t$ and $k, m_1, \ldots, m_{2^t+1}$ 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*

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

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

$$\zeta^{f(\mathbf{x})} = F(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n \tag{8}$$

is a gbent function.

Proof We compute

$$\begin{aligned}
\mathcal{H}_f(\mathbf{u}) &= 2^{-t} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^{-t} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} F(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^{-t} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{i=1}^{2^t+1} \zeta^{m_i} \phi_{E_i}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= 2^{-t} \sum_{i=1}^{2^t+1} \zeta^{m_i} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \phi_{E_i}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^{-t} \sum_{i=1}^{2^t+1} \zeta^{m_i} \sum_{\mathbf{x}\in E_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= 2^{-t} \sum_{i=1}^{2^t+1} \zeta^{m_i} 2^t \phi_{E_i^\perp}(\mathbf{u}) \\
&= \sum_{i=1}^{2^t+1} \zeta^{m_i} \phi_{E_i^\perp}(\mathbf{u}) = \begin{cases} \zeta^{m_i} & \text{if } \mathbf{u} \in E_i^\perp \backslash \{0\}, \\ \zeta^k & \text{if } \mathbf{u} = 0, \end{cases}
\end{aligned}$$

which proves that f is a generalized bent 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 construction which provides a unique representation of bent functions was proposed by Carlet and Guillot [4]. Below we introduce a class for gbent functions which we refer to as the *generalized spreads class* (GS). We demonstrate that the Dillon type gbent functions as well as generalized Maiorana–McFarland type bent functions belong to GS. The question whether any gbent function is in GS remains open.

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

$$\cup_{i=1}^{k} E_i = \cup_{i=1}^{k} E_i^\perp = \mathbb{Z}_2^n. \tag{9}$$

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

$$\mathcal{E}_\mathbf{x} = \{E_i : \mathbf{x} \in E_i\} \text{ and } \mathcal{E}_\mathbf{x}^\perp = \{E_i^\perp : \mathbf{x} \in E_i^\perp\}. \tag{10}$$

Theorem 10 *Let $m_1, \ldots, m_k \in \mathbb{Z}$ and $F : \mathbb{Z}_2^n \to \mathbb{C}$ be defined by*

$$F(\mathbf{x}) = \sum_{i=1}^{k} \zeta^{m_i} \phi_{E_i}(\mathbf{x}) \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{11}$$

Suppose that

$$\sum_{\{i:E_i \in \mathcal{E}_{\mathbf{x}}\}} \zeta^{m_i}, \sum_{\{i:E_i^{\perp} \in \mathcal{E}_{\mathbf{x}}^{\perp}\}} \zeta^{m_i} \in \{\zeta^j : j = 0, 1, \ldots, q-1\}, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{12}$$

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

$$\zeta^{f(\mathbf{x})} = F(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{13}$$

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

Proof Suppose $f \in \mathcal{GB}_n^q$ satisfies (13). Then

$$\begin{aligned}
\mathcal{H}_f(\mathbf{u}) &= 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} F(\mathbf{x}) (-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \sum_{i=1}^{k} \zeta^{m_i} \phi_{E_i}(\mathbf{x}) (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^{-n/2} \sum_{i=1}^{k} \zeta^{m_i} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \phi_{E_i}(\mathbf{x}) (-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= 2^{-n/2} \sum_{i=1}^{k} \zeta^{m_i} \sum_{\mathbf{x} \in E_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{i=1}^{k} \zeta^{m_i} \phi_{E_i^{\perp}}(\mathbf{u}) = \sum_{\{i:E_i^{\perp} \in \mathcal{E}_{\mathbf{u}}^{\perp}\}} \zeta^{m_i}.
\end{aligned} \tag{14}$$

Therefore any function $f \in \mathcal{GB}_n^q$ satisfying (11) is gbent if the condition (12) 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 11 *Let $m_1, \ldots, m_k \in \mathbb{Z}$ and $F : \mathbb{Z}_2^n \to \mathbb{C}$ be defined by $F(\mathbf{x}) = \sum_{i=1}^{k} \imath^{m_i} \phi_{E_i}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$. The function $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$ defined by $\imath^{f(\mathbf{x})} = F(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$ is a gbent function if and only if $\sum_{\{i:E_i \in \mathcal{E}_{\mathbf{x}}\}} \imath^{m_i}, \sum_{\{i:E_i^{\perp} \in \mathcal{E}_{\mathbf{x}}^{\perp}\}} \imath^{m_i} \in \{\pm 1, \pm\imath\}$, for all $\mathbf{x} \in \mathbb{Z}_2^n$.*

The fact that integers $k, m_1, m_2, \ldots, m_{2^t+1}$ exist (at least for q even) such that $\sum_{i=1}^{2^t+1} \zeta^{m_i} = \zeta^k$ is guaranteed by the main result of Lam and Leung [12, Main Theorem], which we briefly state below. For any given q, let $W(q)$ be the set of weights ℓ for which there exist m_i with $\sum_{i=1}^{\ell} \zeta^{m_i} = 0$. Lam and Leung showed that, if $q = \prod_{i=1}^{r} p_i^{a_i}$, then $W(q) = p_1\mathbb{N} + \cdots + p_r\mathbb{N}$. Thus, in our case, if $q = \prod_{i=1}^{r} p_i^{a_i}$ is even, and so, $p_1 = 2$, then $2^t + 2 = 2(2^{t-1} + 1) \in W(q) = 2\mathbb{N} + \cdots + p_r\mathbb{N}$. It follows that there exist m_i, $1 \le i \le 2^t + 2$, such that $\sum_{i=1}^{2^t+2} \zeta^{m_i} = 0$, and so, $\sum_{i=1}^{2^t+1} \zeta^{m_i} = -\zeta^{2^t+2} = \zeta^{q/2+2^t+2}$, using the fact that $\zeta^{q/2} = -1$, which shows our claim.

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 12 *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 gbent 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 Eq. 12 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,

$$\begin{aligned} E_{\mathbf{z}} &= \sigma(\mathbf{z})^\perp \times \{0, \mathbf{z}\}, \\ K_{\mathbf{z}} &= (\sigma(\mathbf{z})^\perp \times \{0\}) \cup ((\mathbb{Z}_2^t \backslash (\sigma(\mathbf{z})^\perp)) \times \{\mathbf{z}\}), \end{aligned} \tag{15}$$

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

$$\begin{aligned} E_{\mathbf{z}}^\perp &= \{0, \sigma(\mathbf{z})\} \times \mathbf{z}^\perp, \\ K_{\mathbf{z}}^\perp &= (\{0\} \times \mathbf{z}^\perp) \cup (\{\sigma(\mathbf{z})\} \times (\mathbb{Z}_2^t \backslash \mathbf{z}^\perp)). \end{aligned} \tag{16}$$

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

$$F(\mathbf{x}, \mathbf{y}) = \sum_{\mathbf{z} \in \mathbb{Z}_2^t \backslash \{0\}} \zeta^{g(\mathbf{z})} \phi_{E_{\mathbf{z}}}(\mathbf{x}, \mathbf{y}) + \sum_{\mathbf{z} \in \mathbb{Z}_2^t \backslash \{0\}} (-\zeta^{g(\mathbf{z})}) \phi_{K_{\mathbf{z}}}(\mathbf{x}, \mathbf{y}) + \zeta^{g(0)} \phi_{\mathbb{Z}_2^t \times \{0\}}(\mathbf{x}, \mathbf{y}), \tag{17}$$

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

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

When $\mathbf{y} = 0$ 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 $GMMF \subseteq GS$. □

6 A characterization of generalized bent functions in $\mathcal{GB}_n^4$

In this section we start by giving the crosscorrelation spectrum of any two Dillon type functions in $\mathcal{GB}_n^4$. Suppose that $n = 2t$ and $E_i (i = 1, \ldots, 2^t + 1)$ are t-dimensional subspaces of $\mathbb{Z}_2^n$ with $E_i \cap E_j = \{0\}$, if $i \neq j$.

Theorem 13 *Suppose f and g are two Dillon type generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4$ such that $\imath^{f(\mathbf{x})} = \sum_{i=1}^{2^t+1} \imath^{a_i} \phi_{E_i}(\mathbf{x})$ and $\imath^{g(\mathbf{x})} = \sum_{i=1}^{2^t+1} \imath^{b_i} \phi_{E_i}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$ and $\sum_{i=1}^{2^t+1} \imath^{a_i} = \imath^k$, $\sum_{i=1}^{2^t+1} \imath^{a_i} = \imath^\ell$. If $\sum_{i=1}^{2^t+1} \sum_{j=1, j\neq i}^{2^t+1} \imath^{a_i - b_j} = \imath^{k-\ell}$, then*

$$\mathcal{C}_{f,g}(\mathbf{u}) = \begin{cases} 2^t \imath^{a_i - b_i}, & \text{if } \mathbf{u} \neq 0 \\ 2^t \imath^{k-\ell}, & \text{if } \mathbf{u} = 0. \end{cases} \tag{18}$$

Proof Using Theorem 9 we obtain $\mathcal{H}_f(\mathbf{u}) = \sum_{i=1}^{2^t+1} \imath^{a_i} \phi_{E_i^\perp}(\mathbf{u})$ and $\mathcal{H}_g(\mathbf{u}) = \sum_{i=1}^{2^t+1} \imath^{b_i} \phi_{E_i^\perp}(\mathbf{u})$. The crosscorrelation of f and g at $\mathbf{u} \in \mathbb{Z}_2^n$

$$\begin{aligned}
\mathcal{C}_{f,g}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{u})\overline{\mathcal{H}_g(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left(\sum_{i=1}^{2^t+1} \imath^{a_i} \phi_{E_i^\perp}(\mathbf{x})\right) \overline{\left(\sum_{i=1}^{2^t+1} \imath^{b_i} \phi_{E_i^\perp}(\mathbf{x})\right)} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \sum_{i=1}^{2^t+1} \imath^{a_i-b_i} \phi_{E_i^\perp}(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{i=1}^{2^t+1} \imath^{a_i-b_i} \sum_{\mathbf{x}\in E_i^\perp} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{i=1}^{2^t+1} \imath^{a_i-b_i} 2^t \phi_{E_i}(\mathbf{u}) \\
&= 2^t \sum_{i=1}^{2^t+1} \imath^{a_i-b_i} \phi_{E_i}(\mathbf{u}) = \begin{cases} 2^t \imath^{a_i-b_i}, \text{ if } \mathbf{u} \in E_i, \\ 2^t \imath^{k-\ell}, \text{ if } \mathbf{u} = 0. \end{cases}
\end{aligned} \tag{19}$$

Therefore for all $\mathbf{u} \in \mathbb{Z}_2^n$ we have $|\mathcal{C}_{f,g}(\mathbf{u})| = 2^t$. □

Next, we compute the crosscorrelation of two arbitrary generalized Boolean functions in $\mathcal{GB}_n^4$ in terms of the crosscorrelation of their component Boolean functions. As corollaries to the theorem proved below we provide alternative proofs of some results proved by Solé and Tokareva [16].

Theorem 14 *Suppose f and g are two generalized Boolean functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_4$ such that $f(\mathbf{x}) = a_1(\mathbf{x}) + 2b_1(\mathbf{x})$ and $g(\mathbf{x}) = a_2(\mathbf{x}) + 2b_2(\mathbf{x})$, where $a_i, b_i (i = 1, 2)$ are Boolean functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$. Then the crosscorrelation between f and g at $\mathbf{u} \in \mathbb{Z}_2^n$ is*

$$\mathcal{C}_{f,g}(\mathbf{u}) = \frac{1}{2}\left(C_{b_1,b_2}(\mathbf{u}) + C_{a_1+b_1,a_2+b_2}(\mathbf{u})\right) + \frac{\imath}{2}\left(C_{b_1,a_2+b_2}(\mathbf{u}) - C_{a_1+b_1,b_2}(\mathbf{u})\right).$$

Assume that $f : \mathbb{Z}_2^n \to \mathbb{Z}_4$, and write it as $f(\mathbf{x}) = a(\mathbf{x}) + 2b(\mathbf{x})$, where a, b are Boolean functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$. Then the autocorrelation of f at $\mathbf{u} \in \mathbb{Z}_2^n$ is

$$\mathcal{C}_f(\mathbf{u}) = \frac{1}{2}\left(C_b(\mathbf{u}) + C_{a+b}(\mathbf{u})\right).$$

The function $f \in \mathcal{GB}_n^4$ is generalized bent if and only if the functions b and $a + b$ have complementary autocorrelation, that is,

$$C_b(\mathbf{u}) + C_{a+b}(\mathbf{u}) = 0 \text{ for all } \mathbf{u} \in \mathbb{Z}_2^n \backslash \{0\}.$$

Proof We compute

$$\begin{aligned}
\mathcal{C}_{f,g}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \imath^{f(\mathbf{x})-g(\mathbf{x}\oplus\mathbf{u})} = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \imath^{a_1(\mathbf{x})-a_2(\mathbf{x}\oplus\mathbf{u})}(-1)^{b_1(\mathbf{x})\oplus b_2(\mathbf{x}\oplus\mathbf{u})} \\
&= \frac{1}{2}\left(C_{b_1,b_2}(\mathbf{u}) + C_{a_1+b_1,a_2+b_2}(\mathbf{u})\right) + \frac{\imath}{2}\left(C_{b_1,a_2+b_2}(\mathbf{u}) - C_{a_1+b_1,b_2}(\mathbf{u})\right).
\end{aligned} \tag{20}$$

which follows directly from the formula $\imath^{a-b} = \frac{1+(-1)^{a+b}}{2} + \frac{(-1)^b-(-1)^a}{2}\imath$, for all $a, b \in \{0, 1\}$.

The second part follows from (20) by setting $f = g$ (that is, $a_1 = a_2 = a$ and $b_1 = b_2 = b$). □

The following corollary is Theorem 32 proved by Solé and Tokareva [16].

Corollary 15 *Suppose n is a positive even integer and $f \in \mathcal{GB}_n^4$, $a, b \in \mathcal{B}_n$ such that $f(\mathbf{x}) = a(\mathbf{x}) + 2b(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$. Then the following statements are equivalent:*

(*i*) *The generalized Boolean function $f \in \mathcal{GB}_n^4$ is gbent;*
(*ii*) *The n-variable Boolean functions b and $a + b$ are both bent.*

Proof Suppose $f \in \mathcal{GB}_n^4$ is gbent. Therefore, by Theorem 14 the functions $b, a + b$ have complementary autocorrelations which implies that both $b, a + b$ are bent functions (n is even).

Conversely, if b and $a + b$ are bent functions they have complementary autocorrelations, and so, by Theorem 14, f is gbent. □

Next we give an alternate proof of Corollary 43 and a slightly generalized version of its converse presented in Proposition 44 by Solé and Tokareva [16].

Corollary 16 *Suppose $f \in \mathcal{GB}_n^4$, where $f(\mathbf{x}) = a(\mathbf{x}) + 2b(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}_2^n$ for some $a, b \in \mathcal{B}_n$. The function f is gbent if and only if*

(*i*) *$\psi(f)$ is bent, if n is odd.*
(*ii*) *$\psi(f)$ is semibent, if n is even and b and $a + b$ have complementary autocorrelation.*

Proof Let n be an odd positive integer. Suppose $f \in \mathcal{GB}_n^4$ is gbent. Theorem 14 implies that b and $a + b$ have complementary autocorrelation. Therefore by Theorem 4.2 of [14] the function $\psi(f) \in \mathcal{B}_{n+1}$ is bent.

Conversely, we suppose that the function $\psi(f) \in \mathcal{B}_{n+1}$ is bent. Then, by Theorem 4.2 of [14], b and $a + b$ have complementary autocorrelation. Therefore, by Theorem 14 f is gbent.

Let n be an even positive integer. Suppose that $f \in \mathcal{GB}_n^4$ is gbent. This implies that b and $a + b$ have complementary autocorrelation, which in turn implies that b and $a + b$ both are bent functions. Therefore $\psi(f)$ is a semibent function.

Conversely, we suppose that $\psi(f)$ is a semibent function. Let $b(\mathbf{x}) = \psi(f)(0, \mathbf{x})$ and $a(\mathbf{x}) + b(\mathbf{x}) = \psi(f)(1, \mathbf{x})$, for all $\mathbf{x} \in \mathbb{Z}_2^n$. In this case, it is to be noted that b and $a + b$ may or may not have complementary autocorrelation. Therefore, by Theorem 14, the function f is gbent if b and $a + b$ have complementary autocorrelation, otherwise f is not gbent. □

7 A characterization of generalized bent functions in $\mathcal{GB}_n^8$

In this section we extend the result of Solé and Tokareva [16] to generalized Boolean functions from $\mathbb{Z}_2^n$ into $\mathbb{Z}_8$. Let $\zeta = \mathbf{e}^{2\pi\imath/8} = \frac{\sqrt{2}}{2}(1 + \imath)$ be the 8-primitive root of unity. Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_8$ be as in (1), that is,

$$f(\mathbf{x}) = a_0(\mathbf{x}) + a_1(\mathbf{x})2 + a_2(\mathbf{x})2^2, \tag{21}$$

where $a_i(\mathbf{x})$ are Boolean functions, and '+' is the addition modulo 8. The next lemma is a particular case of Theorem 2, which gives the connection between Walsh–Hadamard transforms of f and its components as in (21).

Lemma 17 *Let $f \in \mathcal{GB}_n^8$ as in (21). Then,*

$$4\mathcal{H}_f(\mathbf{u}) = \alpha_0 W_{a_2}(\mathbf{u}) + \alpha_1 W_{a_0 \oplus a_2}(\mathbf{u}) + \alpha_2 W_{a_1 \oplus a_2}(\mathbf{u}) + \alpha_3 W_{a_0 \oplus a_1 \oplus a_2}(\mathbf{u}),$$

where $\alpha_0 = 1 + (1 + \sqrt{2})\imath$, $\alpha_1 = 1 + (1 - \sqrt{2})\imath$, $\alpha_2 = 1 + \sqrt{2} - \imath$, $\alpha_3 = 1 - \sqrt{2} - \imath$.

Corollary 18 *With the notations of the previous lemma, we have*

$$4\sqrt{2}|\mathcal{H}_f(\mathbf{u})|^2 = W^2 - X^2 + 2XY + Y^2 - 2WZ - Z^2 + \sqrt{2}(W^2 + X^2 + Y^2 + Z^2), \tag{22}$$

where, we use for brevity, $W := W_{a_2}(\mathbf{u})$, $X := W_{a_0\oplus a_2}(\mathbf{u})$, $Y := W_{a_1\oplus a_2}(\mathbf{u})$, $Z := W_{a_0\oplus a_1\oplus a_2}(\mathbf{u})$.

Proof By replacing α_i, ζ by their complex representations, the corollary follows in a rather straightforward, albeit tedious manner. □

Theorem 19 *Let* $f \in \mathcal{GB}_n^8$ *as in* (21). *Then:*

(*i*) *If n is even, then f is gbent if and only if* $a_2, a_0 \oplus a_2, a_1 \oplus a_2, a_0 \oplus a_1 \oplus a_2$ *are all bent, and* (∗): $W_{a_0\oplus a_2}(\mathbf{u})W_{a_1\oplus a_2}(\mathbf{u}) = W_{a_2}(\mathbf{u})W_{a_0\oplus a_1\oplus a_2}(\mathbf{u})$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n$;

(*ii*) *If n is odd, then f is gbent if and only if* $a_2, a_0\oplus a_2, a_1\oplus a_2, a_0\oplus a_1\oplus a_2$ *are semibent satisfying* (∗∗): $W_{a_0\oplus a_2}(\mathbf{u}) = W_{a_2}(\mathbf{u}) = 0$ *and* $|W_{a_1\oplus a_2}(\mathbf{u})| = |W_{a_0\oplus a_1\oplus a_2}(\mathbf{u})| = \sqrt{2}$; *or,* $|W_{a_0\oplus a_2}(\mathbf{u})| = |W_{a_2}(\mathbf{u})| = \sqrt{2}$ *and* $W_{a_1\oplus a_2}(\mathbf{u}) = W_{a_0\oplus a_1\oplus a_2}(\mathbf{u}) = 0$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n$.

Proof We use the W, X, Y, Z notations of Corollary 18. First, assume that $a_2, a_0 \oplus a_2, a_1 \oplus a_2, a_0\oplus a_1\oplus a_2$ are all bent (respectively, semibent). Then, replacing the corresponding values of the Walsh–Hadamard transforms in Eq. 22 and using the imposed condition (∗) (respectively, condition (∗∗)) on the Walsh–Hadamard coefficients, we obtain $4\sqrt{2}|\mathcal{H}_f(\mathbf{u})|^2 = 4\sqrt{2}$, and so, $|\mathcal{H}_f(\mathbf{u})| = 1$, that is, f is gbent.

Conversely, we assume that f is gbent, and so,

$$4\sqrt{2} = W^2 - X^2 + 2XY + Y^2 - 2WZ - Z^2 + \sqrt{2}(W^2 + X^2 + Y^2 + Z^2),$$

which prompts the system

$$W^2 - X^2 + 2XY + Y^2 - 2WZ - Z^2 = 0 \tag{23}$$

$$W^2 + X^2 + Y^2 + Z^2 = 4. \tag{24}$$

We are looking for solutions in $2^{-n/2}\,\mathbb{Z}$ (a subset of $\mathbb{Q}$, if n is even or $\sqrt{2}\,\mathbb{Q}$, if n is odd).

We look at Eq. 24, initially, and apply Jacobi's four squares theorem (see [9]).

Case (i). Let $n = 2k$ be even. Thus, W, X, Y, Z are all rational (certainly, not all 0). Write $W = 2^{-n/2}W'$, $X = 2^{-n/2}X'$, $Y = 2^{-n/2}Y'$, $Z = 2^{-n/2}Z'$, and replace (23) and (24) by the system in integers

$$W'^2 - X'^2 + 2X'Y' + Y'^2 - 2W'Z' - Z'^2 = 0 \tag{25}$$

$$W'^2 + X'^2 + Y'^2 + Z'^2 = 2^{2k+2}. \tag{26}$$

Now, by Jacobi's four-squares theorem, we know there are exactly 24 solutions of (26), which are all variations in ± sign and order of $(\pm 2^k, \pm 2^k, \pm 2^k, \pm 2^k)$ or $(\pm 2^{k+1}, 0, 0, 0)$. Further, it is straightforward to check that among these 24 solutions, only the eight tuples (X', Y', W', Z') in the list below are also satisfying Eq. 25,

$$(-2^k, -2^k, -2^k, -2^k), (2^k, 2^k, -2^k, -2^k), (-2^k, -2^k, 2^k, 2^k), (-2^k, 2^k, -2^k, 2^k),$$
$$(2^k, -2^k, -2^k, 2^k), (-2^k, 2^k, 2^k, -2^k), (2^k, -2^k, 2^k, -2^k), (2^k, 2^k, 2^k, 2^k).$$

This implies that $(X, Y, W, Z) \in 2^{-n/2}\mathbb{Z}^4$ are any of the following:

$$\begin{aligned}&(-1,-1,-1,-1), (1,1,-1,-1), (-1,-1,1,1), (-1,1,-1,1),\\ &(1,-1,-1,1), (-1,1,1,-1), (1,-1,1,-1), (1,1,1,1),\end{aligned} \tag{27}$$

and (i) is shown (one can check easily that these solutions also satisfy condition $(*)$).
Case (ii). Let $n = 2k + 1$ be odd. Then, at least one of X, Y, W, Z is nonzero and belongs to $\sqrt{2}\,\mathbb{Q})$. As before, write $W = 2^{-n/2}W'$, $X = 2^{-n/2}X'$, $Y = 2^{-n/2}Y'$, $Z = 2^{-n/2}Z'$, and replace (23) and (24) by the system in integers

$$W'^2 - X'^2 + 2X'Y' + Y'^2 - 2W'Z' - Z'^2 = 0 \tag{28}$$
$$W'^2 + X'^2 + Y'^2 + Z'^2 = 2 \cdot 2^{2k+2}, \tag{29}$$

and so, by Jacobi's four-squares theorem, Eq. 29 has exactly 24 solutions, which are all variations in $\pm$ sign and order of $(\pm 2^{k+1}, \pm 2^{k+1}, 0, 0)$. Further, it is straightforward to check that among these 24 solutions, the eight tuples (X', Y', W', Z') in the list below are also satisfying Eq. 28,

$$(0, 2^{k+1}, 0, 2^{k+1}), (0, 2^{k+1}, 0, -2^{k+1}), (0, -2^{k+1}, 0, 2^{k+1}), (0, -2^{k+1}, 0, -2^{k+1})$$
$$(2^{k+1}, 0, 2^{k+1}, 0), (2^{k+1}, 0, -2^{k+1}, 0, (-2^{k+1}, 0, 2^{k+1}, 0), (-2^{k+1}, 0, -2^{k+1}, 0).$$

Thus, the solutions (X, Y, W, Z) to (23) and (24) are

$$(0, \sqrt{2}, 0, \sqrt{2}), (0, \sqrt{2}, 0, -\sqrt{2}), (0, -\sqrt{2}, 0, \sqrt{2}), (0, -\sqrt{2}, 0, -\sqrt{2}),$$
$$(\sqrt{2}, 0, \sqrt{2}, 0), (\sqrt{2}, 0, -\sqrt{2}, 0), (-\sqrt{2}, 0, \sqrt{2}, 0), (-\sqrt{2}, 0, -\sqrt{2}, 0),$$

which also satisfy condition $(**)$. The converse is immediate, and (ii) is shown. □

Example 20 A set of Boolean functions is called a *bent set* if the sum of any two different elements of the set is a bent function. Proposition 1 of [1] shows the existence of a bent set (based on a vectorial bent function $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$) of cardinality 2^k, namely $\{F_v : \mathbb{F}_2^n \to \mathbb{F}_2, F_v(\mathbf{x}) = \mathbf{v} \cdot F(\mathbf{x})\}$, which is also closed under addition. Taking any such bent set of cardinality ≥ 4, say $S = \{f_0, f_1, f_2, f_3, \ldots\}$, define $a_0 = f_0 \oplus f_1, a_1 = f_0 \oplus f_2, a_2 = f_0 \oplus f_3$, which satisfy the conditions of Theorem 19(a), because S is a bent set closed under addition.

Example 21 Let $n = 2t$. A polynomial $F(X) \in \mathbb{F}_{2^t}[X]$ is said to be a complete mapping polynomial if $F(X)$ and $F(X) + X$ both correspond to permutations on $\mathbb{F}_{2^t}$; let us denote the permutation corresponding to $F(X)$ by π_F. We establish an isomorphism between $\mathbb{F}_{2^t}$ and $\mathbb{F}_2^t$ and consider the permutation π_F as a mapping from $\mathbb{F}_2^t$ to $\mathbb{F}_2^t$. Let a_0, a_1 and a_2 be defined as follows:

$a_0(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^t$,
$a_1(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^t$,
$a_2(\mathbf{x}, \mathbf{y}) = \pi_F(\mathbf{x}) \cdot \mathbf{y}$ for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^t$.

Since π_F is associated to a complete mapping polynomial all the functions $a_2, a_0 \oplus a_2, a_1 \oplus a_2$ and $a_0 \oplus a_1 \oplus a_2$ are Maiorana–McFarland type bent functions. Further, $W_{a_0 \oplus a_2}(\mathbf{u}, \mathbf{v}) = W_{a_1 \oplus a_2}(\mathbf{u}, \mathbf{v})$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^t$, which implies that $W_{a_0 \oplus a_2}(\mathbf{u}, \mathbf{v}) W_{a_1 \oplus a_2}(\mathbf{u}, \mathbf{v}) = 2^n$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^t$, whereas $a_0 \oplus a_1 \oplus a_2 = a_2$ implies that $W_{a_2}(\mathbf{u}, \mathbf{v}) W_{a_0 \oplus a_1 \oplus a_2}(\mathbf{u}, \mathbf{v}) = 2^n$ all $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^t$. Thus, we obtain bent functions a_0, a_1 and a_2 which satisfy the conditions of Theorem 19 for the even case. For details on complete mapping polynomials we refer to [11].

8 Constructions of generalized bent functions in $\mathcal{GB}_n^8$

In this section we characterize and define several classes of gbent Boolean functions.

Theorem 22 *If $f : \mathbb{Z}_2^{n+2} \to \mathbb{Z}_8$ (n even) is given by*

$$f(\mathbf{x}, y, z) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 2c(\mathbf{x}) + 1)y + (4b(\mathbf{x}) + 2c(\mathbf{x}) + 1)z - 2yz,$$

where $a, b, c \in \mathcal{B}_n$ such that all a, b, c, $a \oplus c$, $b \oplus c$ and $a \oplus b$ are bent satisfying

$$W_a(\mathbf{x})W_b(\mathbf{x}) + W_{a\oplus c}(\mathbf{x})W_{b\oplus c}(\mathbf{x}) = -2W_{a\oplus b}(\mathbf{x})W_c(\mathbf{x})), \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{30}$$

then f is gbent in $\mathcal{GB}_{n+2}^8$.

Proof We compute the Walsh–Hadamard coefficients (using that $\zeta = \frac{1}{\sqrt{2}}(1+\imath)$ and $\zeta^2 = \imath$)

$$\begin{aligned}
2^{(n+2)/2}\mathcal{H}_f(\mathbf{u}, v, w) &= \sum_{(\mathbf{x},y,z)\in\mathbb{Z}_2^{n+2}} \zeta^{f(\mathbf{x},y,z)}(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus vy\oplus wz} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{4c(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{(y,z)\in\mathbb{Z}_2^2} \zeta^{(4a(\mathbf{x})+2c(\mathbf{x})+1)y+(4b(\mathbf{x})+2c(\mathbf{x})+1)z-2yz}(-1)^{vy\oplus wz} \\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{c(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \Big(1 + (-1)^v(-1)^{a(\mathbf{x})}\imath^{c(\mathbf{x})}\zeta + (-1)^w(-1)^{b(\mathbf{x})}\imath^{c(\mathbf{x})}\zeta \\
&\quad + (-1)^{a(\mathbf{x})\oplus b(\mathbf{x})\oplus c(\mathbf{x})\oplus v\oplus w}\Big).
\end{aligned}$$

Applying Eq. 3 with $(z, s) = (\imath, c(\mathbf{x}))$, that is, $i^{c(\mathbf{x})} = \frac{1+(-1)^{c(\mathbf{x})}}{2} + \frac{1-(-1)^{c(\mathbf{x})}}{2}\imath$, we obtain

$$\begin{aligned}
2\mathcal{H}_f(\mathbf{u}, v, w) &= W_c(\mathbf{u}) + \frac{(-1)^v\zeta}{2}\left(W_{a\oplus c}(\mathbf{u}) + W_a(\mathbf{u}) + \imath W_{a\oplus c}(\mathbf{u}) - \imath W_a(\mathbf{u})\right) \\
&\quad + \frac{(-1)^w\zeta}{2}\left(W_{b\oplus c}(\mathbf{u}) + W_b(\mathbf{u}) + \imath W_{b\oplus c}(\mathbf{u}) - \imath W_b(\mathbf{u})\right) + (-1)^{v\oplus w}W_{a\oplus b}(\mathbf{u}) \\
&= W_c(\mathbf{u}) + \frac{(-1)^v}{\sqrt{2}}(W_a(\mathbf{u}) + \imath W_{a\oplus c}(\mathbf{u})) + \frac{(-1)^w}{\sqrt{2}}(W_b(\mathbf{u}) + \imath W_{b\oplus c}(\mathbf{u})) \\
&\quad + (-1)^{v\oplus w}W_{a\oplus b}(\mathbf{u}).
\end{aligned}$$

Therefore, the real and the imaginary parts of $\mathcal{H}_f(\mathbf{u}, v, w)$ are

$$\begin{aligned}
Re(\mathcal{H}_f(\mathbf{u}, v, w)) &= W_c(\mathbf{u}) + (-1)^{v\oplus w}W_{a\oplus b}(\mathbf{u}) + \frac{(-1)^v W_a(\mathbf{u}) + (-1)^w W_b(\mathbf{u})}{\sqrt{2}}, \\
Im(\mathcal{H}_f(\mathbf{u}, v, w)) &= \frac{(-1)^v W_{a\oplus c}(\mathbf{u}) + (-1)^w W_{b\oplus c}(\mathbf{u})}{\sqrt{2}}.
\end{aligned}$$

and so,

$$\begin{aligned}
4|\mathcal{H}_f(\mathbf{u}, v, w)|^2 &= \frac{1}{2}\big(W_a(\mathbf{u})^2 + W_b(\mathbf{u})^2 + W_{a\oplus c}(\mathbf{u})^2 + W_{b\oplus c}(\mathbf{u})^2 \\
&\quad + 2W_c(\mathbf{u})^2 + 2W_{a\oplus b}(\mathbf{u})^2\big) \\
&\quad + (-1)^{v+w}(W_a(\mathbf{u})W_b(\mathbf{u}) + W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + 2W_c(\mathbf{u})W_{a\oplus b}(\mathbf{u})) \\
&\quad + \sqrt{2}\big((-1)^v(W_a(\mathbf{u})W_c(\mathbf{u}) + W_b(\mathbf{u})W_{a\oplus b}(\mathbf{u})) + (-1)^w(W_b(\mathbf{u})W_c(\mathbf{u}) \\
&\quad + W_a(\mathbf{u})W_{a\oplus b}(\mathbf{u}))\big)
\end{aligned} \tag{31}$$

Since $a, b, c, a \oplus c, b \oplus c, a \oplus b$ are all bent then $|W_a(\mathbf{u})| = |W_b(\mathbf{u})| = |W_c(\mathbf{u})| = |W_{a\oplus b}(\mathbf{u})| = |W_{a\oplus c}(\mathbf{u})| = |W_{b\oplus c}(\mathbf{u})| = 1$. Further, from the imposed conditions on these functions' Walsh–Hadamard coefficients, we see that $W_a(\mathbf{u})W_b(\mathbf{u}) + W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) +$

$2W_c(\mathbf{u})W_{a\oplus b}(\mathbf{u}) = 0$, and also $W_a(\mathbf{u})W_c(\mathbf{u}) + W_b(\mathbf{u})W_{a\oplus b}(\mathbf{u}) = 0$, $W_b(\mathbf{u})W_c(\mathbf{u}) + W_a(\mathbf{u})W_{a\oplus b}(\mathbf{u}) = 0$ (that is because if $W_a(\mathbf{u})$ and $W_b(\mathbf{u})$ have the same sign, then $W_c(\mathbf{u})$, $W_{a\oplus b}$ have opposite signs; further, $W_a(\mathbf{u})$ and $W_b(\mathbf{u})$ have opposite signs, then $W_c(\mathbf{u})$, $W_{a\oplus b}$ have the same sign). Using these equations, we get that $4|\mathcal{H}_f(\mathbf{u}, v, w)|^2 = 4$, and so, f is gbent.

□

Remark 23 It is rather straightforward to see that condition (30) has 16 solutions. More precisely, $(W_a(\mathbf{x}), W_b(\mathbf{x}), W_{a\oplus c}(\mathbf{x}), W_{b\oplus c}, W_{a\oplus b}(\mathbf{x}), W_c(\mathbf{x}))$ could be any of the following tuples:

$(-1,-1,-1,-1,-1,1)$; $(-1,-1,-1,-1,1,-1)$; $(-1,1,1,1,-1,1)$; $(-1,-1,1,1,1,-1)$;
$(-1,1,-1,1,-1,-1)$; $(-1,1,-1,1,1,1)$; $(-1,1,1,-1,1,-1)$; $(-1,1,1,-1,1,1)$;
$(1,-1,-1,1,-1,-1)$; $(1,-1,-1,1,1,1)$; $(1,-1,1,-1,1,-1)$; $(1,-1,1,-1,1,1)$;
$(1,1,-1,-1,-1,1)$; $(1,1,-1,-1,1,-1)$; $(1,1,1,1,-1,1)$; $(1,1,1,1,1,-1)$.

Theorem 24 *If $f : \mathbb{Z}_2^{n+2} \to \mathbb{Z}_8$ (n even) is given by*

$$f^\epsilon(\mathbf{x}, y, z) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 1)y + (4b(\mathbf{x}) + 1)z + 2\epsilon yz, \tag{32}$$

where $\epsilon \in \{1, -1\}$, $a, b, c \in \mathcal{B}_n$ such that all c, $a \oplus c$, $b \oplus c$ and $a \oplus b \oplus c$ are bent, with

$$W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + \epsilon W_c(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}) = 0, \text{ for all } \mathbf{u} \in \mathbb{Z}_2^n, \tag{33}$$

then f is gbent in $\mathcal{GB}_{n+2}^8$.

Proof As in the proof of Theorem 22, we compute the Walsh–Hadamard coefficients, obtaining

$$\begin{aligned}
&2\mathcal{H}_{f^\epsilon}(\mathbf{u}, v, w)\\
&= W_c(\mathbf{u}) + (-1)^v \zeta W_{a\oplus c}(\mathbf{u}) + (-1)^w \zeta W_{b\oplus c}(\mathbf{u}) + (-1)^{v\oplus w}\zeta^{2+2\epsilon} W_{a\oplus b\oplus c}(\mathbf{u})\\
&= W_c(\mathbf{u}) - \epsilon(-1)^{v\oplus w} W_{a\oplus b\oplus c}(\mathbf{u}) + \frac{(-1)^v W_{a\oplus c}(\mathbf{u}) + (-1)^w W_{b\oplus c}(\mathbf{u})}{\sqrt{2}}\\
&+ \imath \frac{(-1)^v W_{a\oplus c}(\mathbf{u}) + (-1)^w W_{b\oplus c}(\mathbf{u})}{\sqrt{2}},
\end{aligned}$$

using the fact that $\zeta^{2+2\epsilon} = -\epsilon$, for $\epsilon \in \{1, -1\}$. Taking the square of the complex norm, we get

$$\begin{aligned}
4|\mathcal{H}_{f^\epsilon}(\mathbf{u}, v, w)|^2 = {} & W_{a\oplus c}(\mathbf{u})^2 + W_{b\oplus c}(\mathbf{u})^2 + W_c(\mathbf{u})^2 + W_{a\oplus b\oplus c}(\mathbf{u})^2\\
&+2(-1)^{v+w}\left(W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + \epsilon W_c(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u})\right)\\
&+\sqrt{2}\left((-1)^v(W_{a\oplus c}(\mathbf{u})W_c(\mathbf{u}) + \epsilon W_{b\oplus c}(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}))\right.\\
&\left.+(-1)^w(W_{b\oplus c}(\mathbf{u})W_c(\mathbf{u}) + \epsilon W_{a\oplus c}(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}))\right) = 4,
\end{aligned}$$

because $c, a\oplus c, b\oplus c$ and $a\oplus b\oplus c$ are all bent, so their Walsh–Hadamard coefficients are 1 in absolute values, and Eq. 33 implies that the remaining coefficients are all 0 (that can be seen by the following argument: if $A, B, C, D \in \{\pm 1\}$, and $AB + CD = 0$, then by multiplying by BC, we get $AC + BD = 0$, and by multiplying by AC we get $BC + AD = 0$).

Therefore, $|\mathcal{H}_{f^\epsilon}(\mathbf{u}, v, w)|^2 = 1$, so f is gbent, and the theorem is proved. □

Remark 25 The Eq. 33 has 8 solutions (as expected, since there are four degrees of freedom and one constraint). Moreover, one can give plenty of concrete examples of functions a, b, c

satisfying the conditions of our theorem. For example, if $\epsilon = -1$, one could take in Eq. 32, a bent Boolean c, and $a = b$ such that $c \oplus a$ is bent (for instance, if $a = b$ are affine functions, that condition is immediate). Then, $W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + \epsilon W_c(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}) = W_{c\oplus a}(\mathbf{u})^2 - W_c(\mathbf{u})^2 = 0$, and so, g as in our theorem is gbent.

Theorem 26 *Let $f : \mathbb{Z}_2^{n+1} \to \mathbb{Z}_8$ (n is even) be given by*

$$f(\mathbf{x}, y) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 4c(\mathbf{x}) + 2\epsilon)y, \tag{34}$$

where $\epsilon \in \{1, -1\}$. Then f is gbent in $\mathcal{GB}_{n+1}^8$ if and only if a, c are bent in $\mathcal{B}_n$. Moreover, if g is given by

$$g(\mathbf{x}, y) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 2c(\mathbf{x}) + 2\epsilon)y, \tag{35}$$

where $\epsilon \in \{1, -1\}$, $a, c \in \mathcal{B}_n$ such that $a, c, a \oplus c$ are all bent, then g is gbent in $\mathcal{GB}_{n+1}^8$. Further, let h be given by

$$h(\mathbf{x}, y) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 2\epsilon)y, \tag{36}$$

where $\epsilon \in \{1, -1\}$. Then h is gbent in $\mathcal{GB}_{n+1}^8$ if and only if $c, a \oplus c$ are bent in $\mathcal{B}_n$.

Proof We will show the first claim, since the proof of the remaining ones are absolutely similar. As in the proof of Theorem 22, the Walsh–Hadamard coefficients at an arbitrary input $(\mathbf{u}, v)$ are

$$\sqrt{2}\mathcal{H}_f(\mathbf{u}, v) = W_c(\mathbf{u}) + \imath^{\epsilon}(-1)^v W_a(\mathbf{u}) = W_c(\mathbf{u}) + \epsilon\,\imath(-1)^v W_a(\mathbf{u}),$$

and so,

$$2|\mathcal{H}_f(\mathbf{u}, v)|^2 = W_c(\mathbf{u})^2 + W_a(\mathbf{u})^2.$$

If a, c are bent, then $|W_c(\mathbf{u})| = |W_a(\mathbf{u})| = 1$, and so $|\mathcal{H}_f(\mathbf{u}, v)| = 1$, that is f is gbent. If f is gbent, then the equation $W_c(\mathbf{u})^2 + W_a(\mathbf{u})^2 = 2$ has as rational solutions only $|W_c(\mathbf{u})| = |W_a(\mathbf{u})| = 1$, and so, a, c are bent. □

Acknowledgement We gratefully thank the reviewers for the detailed and excellent comments, which improved the quality of the paper.

References

1. Bey C., Kyureghyan G.M.: On Boolean functions with the sum of every two of them being bent. Des. Codes Cryptogr. **49**, 341–346 (2008).
2. Carlet C.: Generalized partial spreads. IEEE Trans. Inf. Theory **41**, 1482–1487 (1995).
3. Carlet C., Guillot P.: A characterization of binary bent functions. J. Comb. Theory (A) **76**(2), 328–335 (1996).
4. Carlet C., Guillot P.: An alternate characterization of the bentness of binary functions, with uniqueness. Des. Codes Cryptogr. **14**(2), 133–140 (1998).
5. Carlet C.: Boolean functions for cryptography and error correcting codes. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010).
6. Carlet C.: Vectorial Boolean functions for cryptography. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398–469. Cambridge University Press, Cambridge (2010).
7. Cusick T.W., Stănică P.: Cryptographic Boolean Functions and Applications. Elsevier, Amsterdam (2009).
8. Dillon J.F.: Elementary Hadamard difference sets. In: Proceedings of the Sixth S.E. Conference of Combinatorics, Graph Theory, and Computing, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, pp. 237–249 (1975).

9. Hirschhorn M.D.: A simple proof of Jacobi's four-square theorem. Proc. Am. Math. Soc. **101**, 436–438 (1987).
10. Kumar P.V., Scholtz R.A., Welch L.R.: Generalized bent functions and their properties. J. Comb. Theory (A) **40**, 90–107 (1985).
11. Laigle-Chapuy Y.: Permutation polynomials and applications to coding theory. Finite Fields Appl. **13**, 58–70 (2007).
12. Lam T.Y., Leung K.H.: On vanishing sums of roots of unity. J. Algebra **224**(1), 91–109 (2000).
13. Rothaus O.S.: On bent functions. J. Comb. Theory Ser. A **20**, 300–305 (1976).
14. Sarkar P., Maitra S.: Cross-correlation analysis of cryptographically useful Boolean functions and S-boxes. Theory Comput. Syst. **35**, 39–57 (2002).
15. Schmidt K.-U.: Quaternary constant-amplitude codes for multicode CDMA. In: IEEE International Symposium on Information Theory, ISIT'2007, Nice, France, June 24–29, 2007, pp. 2781–2785. Available at http://arxiv.org/abs/cs.IT/0611162.
16. Solé P., Tokareva N.: Connections Between Quaternary and Binary Bent Functions. http://eprint.iacr.org/2009/544.pdf; see also, Prikl. Diskr. Mat. 1, 16–18 (2009).
17. Stănică P., Gangopadhyay S., Chaturvedi A., Kar Gangopadhyay A., Maitra S.: Nega-Hadamard transform, bent and negabent functions. In: Carlet C., Pott A. (eds.) Sequences and Their Applications—SETA 2010, LNCS 6338, 359–372 (2010).
18. Stănică P., Gangopadhyay S., Singh B.K.: Some Results Concerning Generalized Bent Functions. http://eprint.iacr.org/2011/290.pdf.
19. Stănică P., Martinsen T.: Octal Bent Generalized Boolean Functions. http://eprint.iacr.org/2011/089.pdf.
20. Zhao Y., Li H.: On bent functions with some symmetric properties. Discret. Appl. Math. **154**, 2537–2543 (2006).