Generalized Bent Functions and Their Gray Images

Thor Martinsen[1], Wilfried Meidl[2], and Pantelimon Stănică[1](✉)

[1] Department of Applied Mathematics, Naval Postgraduate School,
Monterey, CA 93943–5216, USA
{tmartins,pstanica}@nps.edu
[2] Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040 Linz, Austria
meidlwilfried@gmail.com

Abstract. In this paper we prove that generalized bent (gbent) functions defined on $\mathbb{F}_2^n$ with values in $\mathbb{Z}_{2^k}$ are regular, and show connections between the (generalized) Walsh spectrum of these functions and their components. Moreover we analyze generalized bent and semibent functions with values in $\mathbb{Z}_{16}$ in detail, extending earlier results on gbent functions with values in $\mathbb{Z}_4$ and $\mathbb{Z}_8$.

1 Introduction

Let $\mathbb{V}_n$ be an n-dimensional vector space over $\mathbb{F}_2$ and for an integer q, let $\mathbb{Z}_q$ be the ring of integers modulo q. For a *generalized Boolean function* f from $\mathbb{V}_n$ to $\mathbb{Z}_q$ the *generalized Walsh-Hadamard transform* is the complex valued function

$$\mathcal{H}_f^{(q)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_q^{f(\mathbf{x})}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle}, \quad \zeta_q = e^{\frac{2\pi i}{q}},$$

where $\langle \mathbf{u},\mathbf{x}\rangle$ denotes a (nondegenerate) inner product on $\mathbb{V}_n$ (we shall use ζ, $\mathcal{H}_f$, instead of ζ_q, respectively, $\mathcal{H}_f^{(q)}$, when q is fixed). Throughout, we identify $\mathbb{V}_n$ with the vector space $\mathbb{F}_2^n$ of n-tuples over $\mathbb{F}_2$, and we use the regular scalar (inner) product $\langle \mathbf{u},\mathbf{x}\rangle = \mathbf{u}\cdot\mathbf{x}$. We denote the set of all generalized Boolean functions by $\mathcal{GB}_n^q$ and when $q=2$, by $\mathcal{B}_n$.

We recall that for $q=2$, where the generalized Walsh-Hadamard transform of f reduces to the conventional *Walsh-Hadamard transform*

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} (-1)^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}},$$

a function f for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u}\in\mathbb{V}_n$ is called a *bent* function. Similarly, we say that function $f : \mathbb{V}_n \to \mathbb{Z}_q$ is a *generalized bent* (*gbent*) if

---

S. Duquesne and S. Petkova-Nikova (Eds.): WAIFI 2016, LNCS 10064, pp. 160–173, 2016.
DOI: 10.1007/978-3-319-55227-9_12

$|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$. Further recall that $f \in \mathcal{B}_n$ is called *plateaued* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$ for a fixed integer s depending on f (we also call f then *s-plateaued*). If $s = 1$ (n must then be odd), or $s = 2$ (n must then be even), we call f semibent. With this notation, a semibent function is an s-plateaued Boolean function with smallest possible $s > 0$. Accordingly we call a function $f \in \mathcal{GB}_n^q$, with $q = 2^k$, $k > 1$, *generalized semibent* (*gsemibent*, for short) if $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{(n+1)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$, and more general, *generalized s-plateaued* if $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$.

Let $f : \mathbb{V}_m \to \mathbb{Z}_q$. If $2^{k-1} < q \leq 2^k$, we associate a unique sequence of Boolean functions $a_i : \mathbb{V}_m \to \mathbb{F}_2$, $1 \leq i \leq k$, such that (the addition below is in $\mathbb{Z}_q$)

$$f(\mathbf{x}) = a_1(\mathbf{x}) + \cdots + 2^{k-1} a_k(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{V}_m.$$

If $q = 2^k$, following Carlet [1], we further define the *generalized Gray map* $\psi(f) : \mathcal{GB}_n^q \to \mathcal{B}_{n+k-1}$ by $\psi(f)(\mathbf{x}, y_1, \ldots, y_{k-1}) = \bigoplus_{i=1}^{k-1} a_i(\mathbf{x}) y_i \oplus a_k(\mathbf{x})$.

Generalized bent functions were introduced in [7] in connection with applications in CDMA systems, and lately have attracted increasing attention, see e.g. [2,3,8,9].

In [8,9] gbent functions $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x})$ in $\mathcal{GB}_n^4$ and $f = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x})$ in $\mathcal{GB}_n^8$ were completely characterized in terms of properties of the Boolean functions $a_i(\mathbf{x})$. In particular, relations between gbentness of f and bentness of associated Boolean functions have been investigated. In [9] it was moreover shown that $f \in \mathcal{GB}_n^4$, with $f(\mathbf{x}) = a_1 + 2a_2(\mathbf{x})$, $a_1, a_2 \in \mathcal{B}_n$, is gbent if and only if the Gray image $\psi(f)$ is bent if n is odd, or semibent and the associated a_2 and $a_1 \oplus a_2$ have complementary autocorrelation if n is even (see [9] for the details). Currently one observes a lot of research activities on gbent functions for general k, and we expect that many more general results will be discovered in the near future. Our generalizations in Sect. 2, where we analyze gbent functions in terms of their components, are some first results. In particular we show that a gbent function in even dimension is an affine space of bent functions and we decompose a gbent function in $\mathcal{GB}_n^{2^k}$ into two gbent functions in $\mathcal{GB}_n^{2^{k-1}}$. In Sect. 3 we analyze gbent functions in $\mathcal{GB}_n^{16}$ in detail.

2 Gbent Functions and Their Components

In accordance with the terminology for bent functions, we call a gbent function $f \in \mathcal{GB}_n^q$ *regular*, if $\mathcal{H}_f(\mathbf{u}) = 2^{n/2} \zeta_q^{f^*(\mathbf{u})}$ for some function $f^* \in \mathcal{GB}_n^q$. We start with a theorem about the regularity of gbent functions, which is also of independent interest. We prove the result by modifying a method of Kumar et al. [6].

Theorem 1. *All gbent functions $f \in \mathcal{GB}_n^{2^k}$ are regular, except for n odd and $k = 2$, in which case we have $\mathcal{H}_f^4(\mathbf{u}) = 2^{\frac{n-1}{2}}(\pm 1 \pm i)$.*

Proof. If $k = 1$, the result is known, as we are dealing with classical bent functions. Let $k \geq 2$. Let $\zeta = e^{\frac{2\pi i}{2^k}}$ be a 2^k-primitive root of unity. It is known that

$\mathbb{Z}[\zeta]$ is the ring of algebraic integers in the cyclotomic field $\mathbb{Q}(\zeta)$. We recall some facts from [6] (we change the notations slightly). The decomposition for the ideal generated by 2 in $\mathbb{Z}[\zeta]$ has the form $\langle 2\rangle = P^{2^{k-1}}$, where $P = \langle 1-\zeta\rangle$ is a prime ideal in $\mathbb{Z}[\zeta]$. The decomposition group

$$G_2 = \{\sigma \text{ in the Galois group of } \mathbb{Q}(\zeta)/\mathbb{Q} \mid \sigma(P) = P\}$$

contains also the conjugation isomorphism $\sigma^*(z) = z^{-1}$ (Proposition 2 in [6]). Observe that $\mathcal{H}_f^{(2^k)}(\mathbf{u})\overline{\mathcal{H}_f^{(2^k)}(\mathbf{u})} = 2^n$. Now, as in Property 7 of [6], observing that our generalized Walsh transform is simply $S(f, 2^{k-1}\mathbf{u})$ (in the notations of Kumar et al. [6]; $\mathbf{u}$ is a binary vector in our case), then $\mathcal{H}_f^{(2^k)}(\mathbf{u})$ and $\overline{\mathcal{H}_f^{(2^k)}(\mathbf{u})}$ will generate the same ideal in $\mathbb{Z}[\zeta]$ and so, $2^{-n}(\mathcal{H}_f^{(2^k)}(\mathbf{u}))^2$ is a unit, and consequently, $2^{-n/2}\mathcal{H}_f^{(2^k)}(\mathbf{u})$ is an algebraic integer. Therefore, by Proposition 1 of [6] (which, in fact, is an old result of Kronecker from 1857), $2^{-n/2}\mathcal{H}_f^{(2^k)}(\mathbf{u})$ must be a root of unity. That alone would still not be enough to show regularity since this root of unity may be in a cyclotomic field outside $\mathbb{Q}(\zeta)$, however, that is not the case here, since the Gauss quadratic sum $G(2^k) = \sum_{i=0}^{2^k-1} \zeta^{i^2} = 2^{k/2}(1+i)$ and so, $\sqrt{2} \in \mathbb{Q}(\zeta)$, unless $k = 2$ (since then $1 + i \notin \mathbb{Q}(\zeta)$). The first assertion is shown for n even, as well as for n odd with $k \geq 3$.

When n is odd and $k = 2$, then $\mathcal{H}_f^{(4)}(\mathbf{u}) = \sum_{\mathbf{u}\in\mathbb{V}_n} i^{f(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = a + bi$, for some integers a, b. Since f is gbent, with $|\mathcal{H}_f^{(4)}(\mathbf{u})|^2 = 2^n$ we get the diophantine equation $a^2 + b^2 = 2^n$. If n is even, the only solutions are $(a, b) = (\pm 2^{n/2}, 0)$, or $(0, \pm 2^{n/2})$. If n is odd, the solutions are $(a, b) = (\pm 2^{\lfloor n/2\rfloor}, \pm 2^{\lfloor n/2\rfloor})$ (independent choices of signs). The theorem is shown.

From the definition of a Boolean bent function via the Walsh-Hadamard transform we immediately obtain the following equivalent definition, where we denote the support of a Boolean function f by $\mathrm{supp}(f) := \{\mathbf{x} \in \mathbb{V}_n \ : \ f(\mathbf{x}) = 1\}$: A Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is bent if and only if for every $\mathbf{u} \in \mathbb{V}_n$ the function $f_{\mathbf{u}}(\mathbf{x}) := f(\mathbf{x}) \oplus \mathbf{u}\cdot\mathbf{x}$ satisfies $|\mathrm{supp}(f_{\mathbf{u}})| = 2^{n-1} \pm 2^{n/2}$. Our next target is to show an analog description for gbent functions. We use the following lemma.

Lemma 1. *Let* $q = 2^k$, $k > 1$, $\zeta = e^{2\pi i/q}$. *If* $\rho_l \in \mathbb{Q}$, $0 \leq l \leq q-1$ *and* $\sum_{l=0}^{q-1} \rho_l \zeta^l = r$ *is rational, then* $\rho_j = \rho_{2^{k-1}+j}$, *for* $1 \leq j \leq 2^{k-1} - 1$.

Proof. Since $\zeta^{2^{k-1}+l} = -\zeta^l$ for $0 \leq l \leq 2^{k-1} - 1$, we can write every element z of the cyclotomic field $\mathbb{Q}(\zeta)$ as

$$z = \sum_{l=0}^{2^{k-1}-1} \lambda_l \zeta^l,\ \lambda_l \in \mathbb{Q}, 0 \leq l \leq 2^{k-1} - 1.$$

As $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(q) = 2^{k-1}$ (φ is Euler's totient function), the set $\{1, \zeta, \ldots, \zeta^{2^{k-1}-1}\}$ is a basis of $\mathbb{Q}(\zeta)$. Since

$$0 = \sum_{l=0}^{q-1} \rho_l \zeta^l - r = (\rho_0 - \rho_{2^{k-1}} - r) + \sum_{l=1}^{2^{k-1}-1} (\rho_j - \rho_{2^{k-1}+j})\zeta^l,$$

the assertion of the lemma follows.

Proposition 1. *Let* $n = 2m$ *be even, and for a function* $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ *and* $\mathbf{u} \in \mathbb{V}_n$*, let* $f_{\mathbf{u}}(\mathbf{x}) = f(\mathbf{x}) + 2^{k-1}(\mathbf{u} \cdot \mathbf{x})$*, and let* $b_j^{(\mathbf{u})} = |\mathbf{x} \in \mathbb{V}_n \ :\ f_{\mathbf{u}}(\mathbf{x}) = j\}|$*,* $0 \le j \le 2^k - 1$*. Then* f *is gbent if and only if for all* $\mathbf{u} \in \mathbb{V}_n$ *there exists an integer* $\rho_{\mathbf{u}}$*,* $0 \le \rho_{\mathbf{u}} \le 2^{k-1} - 1$*, such that*

$$b^{(\mathbf{u})}_{2^{k-1}+\rho_{\mathbf{u}}} = b^{(\mathbf{u})}_{\rho_{\mathbf{u}}} \pm 2^m \text{ and } b^{(\mathbf{u})}_{2^{k-1}+j} = b^{(\mathbf{u})}_j, \text{ for } 0 \le j \le 2^{k-1} - 1, j \ne \rho_{\mathbf{u}}.$$

Proof. First suppose that f is gbent. Then by Theorem 1, f is a regular gbent function. Hence

$$\mathcal{H}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x})+2^{k-1}(\mathbf{u}\cdot\mathbf{x})} = \mathcal{H}_{f_{\mathbf{u}}}(0) = \sum_{j=0}^{2^k-1} b_j^{(\mathbf{u})}\zeta^j = 2^m\zeta^r$$

for some $0 \le r \le 2^k - 1$. With $\rho_{\mathbf{u}} = r$ if $0 \le r \le 2^{k-1} - 1$, and $\rho_{\mathbf{u}} = r - 2^{k-1}$ otherwise, the claim follows from Lemma 1.

The converse statement is verified in a straightforward manner.

We now can present connections between gbent functions and their components for the general case of gbent functions in $\mathcal{GB}_n^{2^k}$, $k > 1$. This generalizes the corresponding results for $k = 2$ and $k = 3$ in [8] and in [9].

Theorem 2. *Let* n *be even, and let* $f(\mathbf{x})$ *be a gbent function in* $\mathcal{GB}_n^{2^k}$*,* $k > 1$*, (uniquely) given as*

$$f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) + 2^{k-1}a_k(\mathbf{x}),$$

$a_i \in \mathcal{B}_n$*,* $1 \le i \le k$*. Then all Boolean functions of the form*

$$g_{\mathbf{c}}(\mathbf{x}) = c_1a_1(\mathbf{x}) \oplus c_2a_2(\mathbf{x}) \oplus \cdots \oplus c_{k-1}a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x}),$$

$\mathbf{c} = (c_1, c_2, \ldots, c_{k-1}) \in \mathbb{F}_2^{k-1}$*, are bent functions.*

Proof. As in Proposition 1, for the gbent function f we denote by $f_{\mathbf{u}}$ the function $f_{\mathbf{u}}(\mathbf{x}) = a_1(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) + 2^{k-1}(a_k(\mathbf{x}) + \mathbf{u}\cdot\mathbf{x})$ in $\mathcal{GB}_n^{2^k}$. Again, the integer $b_r^{(\mathbf{u})}$, $0 \le r \le 2^k - 1$, is defined as $b_r^{(\mathbf{u})} = |\{\mathbf{x} \in \mathbb{V}_n \ :\ f_{\mathbf{u}}(\mathbf{x}) = r\}|$. By Proposition 1, $b^{(\mathbf{u})}_{r+2^{k-1}} = b_r^{(\mathbf{u})}$ for all $0 \le r \le 2^{k-1} - 1$, except for one element $\rho_{\mathbf{u}} \in \{0, \ldots, 2^{k-1} - 1\}$ depending on $\mathbf{u}$, for which $b^{(\mathbf{u})}_{\rho_{\mathbf{u}}+2^{k-1}} = b^{(\mathbf{u})}_{\rho_{\mathbf{u}}} \pm 2^{n/2}$.

Since it is somewhat easier to follow, we first show the bentness of $a_k(\mathbf{x}) = g_{\mathbf{0}}(\mathbf{x})$. In the second step we show the general case.

For $r \neq \rho_{\mathbf{u}}$, $0 \leq r \leq 2^{k-1} - 1$, consider all $\mathbf{x} \in \mathbb{V}_n$ for which $a_1(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) = r$. Since $b^{(\mathbf{u})}_{r+2^{k-1}} = b^{(\mathbf{u})}_r$, for exactly half of these $\mathbf{x}$ we have $a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x} = 0$ (note that the number of these $\mathbf{x}$ must be even). Among all $\mathbf{x} \in \mathbb{V}_n$ for which $a_1(\mathbf{x}) + \cdots + 2^{k-2}a_{k-1}(\mathbf{x}) = \rho_{\mathbf{u}}$, there are $b^{(\mathbf{u})}_{\rho_u}$ for which $a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x} = 0$, and there are $b^{(\mathbf{u})}_{\rho_{\mathbf{u}}+2^{k-1}} = b^{(\mathbf{u})}_{\rho_u} \pm 2^{n/2}$ for which $a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x} = 1$. Hence for the Walsh-Hadamard transform of a_k we get

$$\mathcal{W}_{a_k}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}} = \pm 2^{n/2},$$

which shows that a_k is bent.

To show that $g_{\mathbf{c}}$ is bent for every $\mathbf{c} \in \mathbb{F}_2^{k-1}$, we write $f_{\mathbf{u}}(\mathbf{x})$, $\mathbf{u} \in \mathbb{V}_n$, as

$$\begin{aligned} f_{\mathbf{u}}(\mathbf{x}) &= c_1 a_1(\mathbf{x}) + \cdots + c_{k-1}2^{k-2}a_{k-1}(\mathbf{x}) \ + \ \bar{c}_1 a_1(\mathbf{x}) + \cdots + \bar{c}_{k-1}2^{k-2}a_{k-1}(\mathbf{x}) \\ &\quad + 2^{k-1}(a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}) := h(\mathbf{x}) + \bar{h}(\mathbf{x}) + 2^{k-1}(a_k(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}), \end{aligned}$$

where $\bar{c} = c \oplus 1$. Note that every $0 \leq r \leq 2^{k-1} - 1$ in the value set of $a_1(x) + \cdots + 2^{k-2}a_{k-2}(\mathbf{x})$ has then a unique representation as $h(\mathbf{x}) + \bar{h}(\mathbf{x})$. Consider $\mathbf{x}$ for which $h(\mathbf{x}) + \bar{h}(\mathbf{x}) = r + s \neq \rho_{\mathbf{u}}$. Again from $b^{(\mathbf{u})}_{r+2^{k-1}} = b^{(\mathbf{u})}_r$ we infer that for half of those $\mathbf{x}$ we have $a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 0$. Hence also

$$g_{\mathbf{c}}(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = c_1 a_1(\mathbf{x}) \oplus \cdots \oplus c_{k-1}a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 0$$

for exactly half of those $\mathbf{x}$. (Observe that $h(\mathbf{x}_1) = h(\mathbf{x}_2) = r$ implies $c_1 a_1(\mathbf{x}_1) \oplus \cdots \oplus c_{k-1}a_{k-1}(\mathbf{x}_1) = c_1 a_1(\mathbf{x}_2) \oplus \cdots \oplus c_{k-1}a_{k-1}(\mathbf{x}_2)$.) Similarly as above, among all $\mathbf{x} \in \mathbb{V}_n$ for which $h(\mathbf{x}) + \bar{h}(\mathbf{x}) = \rho_{\mathbf{u}}$, there are $b^{(\mathbf{u})}_{\rho_u}$ for which $a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 0$, and there are $b^{(\mathbf{u})}_{\rho_{\mathbf{u}}+2^{k-1}} = b^{(\mathbf{u})}_{\rho_u} \pm 2^{n/2}$ for which $a_k(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x} = 1$. From this we conclude that $|\{\mathbf{x} \in \mathbb{V}_n \ : \ h(\mathbf{x}) + \bar{h}(\mathbf{x}) = \rho_u \text{ and } f_{\mathbf{u}}(\mathbf{x}) = 1\}| - |\{\mathbf{x} \in \mathbb{V}_n \ : \ h(\mathbf{x}) + \bar{h}(\mathbf{x}) = \rho_u \text{ and } f_{\mathbf{u}}(\mathbf{x}) = 0\}| = \pm 2^{n/2}$. Therefore

$$\mathcal{W}_{g_{\mathbf{c}}}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{g_{\mathbf{c}}(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} = \pm 2^{n/2},$$

and $g_{\mathbf{c}}$ is bent.

We remark that the necessary conditions in Theorem 2 are not sufficient when $k > 2$. The additional conditions on the Walsh spectra for $k = 3$ given in [9, Theorem 19] and for $k = 4$ given in our Theorem 7 are required, as one can easily confirm with examples employing vectorial Maiorana-McFarland bent functions.

The next result on the decomposition of a gbent function in $\mathcal{GB}_n^{2^k}$ into two gbent functions in $\mathcal{GB}_n^{2^{k-1}}$ reveals an inductive approach to the study of gbent functions in $\mathcal{GB}_n^{2^k}$. Note that for $k = 2$ we recover the result in [9] on the decomposition of a gbent function in $\mathcal{GB}_n^4$ into two bent functions.

Theorem 3. *Let* $f \in \mathcal{GB}_n^{2^k}$ *with* $f(\mathbf{x}) = g(\mathbf{x}) + 2h(\mathbf{x}), g \in \mathcal{B}_n, h \in \mathcal{GB}_n^{2^{k-1}}$. *If* n *is even, then the following statements are equivalent.*

(i) f *is gbent in* $\mathcal{GB}_n^{2^k}$*;*

(ii) h *and* $h + 2^{k-2}g$ *are both gbent in* $\mathcal{GB}_n^{2^{k-1}}$ *with* $\mathcal{H}_{h+2^{k-2}g}(\mathbf{u}) = \pm\mathcal{H}_h(\mathbf{u})$, *for all* $\mathbf{u} \in \mathbb{V}_n$.

If n *is odd, then (ii) implies (i).*

Proof. We first show that for n even, h and $h + 2^{k-2}g$ are gbent in $\mathcal{GB}_n^{2^{k-1}}$ if f is gbent in $\mathcal{GB}_n^{2^k}$. In a second step, we show that if h and $h + 2^{k-2}g$ are both gbent in $\mathcal{GB}_n^{2^{k-1}}$, then f is gbent in $\mathcal{GB}_n^{2^k}$ if and only if $\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) = \pm\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})$, for all $\mathbf{u} \in \mathbb{V}_n$. This will conclude the proof for both, n even and n odd.

Let $\mathbf{u} \in \mathbb{V}_n$, and for $e \in \{0, 1\}$ and $r \in \{0, \ldots, 2^{k-1} - 1\}$, let

$$S^{(\mathbf{u})}(e, r) = \{\mathbf{x} \in \mathbb{V}_n \ : \ g(\mathbf{x}) = e \text{ and } h(\mathbf{x}) + 2^{k-2}(\mathbf{u} \cdot \mathbf{x}) = r\}.$$

With the notations of Proposition 1, we have $f_{\mathbf{u}}(\mathbf{x}) = f(\mathbf{x}) + 2^{k-1}(\mathbf{u} \cdot \mathbf{x}) = g(\mathbf{x}) + 2(h(\mathbf{x}) + 2^{k-2}(\mathbf{u} \cdot \mathbf{x}))$, and $|S^{(\mathbf{u})}(e, r)| = b_{e+2r}^{(\mathbf{u})}$. If f is gbent, by Proposition 1, there exist $\epsilon \in \{0, 1\}$ and $0 \le \rho_{\mathbf{u}} \le 2^{k-2} - 1$, for which $|S^{(\mathbf{u})}(\epsilon, \rho_{\mathbf{u}} + 2^{k-2})| = |S^{(\mathbf{u})}(\epsilon, \rho_{\mathbf{u}})| \pm 2^{n/2}$. For $(e, r) \neq (\epsilon, \rho_{\mathbf{u}})$, we have $|S^{(\mathbf{u})}(e, r + 2^{k-2})| = |S^{(\mathbf{u})}(e, r)|$. Observing that $\{\mathbf{x} \in \mathbb{V}_n \ : \ h(\mathbf{x}) + 2^{k-2}(\mathbf{u} \cdot \mathbf{x}) = r\} = S^{(u)}(0, r) \cup S^{(u)}(1, r)$, we obtain

$$\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^{k-1}}^{h(\mathbf{x})}(-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^{k-1}}^{h(\mathbf{x}) + 2^{k-2}(\mathbf{u} \cdot \mathbf{x})} = \pm\zeta_{2^{k-1}}^{\rho_{\mathbf{u}}} 2^{n/2}.$$

Consequently, h is gbent in $\mathcal{GB}_n^{2^{k-1}}$. For $h + 2^{k-2}g \in \mathcal{GB}_n^{2^{k-1}}$ we have

$$\begin{aligned}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^{k-1}}^{h(\mathbf{x}) + 2^{k-2}(\mathbf{u} \cdot \mathbf{x}) + 2^{k-2} g\mathbf{x}} = \sum_{\substack{e \in \mathbb{F}_2 \\ r \in \mathbb{Z}_{2^{k-1}}}} \sum_{x \in S^{(u)}(e,r)} \zeta_{2^{k-1}}^{r + 2^{k-2}e} \\ &= \sum_{\substack{e \in \mathbb{F}_2 \\ r \in \mathbb{Z}_{2^{k-1}}}} |S^{(u)}(e, r)| \zeta_{2^{k-1}}^{r + 2^{k-2}e} = \pm\zeta_{2^{k-1}}^{\rho_{\mathbf{u}} + 2^{k-2}\epsilon} 2^{n/2},\end{aligned}$$

which implies that also $h + 2^{k-2}g$ is gbent in $\mathcal{GB}_n^{2^{k-1}}$.

To show the condition $\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) = \pm\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})$, we first observe that

$$\begin{aligned}2\mathcal{H}_f^{(2^k)}(\mathbf{u}) &= 2 \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta_{2^k}^{g(\mathbf{x})} \zeta_{2^{k-1}}^{h(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} \\ &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} \left(1 + (-1)^{g(\mathbf{x})} + (1 - (-1)^{g(\mathbf{x})})\zeta_{2^k}\right) \zeta_{2^{k-1}}^{h(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} \\ &= (1 + \zeta_{2^k})\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) + (1 - \zeta_{2^k})\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}). \qquad (1)\end{aligned}$$

Writing $\zeta_{2^k} = x + yi$, $\mathcal{H}_h^{(2^{k-1})}(\mathbf{u}) = a + bi$ and $\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}) = c + di$, from Eq. (1), taking the complex norm, squaring and rearranging terms (recall that $|\zeta_{2^k}|^2 = x^2 + y^2 = 1$), we get

$$\begin{aligned} 2|\mathcal{H}_f^{(2^k)}(\mathbf{u})|^2 &= \frac{1}{2}(a^2+b^2)(1+2x+x^2+y^2) + \frac{1}{2}(c^2+d^2)(1-2x+x^2+y^2) \\ &\qquad - (ac+bd)(\mathbf{x}^2+y^2-1) + 2(ad-bc)y \\ &= |\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})|^2(1+x) + |\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})|^2(1-x) \\ &\quad + 2y\,\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right). \end{aligned} \tag{2}$$

If h, $h+2^{k-2}g$ are gbent, i.e. $|\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})|^2 = |\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})|^2 = 2^n$ for all $\mathbf{u} \in \mathbb{V}_n$, then we immediately see that $|\mathcal{H}_f^{(2^k)}(\mathbf{u})|^2 = 2^n$ for all $\mathbf{u} \in \mathbb{V}_n$, and hence f is gbent if and only if $\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right) = 0$, for all $\mathbf{u} \in \mathbb{V}_n$.

We now argue that the condition $\Im\left(\overline{\mathcal{H}_h^{(2^{k-1})}(\mathbf{u})}\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u})\right) = 0$ is equivalent to $\mathcal{H}_{h+2^{k-2}g}(\mathbf{u}) = \pm\mathcal{H}_h(\mathbf{u})$. For easy writing, let f_0, f_1 be the gbent functions in the indices above. By the regularity of gbent functions (when n is even or $k \geq 3$), $\mathcal{H}_{f_0}(\mathbf{u}) = 2^{n/2}\zeta_{2^{k-1}}^i$, $\mathcal{H}_{f_1}(\mathbf{u}) = 2^{n/2}\zeta_{2^{k-1}}^j$ for some integers $0 \leq i, j \leq 2^k - 1$. Hence $\overline{\mathcal{H}_{f_0}(\mathbf{u})}\,\mathcal{H}_{f_1}(\mathbf{u})$ is real if and only if $\zeta_{2^k}^{j-i} = \pm 1$, i.e. $i = j$ or $i = j + 2^{k-1}$ (modulo 2^k). Equivalently, $\mathcal{H}_{f_1}(\mathbf{u}) = \pm\mathcal{H}_{f_0}(\mathbf{u})$. If n is odd and $k = 2$, then $\mathcal{H}_f(\mathbf{u}) = 2^{n/2}\zeta_8^i$, $i \in \{1, 3, 5, 7\}$, and the same argument works.

We close this section with some remarks on relations between gbent functions in $\mathcal{GB}_n^{2^k}$, n even, and relative difference sets. First note that the characters of $\mathbb{V}_n \times \mathbb{Z}_{2^k}$ are $\chi_{\mathbf{u},a}(\mathbf{x}, z) = \zeta_{2^k}^{az}(-1)^{\langle\mathbf{u},\mathbf{x}\rangle}$, $\mathbf{u} \in \mathbb{V}_n$, $a \in \mathbb{Z}_{2^k}$. Recall that if $|\chi_{\mathbf{u},a}(D)| = 2^{n/2}$ for all nonzero $a \in \mathbb{Z}_{2^k}$ and all $\mathbf{u} \in \mathbb{V}_n$, then the graph $D = \{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in \mathbb{V}_n\}$ of f forms a relative difference set in $\mathbb{V}_n \times \mathbb{Z}_{2^k}$ (see for instance Sect. 2.4. in [10]). Equivalently, if af is gbent for all nonzero a, then D is a relative difference set. As easily seen, it is sufficient that $2^t f$ is gbent for all $0 \leq t \leq k-1$. Using Theorem 2, it is not hard to show that $F(\mathbf{x}) = (a_0(\mathbf{x}), \ldots, a_{k-1}(\mathbf{x}))$ is then a vectorial bent function, hence also a relative difference set in an elementary abelian group. Such gbent functions, which seem quite rare, may be of particular interest for future research. For an example of a class of such gbent functions obtained from partial spreads we refer to [5].

3 Complete Characterization of Generalized Bent and Semibent Functions in $\mathcal{GB}_n^{16}$

We write $f \in \mathcal{GB}_n^{16}$ as

$$\begin{aligned} f(\mathbf{x}) &= a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x}) \\ &= b_1(\mathbf{x}) + 2^2b_2(\mathbf{x}) = a_1(\mathbf{x}) + 2d(\mathbf{x}), \end{aligned}$$

where $a_i(\mathbf{x}) \in \mathcal{B}_n$, $i = 1, 2, 3, 4$, $b_1(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x})$, $b_2(\mathbf{x}) = a_3(\mathbf{x}) + 2a_4(\mathbf{x})$ are in $\mathcal{GB}_n^4$, and $d(\mathbf{x}) = a_2(\mathbf{x}) + 2a_3(\mathbf{x}) + 2^2 a_4(\mathbf{x}) \in \mathcal{GB}_n^8$.

Our objective is to show necessary *and* sufficient conditions on the components $a_1, a_2, a_3, a_4, b_1, b_2, d$ for the gbentness of f. For the conditions on a_1 and d for the gbentness of $a_1(\mathbf{x}) + 2d(\mathbf{x})$ when n is even, we can apply Theorem 3: $f(\mathbf{x}) = a_1(\mathbf{x}) + 2d(\mathbf{x})$ is gbent if and only if d and $d + 4a_1$ are gbent in $\mathcal{GB}_n^8$ and $\mathcal{H}_d^{(8)}(\mathbf{u}) = \pm\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})$ for all $\mathbf{u} \in \mathbb{V}_n$.

We start with a complete characterization of gbent functions in $\mathcal{GB}_n^{16}$ in terms of a_1, a_2, a_3, a_4. By this we extend results in [8,9] on gbent functions in $\mathcal{GB}_n^4$ and $\mathcal{GB}_n^8$. We then also will characterize gsemibent functions $f \in \mathcal{GB}_n^{16}$ in terms of a_1, a_2, a_3, a_4.

Theorem 4. *Suppose that* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x}) + 2^3 a_4(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \le i \le 4$. *Then* f *is gbent in* $\mathcal{GB}_n^{16}$ *if and only if the conditions* (i) *(if* n *is even), or* (ii) *(if* n *is odd) hold:*

(i) *For all* $c_i \in \mathbb{F}_2$, $i = 1, 2, 3$, *the Boolean function* $c_1a_1 \oplus c_2a_2 \oplus c_3a_3 \oplus a_4$ *is bent, and for all* $\mathbf{u} \in \mathbb{V}_n$ *we have*

$$\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u})$$
$$= \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}), \text{ and}$$
$$\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u}).$$

(ii) *For all* $c_i \in \mathbb{F}_2$, $i = 1, 2, 3$, *the Boolean function* $c_1a_1 \oplus c_2a_2 \oplus c_3a_3 \oplus a_4$ *is semibent, and for all* $\mathbf{u} \in \mathbb{V}_n$ *we either have*

$$\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = \pm 2^{n+1} \text{ and}$$
$$\mathcal{W}_{a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}) = 0,$$

or

$$\mathcal{W}_{a_2\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u}) = 0 \text{ and}$$
$$\mathcal{W}_{a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u}) = \pm 2^{n+1}.$$

Our proof for Theorem 4 is quite technical and in parts computer-assisted. Hence we omit is here and present it in the appendix.

The result on the semibentness of functions in $\mathcal{GB}_n^{16}$ is obtained with the same approach. For the proof we again refer to the appendix.

Theorem 5. *Let* $f \in \mathcal{GB}_n^{16}$ *be given as* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x}) + 2^3 a_4(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \le i \le 4$. *Then* f *is gsemibent when* n *is odd, and generalized* 2*-plateaued when* n *is even, if and only if the Boolean function* $c_1a_1 \oplus c_2a_2 \oplus c_3a_3 \oplus a_4$ *is semibent for all* $c_i \in \mathbb{F}_2$, $i = 1, 2, 3$, *such that for all* $\mathbf{u} \in \mathbb{V}_n$ *their Walsh-Hadamard transforms are either all zero, or they satisfy*

$$\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_2+a_4}(\mathbf{u}) = \mathcal{W}_{a_3+a_4}(\mathbf{u})\mathcal{W}_{a_2+a_3+a_4}(\mathbf{u})$$
$$= \mathcal{W}_{a_1+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_2+a_4}(\mathbf{u}) = \mathcal{W}_{a_1+a_3+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_2+a_3+a_4}(\mathbf{u}), \text{ and}$$
$$\mathcal{W}_{a_4}(\mathbf{u})\mathcal{W}_{a_3+a_4}(\mathbf{u}) = \mathcal{W}_{a_1+a_4}(\mathbf{u})\mathcal{W}_{a_1+a_3+a_4}(\mathbf{u}).$$

In the light of Theorem 4, one may expect that with a similar approach one can also show relations between gbentness in $\mathcal{GB}_n^{16}$ and in $\mathcal{GB}_n^4$. We here only state the theorem. For the proof we refer to our eprint [4].

Theorem 6. *Let* $f \in \mathcal{GB}_n^{16}$ *with* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2 a_3(\mathbf{x}) + 2^3 a_4(\mathbf{x}) = b_1(\mathbf{x}) + 2^2 b_2(\mathbf{x})$*, where* $b_1 = a_1 + 2a_2, b_2 = a_3 + 2a_4 \in \mathcal{GB}_n^4$*. The function* f *is gbent in* $\mathcal{GB}_n^{16}$ *if and only if* $b_2, b_1+b_2, 2b_1+b_2, 3b_1+b_2$ *are gbent in* $\mathcal{GB}_n^4$ *with their generalized Walsh-Hadamard transforms satisfying the following conditions,* (i) *for* n *even, respectively,* (ii) *for* n *odd, for all* $\mathbf{u} \in \mathbb{V}_n$*:*

(i) $2^{-n/2}(\mathcal{H}_{3b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_1+b_2}(\mathbf{u}), \mathcal{H}_{2b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_2}(\mathbf{u}))$ *belongs to one of* $(\epsilon,\epsilon,\epsilon,\epsilon)$, $(\epsilon,\epsilon,-\epsilon,-\epsilon)$, $(\epsilon,-\epsilon,\epsilon i,-\epsilon i)$, $(\epsilon - \epsilon,-\epsilon i,\epsilon i)$, $(\epsilon i,\epsilon i,\epsilon i,\epsilon i)$, $(\epsilon i,\epsilon i,-\epsilon i,-\epsilon i)$, $(\epsilon i,-\epsilon i,\epsilon,-\epsilon)$, $(-\epsilon i,\epsilon i,-\epsilon,\epsilon)$*, where* $\epsilon \in \{\pm 1\}$*.*

(ii) $2^{-(n-1)/2}(\mathcal{H}_{3b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_1+b_2}(\mathbf{u}), \mathcal{H}_{2b_1+b_2}(\mathbf{u}), \mathcal{H}_{b_2}(\mathbf{u}))$ *belongs to one of* $(\epsilon+\mu i,\epsilon+\mu i,\epsilon+\mu i,\epsilon+\mu i)$, $(\epsilon+\mu i,\epsilon+\mu i,-\epsilon-\mu i,-\epsilon-\mu i)$, $(\epsilon+\mu i,-\epsilon-\mu i,\epsilon-\mu i,-\epsilon+\mu i)$, $(\epsilon+\mu i,-\epsilon-\mu i,-\epsilon+\mu i,\epsilon-\mu i)$*, for* $\epsilon,\mu \in \{\pm 1\}$*.*

We close this section with some results on the Gray image $\psi(f)$ of gbent functions f in $\mathcal{GB}_n^8$ and $\mathcal{GB}_n^{16}$, extending the corresponding results in [9].

Lemma 2. *Let* $n, k \geq 2$ *be positive integers and* $\psi : \mathbb{V}_{n+k-1} \to \mathbb{F}_2$ *be defined by* $\psi(\mathbf{x}, y_1, y_2, \ldots, y_{k-1}) = a_k(\mathbf{x}) \oplus \bigoplus_{i=1}^{k-1} y_i a_i(\mathbf{x})$*, where* $a_i \in \mathcal{B}_n$*,* $1 \leq i \leq k$*. Denote by* $\mathbf{a}(\mathbf{x})$ *the vectorial Boolean function* $\mathbf{a}(\mathbf{x}) = (a_1(\mathbf{x}), \ldots, a_{k-1}(\mathbf{x}))$ *and let* $\mathbf{u} \in \mathbb{V}_n$ *and* $\mathbf{v} = (v_1, \ldots, v_{k-1}) \in \mathbb{V}_{k-1}$*. The Walsh-Hadamard transform of* ψ *at* $(\mathbf{u}, \mathbf{v})$ *is then*

$$\mathcal{W}_\psi(\mathbf{u}, v_1, \ldots, v_{k-1}) = \sum_{\alpha \in \mathbb{V}_{k-1}} (-1)^{\alpha \cdot \mathbf{v}} \mathcal{W}_{a_k \oplus \alpha \cdot \mathbf{a}}(\mathbf{u}).$$

Proof. We will show our claim by induction on k. For $k = 2$ we have

$$\begin{aligned} \mathcal{W}_\psi(\mathbf{u}, v_1) &= \sum_{\substack{\mathbf{x} \in \mathbb{V}_n \\ y_1 \in \mathbb{F}_2}} (-1)^{y_1 a_1(\mathbf{x}) \oplus a_2(\mathbf{x})} (-1)^{v_1 y_1 \oplus \mathbf{u} \cdot \mathbf{x}} \\ &= \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{a_2(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} + \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{a_1(\mathbf{x}) \oplus a_2(\mathbf{x})} (-1)^{v_1 \oplus \mathbf{u} \cdot \mathbf{x}} \\ &= \mathcal{W}_{a_2}(\mathbf{u}) + (-1)^{v_1} \mathcal{W}_{a_1 \oplus a_2}(\mathbf{u}). \end{aligned}$$

Now let

$$\begin{aligned} &\psi(\mathbf{x}, y_1, \ldots, y_k) = \psi_1(\mathbf{x}, y_1, \ldots, y_{k-1}) \oplus y_k a_k(\mathbf{x}), \text{ where} \\ &\psi_1(\mathbf{x}, y_1, \ldots, y_{k-1}) = a_{k+1}(\mathbf{x}) \oplus \bigoplus_{i=1}^{k-1} y_i a_i(\mathbf{x}). \end{aligned}$$

Then $\mathcal{W}_\psi(\mathbf{u}, \mathbf{v}, v_k) = \mathcal{W}_{\psi_1}(\mathbf{u}, \mathbf{v}) + (-1)^{v_k} \mathcal{W}_{\psi_1 \oplus a_{k+1}}(\mathbf{u}, \mathbf{v})$, which implies our claim by the induction assumption.

Theorem 7. *We have:*

(*i*) *Let* $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) \in \mathcal{G}B_n^8$ *be gbent. Then its Gray image* $\psi(f)$ *is semibent in* $\mathcal{B}_{n+2}$.

(*ii*) *Let* $f = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + 2^2a_3(\mathbf{x}) + 2^3a_4(\mathbf{x}) \in \mathcal{GB}_n^{16}$ *be gbent. Then* $\psi(f)$ *is semibent in* $\mathcal{B}_{n+3}$ *if* n *is odd, and* 3*-plateaued in* $\mathcal{B}_{n+3}$ *if* n *is even.*

Proof. (*i*) By Lemma 2, for $\psi(f)(\mathbf{x}, y_1, y_2) = a_1(\mathbf{x})y_1 + a_2(\mathbf{x})y_2 + a_3(\mathbf{x})$,

$$\begin{aligned}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) =& \mathcal{W}_{a_3}(\mathbf{u}) + (-1)^{v_1}\mathcal{W}_{a_3\oplus a_1}(\mathbf{u}) \\ &+ (-1)^{v_2}\mathcal{W}_{a_3\oplus a_2}(\mathbf{u}) + (-1)^{v_1+v_2}\mathcal{W}_{a_3\oplus a_2\oplus a_1}(\mathbf{u}).\end{aligned} \tag{3}$$

Assume first that n is even. Since f is gbent, by [9, Theorem 19], for the bent components we have $\mathcal{W}_{a_3}(\mathbf{u})\mathcal{W}_{a_1\oplus a_2\oplus a_3}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3}(\mathbf{u})\mathcal{W}_{a_2\oplus a_3}(\mathbf{u})$, for all $\mathbf{u} \in \mathbb{V}_n$. Take $\mathcal{W}_{a_3}(\mathbf{u}) = \mu_1(\mathbf{u})2^{n/2}, \mathcal{W}_{a_3\oplus a_1}(\mathbf{u}) = \mu_2(\mathbf{u})2^{n/2}, \mathcal{W}_{a_3\oplus a_2}(\mathbf{u}) = \mu_3(\mathbf{u})2^{n/2}, \mathcal{W}_{a_3\oplus a_2\oplus a_1}(\mathbf{u}) = \mu_4(\mathbf{u})2^{n/2}$, for some $\mu_i \in \{-1, 1\}, 1 \le i \le 4$. Thus, $\mu_1(\mathbf{u})\mu_4(\mathbf{u}) = \mu_2(\mathbf{u})\mu_3(\mathbf{u})$. Using these in Eq. (3), we obtain

$$2^{-n/2}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) = \mu_1(\mathbf{u}) + (-1)^{v_1}\mu_2(\mathbf{u}) + (-1)^{v_2}\mu_3(\mathbf{u}) + (-1)^{v_1\oplus v_2}\mu_4(\mathbf{u}).$$

For $(\mu_1(\mathbf{u}), \mu_2(\mathbf{u}), \mu_3(\mathbf{u}), \mu_4(\mathbf{u}))$ with values in the set

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

$2^{-n/2}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2)$ takes one of the following values

$$\begin{aligned}&(-1)^{v_1\oplus v_2\oplus 1} + (-1)^{v_1\oplus 1} + (-1)^{v_2\oplus 1} - 1, (-1)^{v_1\oplus v_2} + (-1)^{v_1\oplus 1} + (-1)^{v_2} - 1,\\ &(-1)^{v_1\oplus v_2} + (-1)^{v_1} + (-1)^{v_2\oplus 1} - 1, (-1)^{v_1\oplus v_2\oplus 1} + (-1)^{v_1} + (-1)^{v_2} - 1,\\ &(-1)^{v_1\oplus v_2} + (-1)^{v_1\oplus 1} + (-1)^{v_2\oplus 1} + 1, (-1)^{v_1\oplus v_2\oplus 1} + (-1)^{v_1\oplus 1} + (-1)^{v_2} + 1,\\ &(-1)^{v_1\oplus v_2\oplus 1} + (-1)^{v_1} + (-1)^{v_2\oplus 1} + 1, (-1)^{v_1\oplus v_2} + (-1)^{v_1} + (-1)^{v_2} + 1.\end{aligned}$$

Therefore, $\mathcal{W}_{\psi(f)}$ attains the values $0, \pm 2^{(n+4)/2}$, thus $\psi(f)$ is semibent.

We now consider the case of odd n. Then, by [9, Theorem 19], $a_3, a_1 \oplus a_3, a_2 \oplus a_3, a_1 \oplus a_2 \oplus a_3$ are all semibent and, $\mathcal{W}_{a_3}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3}(\mathbf{u}) = 0$ and $|\mathcal{W}_{a_1\oplus a_2\oplus a_3}(\mathbf{u})| = |\mathcal{W}_{a_2\oplus a_3}(\mathbf{u})| = 2^{(n+1)/2}$, or $|\mathcal{W}_{a_3}(\mathbf{u})| = |\mathcal{W}_{a_1\oplus a_3}(\mathbf{u})| = 2^{(n+1)/2}$ and $\mathcal{W}_{a_1\oplus a_2\oplus a_3}(\mathbf{u}) = \mathcal{W}_{a_2\oplus a_3}(\mathbf{u}) = 0$.

Case 1. Let $\mathcal{W}_{a_3}(\mathbf{u}) = \mathcal{W}_{a_1\oplus a_3}(\mathbf{u}) = 0$, $\mathcal{W}_{a_1\oplus a_2\oplus a_3}(\mathbf{u}) = \epsilon_1(\mathbf{u})2^{(n+1)/2}$, $\mathcal{W}_{a_2\oplus a_3}(\mathbf{u}) = \epsilon_2(\mathbf{u})2^{(n+1)/2}$, with $\epsilon_1, \epsilon_2 \in \{-1, 1\}$. With (3),

$$\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) = (-1)^{v_2}2^{(n+1)/2}\left(\epsilon_1(\mathbf{u}) + (-1)^{v_1}\epsilon_2(\mathbf{u})\right),$$

from which we infer that $\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) \in \{0, \pm 2^{(n+3)/2}\}$, for all combinations of $\epsilon_i(\mathbf{u})$ and v_i, $i = 1, 2$. Therefore $\psi(f)$ is semibent.

Case 2. Let $\mathcal{W}_{a_3}(\mathbf{u}) = \epsilon_1(\mathbf{u})2^{(n+1)/2}$, $\mathcal{W}_{a_1\oplus a_3}(\mathbf{u}) = \epsilon_2(\mathbf{u})2^{(n+1)/2}$, $\mathcal{W}_{a_1\oplus a_2\oplus a_3}(\mathbf{u}) = \mathcal{W}_{a_2\oplus a_3}(\mathbf{u}) = 0$, with $\epsilon_1, \epsilon_2 \in \{-1, 1\}$. As before, from (3) we obtain

$$\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) = 2^{(n+1)/2}\left(\epsilon_1(\mathbf{u}) + (-1)^{v_1}\epsilon_2(\mathbf{u})\right),$$

from which we infer that $\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2) \in \{0, \pm 2^{(n+3)/2}\}$ and therefore $\psi(f)$ is semibent.

(*ii*) By Lemma 2, for $\psi(f)(\mathbf{x}, y_1, y_2, y_3) = a_4(\mathbf{x}) \bigoplus_{i=1}^{3} y_i a_i(\mathbf{x})$,

$$\begin{aligned}\mathcal{W}_{\psi(f)}(\mathbf{u}, v_1, v_2, v_3) &= \mathcal{W}_{a_4}(\mathbf{u}) + (-1)^{v_1}\mathcal{W}_{a_4\oplus a_1}(\mathbf{u})\\ &+ (-1)^{v_2}\mathcal{W}_{a_4\oplus a_2}(\mathbf{u}) + (-1)^{v_3}\mathcal{W}_{a_4\oplus a_3}(\mathbf{u})\\ &+ (-1)^{v_1\oplus v_2}\mathcal{W}_{a_4\oplus a_2\oplus a_1}(\mathbf{u}) + (-1)^{v_1\oplus v_3}\mathcal{W}_{a_4\oplus a_3\oplus a_1}(\mathbf{u})\\ &+ (-1)^{v_2\oplus v_3}\mathcal{W}_{a_4\oplus a_3\oplus a_2}(\mathbf{u}) + (-1)^{v_1\oplus v_2\oplus v_3}\mathcal{W}_{a_4\oplus a_3\oplus a_2\oplus a_1}(\mathbf{u}).\end{aligned}$$

By going through the 32 cases of Theorem 4 for the Walsh-Hadamard transforms in the expression above (16 for n even and 16 for n odd), we obtain that the Walsh-Hadamard spectrum is $\{0, \pm 2^{3+n/2}\}$ (for n even) and $\{0, \pm 2^{2+(n+1)/2}\}$ (for n odd), hence the claim.

Acknowledgements. Work by P.S. started during a very enjoyable visit at RICAM. Both the second and third named author thank the institution for the excellent working conditions. The second author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

A Appendix

Proof of Theorem 4*:* Let $\mathbf{u} \in \mathbb{V}_n$. Eq. (2) for $k = 4$ implies

$$16\sqrt{2}|\mathcal{H}_f^{(16)}(\mathbf{u})|^2 = (2 + \sqrt{2+\sqrt{2}})4\sqrt{2}|\mathcal{H}_d^{(8)}(\mathbf{u})|^2 + (2 - \sqrt{2+\sqrt{2}})4\sqrt{2}|\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})|^2 + 8\sqrt{4-2\sqrt{2}}\,\Im\left(\overline{\mathcal{H}_d^{(8)}(\mathbf{u})}\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})\right). \tag{4}$$

We denote by A, C, D, W the Walsh-Hadamard transforms $\mathcal{W}_{a_4}(\mathbf{u})$, $\mathcal{W}_{a_2\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_3\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_2\oplus a_3\oplus a_4}(\mathbf{u})$ (in that order). We denote by B, X, Y, Z the Walsh-Hadamard transforms $\mathcal{W}_{a_1\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_1\oplus a_2\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_1\oplus a_3\oplus a_4}(\mathbf{u})$, $\mathcal{W}_{a_1\oplus a_2\oplus a_3\oplus a_4}(\mathbf{u})$ (in that order). By [9, Lemma 17], we know that the generalized Walsh-Hadamard transform of any function in $\mathcal{GB}_n^8$, say d and $d + 4a_1$ with $d = a_2 + 2a_3 + 2^2 a_4$, is of the form

$$4\mathcal{H}_d^{(8)}(\mathbf{u}) = \alpha_0 A + \alpha_1 C + \alpha_2 D + \alpha_3 W, \quad 4\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u}) = \alpha_0 B + \alpha_1 X + \alpha_2 Y + \alpha_3 Z,$$

where $\alpha_0 = 1 + (1+\sqrt{2})i$, $\alpha_1 = 1 + (1-\sqrt{2})i$, $\alpha_2 = 1 + \sqrt{2} - i$, $\alpha_3 = 1 - \sqrt{2} - i$, and moreover that (see also [9, Corollary 18]),

$$4\sqrt{2}|\mathcal{H}_d^{(8)}(\mathbf{u})|^2 = A^2 - C^2 + 2CD + D^2 - 2AW - W^2 + \sqrt{2}(A^2 + C^2 + D^2 + W^2) \tag{5}$$

$$4\sqrt{2}|\mathcal{H}_{d+4a_1}^{(8)}(\mathbf{u})|^2 = B^2 - X^2 + 2XY + Y^2 - 2BZ - Z^2 + \sqrt{2}(B^2 + X^2 + Y^2 + Z^2).$$

Furthermore, with straightforward computations we get

$$\begin{aligned} &8\sqrt{4-2\sqrt{2}}\,\Im\left(\overline{\mathcal{H}_b^{(8)}(\mathbf{u})}\mathcal{H}_{b+4a_1}^{(8)}(\mathbf{u})\right)\\ &= 2\sqrt{2-\sqrt{2}}\,(BC+BD-AX-WX-AY+WY+CZ-DZ)\\ &\quad+2\sqrt{4-2\sqrt{2}}\,(BD+WX-AY-CZ). \end{aligned} \tag{6}$$

Using (5) and (6) in Eq. (4) we obtain

$$\begin{aligned} &16\sqrt{2}|\mathcal{H}_f^{(16)}(\mathbf{u})|^2\\ &= 2(A^2+B^2-C^2+2CD+D^2-2AW-W^2-X^2+2XY+Y^2-2BZ-Z^2)\\ &\quad+2\sqrt{2}(A^2+B^2+C^2+D^2+W^2+X^2+Y^2+Z^2)\\ &\quad+\sqrt{2-\sqrt{2}}\,(A^2-B^2+2BC+C^2+D^2+W^2-2AX-4WX-X^2\\ &\qquad+2WY-Y^2+4CZ-2DZ-Z^2)\\ &\quad+2\sqrt{2+\sqrt{2}}\,(A^2-B^2+BD+CD+D^2-AW+WX-AY-XY\\ &\qquad-Y^2+BZ-CZ). \end{aligned} \tag{7}$$

If f is gbent in $\mathcal{GB}_n^{16}$, i.e., $|\mathcal{H}_f^{(16)}(\mathbf{u})|^2 = 2^n$, by the linear independence of $\{1, \sqrt{2}, \sqrt{2-\sqrt{2}}, \sqrt{2+\sqrt{2}}\}$ (as easily shown, the set forms a basis of $\mathbb{Q}(\sqrt{2}, \sqrt{2-\sqrt{2}})$), we arrive at the following system of equations with solutions in $\mathbb{Z}$,

$$\begin{aligned} &A^2+B^2+C^2+D^2+W^2+X^2+Y^2+Z^2 = 2^{n+3}\\ &A^2+B^2-C^2+2CD+D^2-2AW-W^2-X^2+2XY+Y^2-2BZ-Z^2 = 0\\ &A^2-B^2+2BC+C^2+D^2+W^2-2AX-4WX-X^2\\ &\qquad\qquad+2WY-Y^2+4CZ-2DZ-Z^2 = 0\\ &A^2-B^2+BD+CD+D^2-AW+WX-AY-XY-Y^2+BZ-CZ = 0. \end{aligned} \tag{8}$$

Let 2^t be the largest power of 2 which divides all, A, B, C, D, X, Y, Z and W, i.e., $A = 2^t A_1$, etc., with at least one of the $A_1, B_1, \ldots$ being odd. First, if n is even and $t > \frac{n}{2}$, then $t = \frac{n}{2} + 1$ only. Dividing by 2^{2t}, the first equation of (8) becomes $A_1^2 + B_1^2 + C_1^2 + D_1^2 + W_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 2$, which gives the solution $(\pm 1, \pm 1, 0, 0, 0, 0, 0, 0)$ (and permutations of these values). However, a simple computation reveals that none of these possibilities also satisfies the last three equations of (8). If n is odd and $t > \frac{n+1}{2}$, then $t = \frac{n+3}{2}$, but this implies that only one value out of $A, B, \ldots$ is nonzero. Again, that is impossible to satisfy the last three equations of (8). Assume now that $t < \frac{n}{2}$. The first equation of (8) becomes $A_1^2 + B_1^2 + C_1^2 + D_1^2 + W_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 2^{n+3-2t}$, which is divisible by 2^5 (when n is even, since $t \le \frac{n-2}{2}$), respectively 2^4 (when n is odd, since $t \le \frac{n-1}{2}$). If n is even, this can only happen if $A_1, B_1, \ldots$, are all even, that is, $\equiv 0, 2, 4, 6 \pmod 8$, but that contradicts our assumption that t is the largest power of 2 dividing $A, B, \ldots$. If n is odd and $t \le \frac{n-3}{2}$, the previous argument would work, and if $t = \frac{n-1}{2}$, then $A_1^2 + B_1^2 + C_1^2 + D_1^2 + W_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 16$. By considering every residues for $A_1, B_1, \ldots,$ modulo 4 and imposing the condition that the 2nd, 3rd, 4th equations of our system also must be 0 modulo 16, we only get possibilities $(0,0,2,2,0,0,2,2)$, $(0,2,0,2,0,2,0,2)$, $(0,2,2,0,0,2,2,0)$, $(2,0,0,2,2,0,0,2)$, $(2,0,2,0,2,0,2,0)$, $(2,2,0,0,2,2,0,0)$ for $(A_1, B_1, \ldots)$ modulo 4, but that implies that all $A_1, B_1, \ldots$ are even, contradicting our assumption on t. This shows that the only possibility is $2^t = 2^{n/2}$ if n is even, and $2^t = 2^{(n+1)/2}$ if n is odd.

Thus, one needs to find integer solutions for the equation $A_1^2 + B_1^2 + C_1^2 + D_1^2 + \mathcal{W}_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 8$, for n even, or $A_1^2 + B_1^2 + C_1^2 + D_1^2 + \mathcal{W}_1^2 + X_1^2 + Y_1^2 + Z_1^2 = 4$ for n odd, which also satisfy the last three equations in (8). Mathematica renders the following: if n is even, then $2^{-\frac{n}{2}}(A, C, D, W, B, X, Y, Z)$ (note the order) is one of

$$\begin{array}{ll}
\pm(-1,-1,-1,-1,-1,-1,-1,-1), & \pm(-1,1,-1,1,-1,1,-1,1),\\
\pm(-1,-1,-1,-1,1,1,1,1), & \pm(-1,1,-1,1,1,-1,1,-1),\\
\pm(1,-1,-1,1,-1,1,1,-1), & \pm(1,1,-1,-1,-1,-1,1,1),\\
\pm(1,-1,-1,1,1,-1,-1,1), & \pm(1,1,-1,-1,1,1,-1,-1),
\end{array} \tag{9}$$

and, if n is odd, then $2^{-\frac{n+1}{2}}(A, C, D, W, B, X, Y, Z)$ is one of

$$\begin{array}{ll}
\pm(-1,1,0,0,-1,1,0,0), & \pm(-1,1,0,0,1,-1,0,0),\\
\pm(0,0,-1,1,0,0,-1,1), & \pm(0,0,-1,1,0,0,1,-1),\\
\pm(0,0,1,1,0,0,-1,-1), & \pm(0,0,1,1,0,0,1,1),\\
\pm(1,1,0,0,-1,-1,0,0), & \pm(1,1,0,0,1,1,0,0).
\end{array}$$

We see that in both cases, if f is gbent, then the conditions of the theorem are satisfied. The converse follows with straightforward calculations. □

Proof of Theorem 5: Assume that f is gsemibent in $\mathcal{GB}_n^{16}$ when n is odd, respectively generalized 2-plateaued when n is even. Then $|\mathcal{H}_f^{(16)}(\mathbf{u})| \in \{0, \pm 2^{(n+1)/2}\}$ for n odd, respectively, $|\mathcal{H}_f^{(16)}(\mathbf{u})| \in \{0, \pm 2^{(n+2)/2}\}$ for n even. Using the notations of Theorem 4, from Eq. (7), we immediately get $A = B = C = D = X = Y = W = Z = 0$ if $\mathcal{H}_f^{(16)}(\mathbf{u}) = 0$. If $|\mathcal{H}_f^{(16)}(\mathbf{u})| = 2^{(n+1)/2}$ (for n odd), respectively, $|\mathcal{H}_f^{(16)}(\mathbf{u})| = 2^{(n+2)/2}$ (for n even), then (7) again yields the system of Eq. (8) with the one difference that in the first equation the power of 2 on the right side is 2^{n+4}, respectively, 2^{n+5}. With the same argument as in the proof of Theorem 4 we see that for such $\mathbf{u}$, $2^{-\frac{n+1}{2}}(A, C, D, W, B, X, Y, Z)$ (for n odd), respectively, $2^{-\frac{n+2}{2}}(A, C, D, W, B, X, Y, Z)$ (for n even) can only take the values from Eq. (9).

Straightforwardly, one confirms that the converse is also true, and the theorem is shown. □

References

1. Carlet, C.: $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inf. Theory **44**(4), 1543–1547 (1998)
2. Hodžić, S., Pasalic, E.: Generalized bent functions-some general construction methods and related necessary and sufficient conditions. Crypt. Commun. **7**, 469–483 (2015)
3. Liu, H., Feng, K., Feng, R.: Nonexistence of generalized bent functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_m$. Des. Codes Crypt. **82**, 647–662 (2017)
4. Martinsen, T., Meidl, W., Stănică, P.: Generalized bent functions and their Gray images. http://arxiv.org/pdf/1511.01438
5. Martinsen, T., Meidl, W., Stănică, P.: Partial spread and vectorial generalized bent functions. Des.Codes Crypt. (2017, to appear)
6. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. J. Comb. Theory - Ser. A **40**, 90–107 (1985)
7. Schmidt, K.U.: Quaternary constant-amplitude codes for multicode CDMA. IEEE Trans. Inform. Theory **55**(4), 1824–1832 (2009)
8. Solé, P., Tokareva, N.: Connections between quaternary and binary bent functions. Prikl. Diskr. Mat. **1**, 16–18 (2009). http://eprint.iacr.org/2009/544.pdf
9. Stănică, P., Martinsen, T., Gangopadhyay, S., Singh, B.K.: Bent and generalized bent Boolean functions. Des. Codes Crypt. **69**, 77–94 (2013)
10. Tan, Y., Pott, A., Feng, T.: Strongly regular graphs associated with ternary bent functions. J. Comb. Theory - Ser. A **117**, 668–682 (2010)