



Calhoun: The NPS Institutional Archive
DSpace Repository

Faculty and Researchers

Faculty and Researchers' Publications

2016-04-12

Decomposing generalized bent and hyperbent functions

Martinsen, Thor; Meidl, Wilfried; Mesnager, Sihem; Stnic, Pantelimon

arXiv:1604.02830 [cs.IT]

<http://hdl.handle.net/10945/51999>

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

Downloaded from NPS Archive: Calhoun



Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

Decomposing generalized bent and hyperbent functions

Thor Martinsen¹, Wilfried Meidl²,
Sihem Mesnager³, Pantelimon Stănică¹

¹Department of Applied Mathematics,
Naval Postgraduate School, Monterey, CA 93943-5212, U.S.A.;
Email: {tmartins,pstanica}@nps.edu

²Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria;
Email: meidlwilfried@gmail.com

³ Department of Mathematics,
Universities of Paris VIII and XIII and Telecom ParisTech,
LAGA, UMR 7539, CNRS, Sorbonne Paris Cité;
Email: smesnager@univ-paris8.fr

April 12, 2016

Abstract

In this paper we introduce generalized hyperbent functions from \mathbb{F}_{2^n} to \mathbb{Z}_{2^k} , and investigate decompositions of generalized (hyper)bent functions. We show that generalized (hyper)bent functions from \mathbb{F}_{2^n} to \mathbb{Z}_{2^k} consist of components which are generalized (hyper)bent functions from \mathbb{F}_{2^n} to $\mathbb{Z}_{2^{k'}}$ for some $k' < k$. For odd n , we show that the Boolean functions associated to a generalized bent function form an affine space of semibent functions. This complements a recent result for even n , where the associated Boolean functions are bent.

Keywords Boolean functions, Walsh-Hadamard transforms, bent functions, semi-bent functions, hyper bent functions, generalized bent functions, cyclotomic fields.

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 . Let $\Re(z) = \alpha$ and $\Im(z) = \beta i$ be the real and imaginary parts of a complex number $z = \alpha + \beta i$, respectively. For a *generalized Boolean function* $f : \mathbb{V}_n \rightarrow \mathbb{Z}_q$ we define the *generalized Walsh-Hadamard transform* to be the complex valued function

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

where $\zeta_q = e^{\frac{2\pi i}{q}}$ and $\langle \mathbf{u}, \mathbf{x} \rangle$ denotes a (nondegenerate) inner product on \mathbb{V}_n (we often use ζ , \mathcal{H}_f , instead of ζ_q , respectively, $\mathcal{H}_f^{(q)}$, when q is fixed). For $q = 2$, we obtain the usual *Walsh-Hadamard transform*

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

If $\mathbb{V}_n = \mathbb{F}_2^n$, the vector space of the n -tuples over \mathbb{F}_2 , we use the conventional dot product $\mathbf{u} \cdot \mathbf{x}$ for $\langle \mathbf{u}, \mathbf{x} \rangle$. The standard inner product of $u, x \in \mathbb{F}_2^n$ is $\text{Tr}_n(ux)$, where $\text{Tr}_n(z)$ denotes the absolute trace of $z \in \mathbb{F}_2^n$. Most of our general results we will present in the notation of $\mathbb{V}_n = \mathbb{F}_2^n$. For results where we emphasize hyperbent properties we require $\mathbb{V}_n = \mathbb{F}_2^n$.

We use the notations as in [8, 9, 15]. We denote the set of all generalized Boolean functions by \mathcal{GB}_n^q and when $q = 2$, by \mathcal{B}_n . A function $f : \mathbb{V}_n \rightarrow \mathbb{Z}_q$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$. We recall that 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, which only exist for even n since $\mathcal{W}_f(\mathbf{u})$ is an integer. Further, recall that $f \in \mathcal{B}_n$, n odd, is called *semibent* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, 2^{(n+1)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$. A jubilee survey paper on bent functions giving an historical perspective, and making pertinent connections to designs, codes and cryptography is [3]. A book devoted especially to bent functions and containing a complete survey (including variations, generalizations and applications) is [10].

In Section 2 we recall some results which are of importance to our considerations and will be used in the following sections. In Section 3 we introduce generalized hyperbent functions, and show hyperbentness for classes of gbent functions introduced in [9], which can be seen as generalized Dillon's *PS* functions. In Section 4 we investigate decompositions of generalized (hyper)bent functions. We show that generalized (hyper)bent functions from \mathbb{V}_n to \mathbb{Z}_{2^k} consist of components which are generalized (hyper)bent functions from \mathbb{V}_n to $\mathbb{Z}_{2^{k'}}$ for some $k' < k$. For odd n , we show that the Boolean

functions associated to a generalized bent function form an affine space of semibent functions. This complements a recent result for even n , where the associated Boolean functions are bent.

2 Preliminaries

We begin by collecting some results which we will subsequently use in the paper. We start with a lemma, which is Proposition 3 in [8].

Lemma 2.1. *Let $n = 2m$ be even, and for a function $f : \mathbb{V}_n \rightarrow \mathbb{Z}_{2^k}$ 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 $b_j^{(\mathbf{u})} = |\{\mathbf{x} \in \mathbb{V}_n : f_{\mathbf{u}}(\mathbf{x}) = j\}|$, $0 \leq j \leq 2^k - 1$. Then f is gbent if and only if for all $\mathbf{u} \in \mathbb{V}_n$ there exists an integer $\rho_{\mathbf{u}}$, $0 \leq \rho_{\mathbf{u}} \leq 2^{k-1} - 1$, such that*

$$b_{2^{k-1} + \rho_{\mathbf{u}}}^{(\mathbf{u})} = b_{\rho_{\mathbf{u}}}^{(\mathbf{u})} \pm 2^m \text{ and } b_{2^{k-1} + j}^{(\mathbf{u})} = b_j^{(\mathbf{u})}, \text{ for } 0 \leq j \leq 2^{k-1} - 1, j \neq \rho_{\mathbf{u}}.$$

In [8] it is shown that, similar to bent functions (in even and odd characteristic), the value set of $\mathcal{H}_f^{2^k}$ is quite restricted.

Proposition 2.2. *If $f \in \mathcal{GB}_n^{2^k}$ is gbent, then*

$$\mathcal{H}_f^{2^k}(\mathbf{u}) = 2^{n/2} \zeta_{2^k}^{f^*(\mathbf{u})}$$

for some function $f^* \in \mathcal{GB}_n^q$, except for n odd and $k = 2$, in which case we have

$$\mathcal{H}_f^4(\mathbf{u}) = 2^{\frac{n-1}{2}} (\pm 1 \pm i).$$

In accordance with the terminology for classical bent functions we say that gbent functions are regular (except for the case when n is odd and $k = 2$), and we call the function f^* the *dual* of f . With the standard proof for bent functions one can show that the dual f^* is also gbent and $(f^*)^* = f$.

Let $f \in \mathcal{GB}_n^{2^k}$, then we can represent f uniquely as

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

for some Boolean functions a_i , $1 \leq i \leq k$. The nature of these Boolean functions when f is gbent has been one of the main topics in research on gbent functions. In the next proposition and the following remark we summarize some main results on these Boolean functions.

Proposition 2.3. *Let $f(\mathbf{x})$ be a gbent function in $\mathcal{GB}_n^{2^k}$, $k > 1$, (uniquely) given as*

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

$a_i \in \mathcal{B}_n$, $1 \leq i \leq k$, and for $\mathbf{c} = (c_1, c_2, \dots, c_{k-1}) \in \mathbb{F}_2^{k-1}$, let $g_{\mathbf{c}}$ be the Boolean function

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

- (i) [8] *If n is even, then for all $\mathbf{c} \in \mathbb{F}_2^{k-1}$ the Boolean function $g_{\mathbf{c}}$ is a bent function.*
- (ii) [8, 13, 14] *If n is odd, and $k = 2, 3, 4$, then all Boolean functions $g_{\mathbf{c}}$, $\mathbf{c} \in \mathbb{F}_2^{k-1}$, are semibent.*

Remark 2.4. *When n is even, then $a_1(\mathbf{x}) + 2a_2(\mathbf{x}) \in \mathcal{GB}_n^4$ is gbent if and only if a_1 and $a_1 \oplus a_2$ are bent (see [13]). Sufficient conditions on the gbentness of $f \in \mathcal{GB}_n^{2^k}$ are also known for $k = 2$ when n is odd, and in general for $k = 3, 4$ (see [8, 13, 14]).*

Another result about the decomposition of gbent functions is the following theorem of [8].

Theorem 2.5 ([8, Theorem 20]). *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).

Remark 2.6. *In the proof of [8, Theorem 20] it is moreover shown that if h and $h + 2^{k-2}g$ are gbent, then f is gbent if and only if $\mathcal{H}_{h+2^{k-2}g}(\mathbf{u}) = \pm\mathcal{H}_h(\mathbf{u})$ for all $\mathbf{u} \in \mathbb{V}_n$. As one of our achievements here, in our Corollary 4.6 we will show that (i) and (ii) in Proposition 2.5 are equivalent also when n is odd.*

3 Generalized hyperbent functions

Let f be a Boolean function from \mathbb{F}_{2^n} to \mathbb{F}_2 , and let $1 \leq i \leq n$ be an integer with $\gcd(2^n - 1, i) = 1$. The *extended Walsh-Hadamard transform* $\mathcal{W}_{f,i}$ is the integer valued function

$$\mathcal{W}_{f,i}(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)} (-1)^{\text{Tr}_n(ux^i)}.$$

Recall that f is called *hyperbent* if $|\mathcal{W}_{f,i}(u)| = 2^{n/2}$, for all $1 \leq i \leq n$ with $\gcd(2^n - 1, i) = 1$. For background on hyperbent functions we refer to the articles [2, 4, 19].

In this section we introduce the concept of hyperbent functions for generalized Boolean functions, and show the generalized hyperbentness for a class of gbent functions presented in [9]. For a function $f \in \mathcal{GB}_n^{2^k}$ and an integer $1 \leq i \leq n$ with $\gcd(2^n - 1, i) = 1$, we define the *extended generalized Walsh-Hadamard transform* $\mathcal{H}_{f,i}^{(2^k)}$ as a natural extension of $\mathcal{W}_{f,i}$ as

$$\mathcal{H}_{f,i}^{(2^k)}(u) = \sum_{x \in \mathbb{F}_{2^n}} \zeta_q^{f(x)} (-1)^{\text{Tr}_n(ux^i)},$$

and call f a *generalized hyperbent (g-hyperbent)* function if $|\mathcal{H}_{f,i}^{(2^k)}(u)| = 2^{n/2}$, for all $1 \leq i \leq n$ with $\gcd(2^n - 1, i) = 1$.

In [2] Carlet and Gaborit proved that all functions in the class of PS_{ap} are hyperbent. We proceed similarly for a class of gbent functions from $\mathcal{GB}_{2^n}^{2^k}$ presented in [9], which can be seen as a function in a generalized PS_{ap} class. We recall the functions in the next proposition. We use the convention that $\frac{y'}{y} = 0$ if $y = 0$.

Proposition 3.1 ([9, Theorem 1]). *Let $g_j : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, $0 \leq j \leq k-1$, be Boolean functions with $g_j(0) = 0$ and $\sum_{t \in \mathbb{F}_{2^n}} \zeta^{\sum_{j=0}^{k-1} 2^j g_j(t)} = 0$. Then the*

function $f : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^k}$ given by $f(y', y) = \sum_{j=0}^{k-1} 2^j g_j(y'/y)$ is a gbent

function with the dual $f^(y', y) = \sum_{j=0}^{k-1} 2^j g_j(y/y')$.*

To show that these functions are g-hyperbent, we start with some preliminary considerations. Let ω be any element in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$, then $\mathbb{F}_{2^n} =$

$\mathbb{F}_{2^{n/2}} + \omega\mathbb{F}_{2^{n/2}}$. Furthermore, every $y \in \mathbb{F}_{2^{n/2}}$ satisfies $y^{2^{n/2}} = y$, therefore $\text{Tr}(y) = 0$ for $y \in \mathbb{F}_{2^{n/2}}$. With the inner product on \mathbb{F}_{2^n} defined by $\langle y, y' \rangle = \text{Tr}(yy')$, the subspace $\mathbb{F}_{2^{n/2}}$ is orthogonal to itself. Therefore,

$$\sum_{y \in \mathbb{F}_{2^{n/2}}} (-1)^{\text{Tr}(\lambda y)} = \begin{cases} 0 & \text{if } \lambda \notin \mathbb{F}_{2^{n/2}} \\ 2^{n/2} & \text{if } \lambda \in \mathbb{F}_{2^{n/2}} \end{cases} = 2^{n/2} \mathbf{1}_{\mathbb{F}_{2^{n/2}}}(\lambda). \quad (2)$$

Theorem 3.2. *The function f in Proposition 3.1 is g -hyperbent.*

Proof. We let $g(y'/y) := f(y', y)$. Analogous to Carlet and Gaborit's proof, for an integer i coprime to $2^n - 1$, we write (using $x := y' + \omega y$, $z := \frac{y'}{y}$)

$$\begin{aligned} \mathcal{H}_{f,i}^{(q)}(u) &= \sum_{x \in \mathbb{F}_{2^n}} \zeta^{f(x)} (-1)^{\text{Tr}(ax^i)} \\ &= \sum_{y, y' \in \mathbb{F}_{2^{n/2}}} \zeta^{g\left(\frac{y'}{y}\right)} (-1)^{\text{Tr}(a(y' + \omega y)^i)} \\ &= \sum_{y \in \mathbb{F}_{2^{n/2}}^*, y' \in \mathbb{F}_{2^{n/2}}} \zeta^{g\left(\frac{y'}{y}\right)} (-1)^{\text{Tr}(ay^i(z + \omega)^i)} + \sum_{y' \in \mathbb{F}_{2^{n/2}}} \zeta^{g(0) \oplus \text{Tr}(ay'^i)}. \end{aligned}$$

With (2) we obtain

$$\begin{aligned} \mathcal{H}_{f,i}^{(q)}(u) &= \sum_{z \in \mathbb{F}_{2^{n/2}}} \zeta^{g(z)} \sum_{y \in \mathbb{F}_{2^{n/2}}^*} (-1)^{\text{Tr}(a(z + \omega)^i y^i)} + \zeta^{g(0)} 2^{n/2} \cdot \mathbf{1}_{\mathbb{F}_{2^{n/2}}}(a) \\ &= \sum_{z \in \mathbb{F}_{2^{n/2}}} \zeta^{g(z)} \sum_{y \in \mathbb{F}_{2^{n/2}}} (-1)^{\text{Tr}(a(z + \omega)^i y^i)} \\ &\quad - \sum_{z \in \mathbb{F}_{2^{n/2}}} \zeta^{g(z)} + \zeta^{g(0)} 2^{n/2} \cdot \mathbf{1}_{\mathbb{F}_{2^{n/2}}}(a). \end{aligned}$$

Substituting $g(z) = \sum_{j=0}^{k-1} 2^j g_j(z)$ we have:

$$\begin{aligned} &\sum_{z \in \mathbb{F}_{2^{n/2}}} \zeta^{\sum_{j=0}^{k-1} 2^j g_j(z)} \sum_{y \in \mathbb{F}_{2^{n/2}}} (-1)^{\text{Tr}(a(z + \omega)^i y^i)} \\ &- \sum_{z \in \mathbb{F}_{2^{n/2}}} \zeta^{\sum_{i=0}^{k-1} 2^j g_j(z)} + \zeta^{g(0)} 2^{n/2} \cdot \mathbf{1}_{\mathbb{F}_{2^{n/2}}}(a). \end{aligned}$$

By [2, Lemma 1], if $a \notin \mathbb{F}_{2^n}$, then there exists a unique z such that $a(z + \omega)^i \in \mathbb{F}_{2^{n/2}}$, which in turn means that $\text{Tr}(a(z + \omega)^i y^i) = 0$, since $y^i \in \mathbb{F}_{2^{n/2}}$. Hence, the first term $\sum_z \zeta^{\sum_{j=0}^{k-1} 2^j g_j(z)} \sum_y (-1)^{\text{Tr}(a(z+\omega)^i y^i)}$ in the above expression equals $\zeta^\rho 2^{n/2}$ (for some positive integer ρ), if $a \notin \mathbb{F}_{2^{n/2}}$ and zero otherwise. Moreover, the second term $\sum_z \zeta^{\sum_{j=0}^{k-1} 2^j g_j(z)}$ equals zero by definition, and as previously stated, the last term $\zeta^{\sum_j 2^j g_j(0) \oplus \text{Tr}(ay^i)}$ equals $\zeta^{g(0)} 2^{n/2}$, if $a \in \mathbb{F}_{2^{n/2}}$ and zero otherwise. Therefore, we see that the entire previously displayed expression equals $\zeta^\rho 2^{n/2}$, for some integer ρ , regardless of whether $a \in \mathbb{F}_{2^{n/2}}$ or $a \notin \mathbb{F}_{2^{n/2}}$ and therefore, f is g -hyperbent. \square

More generally, one can generalize a classical construction of Boolean hyperbent functions as follows. We have the multiplicative decomposition $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^m}^* \times U$ where U is a cyclic subgroup of $\mathbb{F}_{2^n}^*$ of order $2^m + 1$, $m = \frac{n}{2}$. Let $f : \mathbb{V}_n \rightarrow \mathbb{Z}_{2^k}$ be such that f is constant on each coset $a\mathbb{F}_{2^m}^*$ for any $a \in U$. Then

Theorem 3.3. *Let $k \geq 3$. Then, f is g -hyperbent if and only if $\sum_{u \in U} \zeta_{2^k}^{f(u)} = \zeta_{2^k}^{f(0)}$.*

Proof.

$$\begin{aligned} \mathcal{H}_f^{(2^k)}(a) &= \sum_{x \in \mathbb{F}_{2^n}} \zeta_{2^k}^{f(x)} (-1)^{\text{Tr}_n(ax^i)} \\ &= \zeta_{2^k}^{f(0)} + \sum_{u \in U} \zeta_{2^k}^{f(u)} \sum_{y \in \mathbb{F}_{2^m}^*} (-1)^{\text{Tr}_n(au^i y^i)} \\ &= \zeta_{2^k}^{f(0)} - \sum_{u \in U} \zeta_{2^k}^{f(u)} + \sum_{u \in U} \zeta_{2^k}^{f(u)} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}_m(\text{Tr}_m^n(au^i) y^i)}. \end{aligned}$$

Now,

$$\sum_{y \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}_m(\text{Tr}_m^n(au^i) y^i)} = \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\text{Tr}_m(\text{Tr}_m^n(au^i) y)},$$

since $\gcd(i, 2^m - 1) = \gcd(i, 2^n - 1) = 1$. Observe that the equation $\text{Tr}_m^n(au^i) = au^i + a^{2^m} u^{-i} = 0$ has a unique solution u_a in U for every $a \neq 0$. Thus, if $a \neq 0$,

$$\mathcal{H}_f^{(2^k)}(a) = \zeta_{2^k}^{f(0)} - \sum_{u \in U} \zeta_{2^k}^{f(u)} + 2^m \zeta_{2^k}^{f(u_a)}.$$

On the other hand,

$$\mathcal{H}_f^{(2^k)}(0) = \zeta_{2^k}^{f(0)} - \sum_{u \in U} \zeta_{2^k}^{f(u)} + 2^m \sum_{u \in U} \zeta_{2^k}^{f(u)}. \quad (3)$$

Suppose that $\sum_{u \in U} \zeta_{2^k}^{f(u)} = \zeta_{2^k}^{f(0)}$. Then

$$\mathcal{H}_f^{(2^k)}(a) = 2^m \zeta_{2^k}^{f(u_a)} \quad \text{and} \quad \mathcal{H}_f^{(2^k)}(0) = 2^m \zeta_{2^k}^{f(0)}. \quad (4)$$

Conversely, suppose that f is g-hyperbent. Then, for $a \neq 0$,

$$\zeta_{2^k}^{f(0)} - \sum_{u \in U} \zeta_{2^k}^{f(u)} + 2^m \zeta_{2^k}^{f(u_a)} = 2^m \zeta_{2^k}^\rho$$

and

$$\zeta_{2^k}^{f(0)} - \sum_{u \in U} \zeta_{2^k}^{f(u)} + 2^m \sum_{u \in U} \zeta_{2^k}^{f(u)} = 2^m \zeta_{2^k}^\phi,$$

for some $\rho \in \mathbb{Z}_{2^k}$ and $\phi \in \mathbb{Z}_{2^k}$. Set $N_r^+ = |\{u \in U \mid f(u) = r\}|$, $N_r^- = |\{u \in U \mid f(u) = r + 2^{k-1}\}|$ and $N_r = N_r^+ - N_r^-$ for $r \in \mathbb{Z}_{2^{k-1}}$ and, for $e \in \mathbb{Z}_{2^k}$, $e = \mathbf{r}(e) + 2^{k-1}s(e)$. Then, equation (3) can be rewritten as

$$\begin{aligned} & \sum_{r \in \mathbb{Z}_{2^{k-1}} \setminus \{\mathbf{r}(\rho), \mathbf{r}(f(0)), \mathbf{r}(f(u_a))\}} N_r \zeta_{2^k}^r + \left(-N_{\mathbf{r}(f(u_a))} + 2^m (-1)^{s(f(u_a))} \right) \zeta_{2^k}^{\mathbf{r}(f(u_a))} \\ & + \left(-N_{\mathbf{r}(f(0))} + (-1)^{s(f(0))} \right) \zeta_{2^k}^{\mathbf{r}(f(0))} + \left(-N_{\mathbf{r}(\rho)} - 2^m (-1)^{s(\rho)} \right) \zeta_{2^k}^{\mathbf{r}(\rho)} = 0. \end{aligned}$$

Thus, since $\{\zeta_{2^k}^\rho, 0 \leq \rho \leq 2^{k-1} - 1\}$ is a basis of $\mathbb{Q}(\zeta_{2^k})$,

$$\begin{aligned} N_{\mathbf{r}} &= -N_{\mathbf{r}(f(u_a))} + 2^m (-1)^{s(f(u_a))} = -N_{\mathbf{r}(f(0))} + (-1)^{s(f(0))} \\ &= -N_{\mathbf{r}(\rho)} - 2^m (-1)^{s(\rho)} = 0, \end{aligned}$$

for every $r \in \mathbb{Z}_{2^{k-1}} \setminus \{\mathbf{r}(\rho), \mathbf{r}(f(0)), \mathbf{r}(f(u_a))\}$. Therefore

$$\begin{aligned} \sum_{u \in U} \zeta_{2^k}^{f(u)} &= \sum_{r \in \mathbb{Z}_{2^{k-1}}} N_r \zeta_{2^k}^r \\ &= 2^m (-1)^{s(f(u_a))} \zeta_{2^k}^{\mathbf{r}(f(u_a))} + (-1)^{s(f(0))} \zeta_{2^k}^{\mathbf{r}(f(0))} - 2^m (-1)^{s(\rho)} \zeta_{2^k}^{\mathbf{r}(\rho)}. \end{aligned}$$

Thus

$$\begin{aligned} & 2^m (-1)^{s(f(0))} \zeta_{2^k}^{\mathbf{r}(f(0))} - 2^m (-1)^{s(\phi)} \zeta_{2^k}^{\mathbf{r}(\phi)} \\ & + (2^n - 2^m) \left((-1)^{s(f(u_a))} \zeta_{2^k}^{f(u_a)} - (-1)^{s(\rho)} \zeta_{2^k}^\rho \right) = 0. \end{aligned}$$

Therefore, $\zeta_{2^k}^{f(0)} = \zeta_{2^k}^\phi$ and $\zeta_{2^k}^{f(u_a)} = \zeta_{2^k}^\rho$ proving that $\sum_{u \in U} \zeta_{2^k}^{f(u)} = \zeta_{2^k}^{f(0)}$. \square

4 Decomposition of gbent and g-hyperbent functions

Let $f \in \mathcal{GB}_n^{2^k}$ be a gbent function. In this section we continue analyzing the nature of Boolean and generalized Boolean functions in $\mathcal{GB}_n^{2^{k'}}$, $k' < k$, of which the gbent function f is (in some sense) composed.

Firstly, any function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^k}$ can be uniquely decomposed as

$$f(x) = \sum_{j=0}^{k-1} 2^j f_j,$$

where the f_j 's are Boolean functions. It has been recalled in Proposition 2.3 that, when n is even, if f is gbent then all its ‘‘components’’ f_j are bent functions. In fact, one can extend the previous results to g-hyperbent functions. To this end, we make some preliminary remarks that will help us in our analysis. Recall that when $\gcd(i, 2^n - 1) = 1$, then the extended Walsh transform of f is

$$\begin{aligned} \mathcal{H}_{f,i}^{(2^k)}(a) &= \sum_{x \in \mathbb{F}_{2^n}} \zeta_{2^k}^{f(x)} (-1)^{\text{Tr}_n(ax^i)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} \zeta_{2^k}^{f(x^j)} (-1)^{\text{Tr}_n(ax)} = \mathcal{H}_{f(x^j)}^{(2^k)}(a) \end{aligned}$$

where j is the inverse of i in \mathbb{Z}_{2^n-1} . Now, saying that f is g-hyperbent is equivalent to say that $f(\mathbf{x}^j)$ is g-bent for every j coprime with $2^n - 1$. Thus, for $k \geq 3$,

$$\mathcal{H}_{f,i}^{(2^k)}(a) = 2^{\frac{n}{2}} \zeta_{2^k}^\rho \tag{5}$$

for some $\rho \in \mathbb{Z}_{2^k}$. Now, Observe that

$$\zeta_{2^k}^{f(x)} = \prod_{j=0}^{k-1} \zeta_{2^k}^{2^j f_j(x)} = \prod_{j=0}^{k-1} \left(\frac{1 + \zeta_{2^k}^{2^j}}{2} + \frac{1 - \zeta_{2^k}^{2^j}}{2} (-1)^{f_j(x)} \right). \tag{6}$$

Set

$$\begin{aligned}
Q(X_1, \dots, X_{k-1}) &= \prod_{j=0}^{k-1} \left(\frac{1 + \zeta_{2^k}^{2^j}}{2} + \frac{1 - \zeta_{2^k}^{2^j}}{2} X_j \right) \\
&= 2^{-k} \prod_{j=0}^{k-1} \sum_{c \in \mathbb{F}_2} \left((1 + \zeta_{2^k}^{2^j + c 2^{k-1}}) X_j^c \right) \\
&= 2^{-k} \sum_{c \in \mathbb{F}_2^k} \left(\prod_{j=0}^{k-1} (1 + \zeta_{2^k}^{2^j + c_j 2^{k-1}}) \right) \prod_{j=0}^{k-1} X_j^{c_j}.
\end{aligned}$$

Set $A_c = 2^{-k} \prod_{j=0}^{k-1} (1 + \zeta_{2^k}^{2^j + c_j 2^{k-1}})$. Then

$$\zeta_{2^k}^{f(x)} = Q \left((-1)^{f_0(x)}, \dots, (-1)^{f_{k-1}(x)} \right) = \sum_{c \in \mathbb{F}_2^k} A_c (-1)^{\sum_{j=0}^{k-1} c_j f_j(x)}. \quad (7)$$

Then, we have the following theorem.

Theorem 4.1. *Let $f : \mathbb{V}_n \rightarrow \mathbb{Z}_{2^k}$, n even. Then f is a g -hyperbent function given as $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + \dots + 2^{k-1}a_k(\mathbf{x})$ if and only if, for each $\mathbf{c} \in \mathbb{F}_2^{k-1}$, the Boolean function $f_{\mathbf{c}}$ defined as*

$$f_{\mathbf{c}}(\mathbf{x}) = c_1 a_1(\mathbf{x}) \oplus c_2 a_2(\mathbf{x}) \oplus \dots \oplus c_{k-1} a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x})$$

is a hyperbent function.

Proof. Let i be coprime with $2^n - 1$. According to (7),

$$\begin{aligned}
\mathcal{H}_{f,i}^{(2^k)}(a) &= \sum_{x \in \mathbb{F}_{2^n}} \sum_{c \in \mathbb{F}_2^k} A_c (-1)^{\sum_{j=0}^{k-1} c_j f_j(x) + \text{Tr}_n(ax^i)} \\
&= \sum_{c \in \mathbb{F}_2^k} A_c \mathcal{W}_{f_{\mathbf{c}},i}(a).
\end{aligned}$$

Now,

$$\begin{aligned}
2^k A_c &= \prod_{j=0}^{k-1} \sum_{d \in \mathbb{Z}_2} \zeta_{2^k}^{d 2^j + d c_j 2^{k-1}} = \sum_{d \in \mathbb{F}_2^k} \zeta_{2^k}^{\sum_{j=0}^{k-1} d_j 2^j + d_j c_j 2^{k-1}} \\
&= \sum_{d \in \mathbb{F}_2^k} \zeta_{2^k}^{\sum_{j=0}^{k-2} d_j 2^j} (-1)^{\sum_{j=0}^{k-1} d_j c_j}.
\end{aligned}$$

Then

$$\begin{aligned}
2^k A_c &= \sum_{d \in \mathbb{F}_2^k} \zeta_{2^k}^{\sum_{j=0}^{k-2} d_j 2^j + 2^{k-1} d_{k-1}} (-1)^{\sum_{j=0}^{k-1} d_j c_j} \\
&= \left(\sum_{d_{k-1} \in \mathbb{F}_2} (-1)^{d_{k-1} + c_{k-1} d_{k-1}} \right) \sum_{(d_0, \dots, d_{k-2}) \in \mathbb{F}_2^{k-1}} \zeta_{2^k}^{\sum_{j=0}^{k-2} d_j 2^j} (-1)^{\sum_{j=0}^{k-2} d_j c_j} \\
&= \begin{cases} 0 & \text{if } c_{k-1} = 0, \\ 2 \sum_{(d_0, \dots, d_{k-2}) \in \mathbb{F}_2^{k-1}} \zeta_{2^k}^{\sum_{j=0}^{k-2} d_j 2^j} (-1)^{\sum_{j=0}^{k-2} d_j c_j} & \text{if } c_{k-1} = 1. \end{cases}
\end{aligned}$$

Define a “dot product” over \mathbb{F}_2^{k-1} by setting $c \cdot d = \sum_{j=0}^{k-2} c_j d_j$ for $c = (c_0, c_1, \dots, c_{k-2}) \in \mathbb{F}_2^{k-1}$ and $d = (d_0, d_1, \dots, d_{k-2}) \in \mathbb{F}_2^{k-1}$. Define the “canonical injection” $\iota : \mathbb{F}_2^{k-1} \rightarrow \mathbb{Z}_{2^{k-1}}$ by $\iota(c) = \sum_{j=0}^{k-2} c_j 2^j$ where $c = (c_0, c_1, \dots, c_{k-2})$. Then

$$\mathcal{H}_{f,i}^{(2^k)}(a) = \frac{1}{2^{k-1}} \sum_{(c,d) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \zeta_{2^k}^{\iota(d)} \mathcal{W}_{f,c,i}(a). \quad (8)$$

Suppose now that $f : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^k}$ is g-hyperbent, so for every i coprime with $2^n - 1$, we have

$$\mathcal{H}_{f,i}^{(2^k)}(a) = 2^{\frac{n}{2}} \zeta_{2^k}^{f_i^*(a)}$$

for some $f_i^* : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^k}$. Fix i coprime with $2^n - 1$ and decompose f_i^* as $f_i^* = g + 2^{k-1}s$ with $g : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^{k-1}}$ and $s : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ so that

$$\mathcal{H}_{f,i}^{(2^k)}(a) = 2^{\frac{n}{2}} (-1)^{s(a)} \zeta_{2^k}^{g(a)}.$$

Then,

$$\sum_{d \in \mathbb{F}_2^{k-1}} \left(\frac{1}{2^{k-1}} \sum_{c \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \mathcal{W}_{f,c,i}(a) \right) \zeta_{2^k}^{\iota(d)} - 2^{\frac{n}{2}} (-1)^{s(a)} \zeta_{2^k}^{g(a)} = 0. \quad (9)$$

Now, $\{1, \zeta_{2^k}, \dots, \zeta_{2^k}^{2^{k-1}-1}\}$ being a basis of $\mathbb{Q}(\zeta_{2^k})$,

$$\frac{1}{2^{k-1}} \sum_{c \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \mathcal{W}_{f,c,i}(a) = \begin{cases} 0 & \text{if } d \neq g(a) \\ 2^{\frac{n}{2}} (-1)^{s(a)} & \text{if } d = g(a). \end{cases} \quad (10)$$

Now, let us invert (10). We have for any $\mathbf{c} \in \mathbb{F}_2^{k-1}$

$$\begin{aligned}\mathcal{W}_{f_{\mathbf{c}},i}(a) &= \frac{1}{2^{k-1}} \sum_{(c,d) \in \mathbb{F}_2^{k-1}} (-1)^{(c+\mathbf{c}) \cdot d} \mathcal{W}_{f_{\mathbf{c}},i}(a) \\ &= \sum_{d \in \mathbb{F}_2^{k-1}} (-1)^{\mathbf{c} \cdot d} \left(\frac{1}{2^{k-1}} \sum_{\mathbf{c} \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \mathcal{W}_{f_{\mathbf{c}},i}(a) \right) \\ &= (-1)^{\mathbf{c} \cdot g(a) + s(a)} 2^{\frac{n}{2}},\end{aligned}$$

for every $a \in \mathbb{F}_{2^n}$. Since i is arbitrary in the preceding calculation, that shows that $f_{\mathbf{c}}$ is hyperbent.

Conversely, suppose that, for every $\gcd(i, 2^n - 1) = 1$, there exists $g_i : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^{k-1}}$ and $s_i : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ such that, for every $c \in \mathbb{F}_2^{k-1}$,

$$\mathcal{W}_{f_{\mathbf{c}},i}(a) = 2^{\frac{n}{2}} (-1)^{c \cdot \iota^{-1}(g_i(a)) + s_i(a)}.$$

Thus, for every $\gcd(i, 2^n - 1) = 1$, we have

$$\begin{aligned}\mathcal{H}_{f,i}^{(2^k)}(a) &= \frac{1}{2^{k-1}} \sum_{(c,d) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \zeta_{2^k}^{\iota(d)} \mathcal{W}_{f_{\mathbf{c}},i}(a) \\ &= 2^{\frac{n}{2}} \cdot \frac{1}{2^{k-1}} \cdot \sum_{(c,d) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{c \cdot d + c \cdot \iota^{-1}(g_i(a)) + s_i(a)} \zeta_{2^k}^{\iota(d)} \\ &= 2^{\frac{n}{2}} (-1)^{s_i(a)} \cdot \sum_{d \in \mathbb{F}_2^{k-1}} \left(\frac{1}{2^{k-1}} \sum_{\mathbf{c} \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot (d + \iota^{-1}(g_i(a)))} \right) \zeta_{2^k}^{\iota(d)} \\ &= 2^{\frac{n}{2}} (-1)^{s_i(a)} \zeta_{2^k}^{g_i(a)}\end{aligned}$$

proving that f is g -hyperbent. \square

Remark 4.2. *In the proof of Theorem 4.1, we have only used the fact that the Walsh transform of $f(\mathbf{x}^i)$ divided by its magnitude is a root of unity. The proof of Theorem 4.1 proposes therefore an alternate proof of (i) of Proposition 2.3. It also shows that the g -bentness of f is equivalent to the bentness of all the “component functions” $f_{\mathbf{c}}$.*

We now turn our attention to the case where n is odd and prove the following.

Theorem 4.3. Let $f : \mathbb{V}_n \rightarrow \mathbb{Z}_{2^k}$, n odd, be a gbent function given as $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + \cdots + 2^{k-1}a_k(\mathbf{x})$. If f is gbent then, for each $\mathbf{c} \in \mathbb{F}_2^{k-1}$, the Boolean function $g_{\mathbf{c}}$ defined as

$$g_{\mathbf{c}}(\mathbf{x}) = c_1 a_1(\mathbf{x}) \oplus c_2 a_2(\mathbf{x}) \oplus \cdots \oplus c_{k-1} a_{k-1}(\mathbf{x}) \oplus a_k(\mathbf{x})$$

is a semibent function.

Proof. We know that $2^{-\frac{n}{2}} \mathcal{H}_f^{(2^k)}(a)$ is a root of unity. Therefore, for every $a \in \mathbb{F}_{2^n}$,

$$\mathcal{H}_f^{(2^k)}(a) = 2^{\frac{n}{2}} \zeta_{2^k}^{f^*(a)} = 2^{\frac{n-1}{2}} \sqrt{2} \zeta_{2^k}^{f^*(a)},$$

for some map $f^* : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^k}$. Recall now that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_{2^k})$. Indeed, $\sqrt{2} = \zeta_8 + \bar{\zeta}_8 = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7 = \zeta_8 - \zeta_8^3 = \zeta_{2^k}^{2^{k-3}} - \zeta_{2^k}^{3 \cdot 2^{k-3}}$. Thus

$$\mathcal{H}_f^{(2^k)}(a) = 2^{\frac{n-1}{2}} \left(\zeta_{2^k}^{f^*(a)+2^{k-3}} - \zeta_{2^k}^{f^*(a)+3 \cdot 2^{k-3}} \right).$$

Write $f^*(a) + 2^{k-3} = g_1(a) + 2^{k-1}s_2(a) + 2^k t_1(a)$ and $f^*(a) + 3 \cdot 2^{k-3} = g_2(a) + 2^{k-1}s_2(a) + 2^k t_2(a)$ so that

$$\mathcal{H}_f^{(2^k)}(a) = 2^{\frac{n-1}{2}} (-1)^{s_1(a)} \zeta_{2^k}^{g_1(a)} - 2^{\frac{n-1}{2}} (-1)^{s_2(a)} \zeta_{2^k}^{g_2(a)}.$$

In the proof of Theorem 4.1, we have established the following relation between the Walsh-Hadamard transform of f and the Walsh transform of its ‘‘component’’ $f_{\mathbf{c}}$ (take $i = 1$ in (11) and recall that ι is the ‘‘canonical’’ injection from \mathbb{F}_2^{k-1} to $\mathbb{Z}_{2^{k-1}}$ which sends (c_0, \dots, c_{k-2}) to $\sum_{j=0}^{k-2} c_j 2^j$), namely,

$$\mathcal{H}_f^{(2^k)}(a) = \frac{1}{2^{k-1}} \sum_{(c,d) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \zeta_{2^k}^{\iota(d)} \cdot \mathcal{W}_{f_{\mathbf{c}}}(a) \quad (11)$$

$$= \sum_{d \in \mathbb{F}_2^{k-1}} \left(\frac{1}{2^{k-1}} \sum_{c \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \mathcal{W}_{f_{\mathbf{c}}}(a) \right) \zeta_{2^k}^{\iota(d)}. \quad (12)$$

Then, one has

$$\frac{1}{2^{k-1}} \sum_{c \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \mathcal{W}_{f_{\mathbf{c}}}(a) = \begin{cases} 0 & \text{if } d \notin \{g_1(a), g_2(a)\} \\ 2^{\frac{n-1}{2}} (-1)^{s_1(a)} & \text{if } d = g_1(a) \\ -2^{\frac{n-1}{2}} (-1)^{s_2(a)} & \text{if } d = g_2(a). \end{cases} \quad (13)$$

Thus

$$\begin{aligned}
\mathcal{W}_{f_{\mathbf{c}}}(a) &= \frac{1}{2^{k-1}} \sum_{(c,d) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{(c+\mathbf{c}) \cdot d} \mathcal{W}_{f_{\mathbf{c}}}(a) \\
&= \sum_{d \in \mathbb{F}_2^{k-1}} (-1)^{\mathbf{c} \cdot d} \frac{1}{2^{k-1}} \sum_{c \in \mathbb{F}_2^{k-1}} (-1)^{c \cdot d} \mathcal{W}_{f_{\mathbf{c}}}(a) \\
&= \frac{(-1)^{\mathbf{c} \cdot g_1(a) + s_1(a)} - (-1)^{\mathbf{c} \cdot g_2(a) + s_2(a)}}{2} 2^{\frac{n+1}{2}}
\end{aligned}$$

proving that $f_{\mathbf{c}}$ is semibent since

$$\frac{(-1)^{\mathbf{c} \cdot g_1(a) + s_1(a)} - (-1)^{\mathbf{c} \cdot g_2(a) + s_2(a)}}{2} \in \{-1, 0, 1\}$$

for every $a \in \mathbb{F}_{2^n}$. □

In the following proposition we decompose a gbent function in $\mathcal{GB}_n^{2^k}$ into two gbent functions in $\mathcal{GB}_n^{2^{k'}}$ for some k' smaller than k . We will show the decomposition more general for g-hyperbent functions, where we consider functions from \mathbb{F}_{2^n} to \mathbb{Z}_{2^k} . The crucial lemma for analyzing the decomposition of f when n is even, is Lemma 2.1. For instance the proof of Proposition 2.3 (i) is based on this lemma.

We intend to show our results on decompositions of gbent functions for n even and for n odd simultaneously. Therefore we first deduce a more complex analog of Lemma 2.1 which is applicable to gbent functions in an odd number of variables.

For $k \geq 3$, let again ζ_{2^k} be a primitive 2^k -root of unity. Then $\zeta_{2^k}^{2^{k-3}}$ is a primitive 2^3 -root of unity, and without loss of generality, we assume that $\zeta_{2^k}^{2^{k-3}} = \zeta_{2^3} = (1+i)/\sqrt{2}$. Recall that for $k \geq 3$ every gbent function is regular, i.e. for an integer $0 \leq \rho_{\mathbf{u}} \leq 2^k - 1$ (depending on \mathbf{u}) we have

$$\begin{aligned}
\mathcal{H}_f^{(2^k)}(\mathbf{u}) &= 2^{n/2} \zeta_{2^k}^{\rho_{\mathbf{u}}} = 2^{n/2} \zeta_{2^k}^{2^{k-3}} \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} \\
&= 2^{\frac{n-1}{2}} (1+i) \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} \\
&= 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} + 2^{\frac{n-1}{2}} \zeta_{2^k}^{2^{k-2}} \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} \\
&= 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} + 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-3}}.
\end{aligned}$$

Proposition 4.4. *For an odd integer n and $k \geq 3$, let f be a function from \mathbb{V}_n to \mathbb{Z}_{2^k} , for $\mathbf{u} \in \mathbb{V}_n$ let $f_{\mathbf{u}}(\mathbf{x}) = f(\mathbf{x}) + 2^{k-1}(\mathbf{u} \cdot \mathbf{x})$, and let $B_{\mathbf{u}}(\rho) = \{\mathbf{x} \in$*

$\mathbb{V}_n : f_{\mathbf{u}}(\mathbf{x}) = \rho\}$. Then f is gbent if and only if for all $\mathbf{u} \in \mathbb{V}_n$ there exists an integer $\rho_{\mathbf{u}}$, $0 \leq \rho_{\mathbf{u}} \leq 2^k - 1$, such that

$$|B_{\mathbf{u}}(\rho_{\mathbf{u}} - 2^{k-3} + 2^{k-1})| = |B_{\mathbf{u}}(\rho_{\mathbf{u}} - 2^{k-3})| \pm 2^{\frac{n-1}{2}}$$

and

$$|B_{\mathbf{u}}(\rho_{\mathbf{u}} + 2^{k-3} + 2^{k-1})| = |B_{\mathbf{u}}(\rho_{\mathbf{u}} + 2^{k-3})| \pm 2^{\frac{n-1}{2}}$$

where in both equations we have the same sign (and the argument of $B_{\mathbf{u}}$ is reduced modulo 2^k), and

$$|B_{\mathbf{u}}(\rho + 2^{k-1})| = |B_{\mathbf{u}}(\rho)|,$$

if $\rho \neq \rho_{\mathbf{u}} \pm 2^{k-3}, \rho_{\mathbf{u}} \pm 2^{k-3} + 2^{k-1}$.

Proof. Let f be a function from \mathbb{V}_n to \mathbb{Z}_{2^k} for which the conditions in the proposition hold. For $\mathbf{u} \in \mathbb{V}_n$, the generalized Walsh-Hadamard transform at \mathbf{u} is then

$$\begin{aligned} \mathcal{H}_f^{(2^k)}(\mathbf{u}) &= \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^k}^{f_{\mathbf{u}}(\mathbf{x})} = \sum_{\rho=0}^{2^k-1} |B_{\mathbf{u}}(\rho)| \zeta_{2^k}^{\rho} \\ &= (|B_{\mathbf{u}}(\rho_{\mathbf{u}} - 2^{k-3})| - (|B_{\mathbf{u}}(\rho_{\mathbf{u}} - 2^{k-3})| \pm 2^{\frac{n-1}{2}})) \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} \\ &\quad + (|B_{\mathbf{u}}(\rho_{\mathbf{u}} + 2^{k-3})| - (|B_{\mathbf{u}}(\rho_{\mathbf{u}} + 2^{k-3})| \pm 2^{\frac{n-1}{2}})) \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-3}} \\ &= \pm 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} \pm 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-3}} = 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}}} \zeta_{2^k}^{2^{k-3}} (\pm i \pm 1) \\ &= 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}}} \frac{1+i}{\sqrt{2}} (\pm i \pm 1) = 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}}} \frac{1+i}{\sqrt{2}} \alpha. \end{aligned}$$

(Here the arguments of $B_{\mathbf{u}}$ are reduced modulo 2^k .) With $\frac{1+i}{\sqrt{2}}(1+i) = \sqrt{2}i = \sqrt{2}\zeta_{2^k}^{2^{k-2}}$, we get $\mathcal{H}_f^{(2^k)}(\mathbf{u}) = 2^{n/2} \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-2}}$ when $\alpha = 1+i$. Similarly, when $\alpha = -1-i$, $\alpha = 1-i$, respectively $\alpha = -1+i$, for $\mathcal{H}_f^{(2^k)}(\mathbf{u})$ we obtain $2^{n/2} \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-2} + 2^{k-1}}$, $2^{n/2} \zeta_{2^k}^{\rho_{\mathbf{u}}}$, respectively $2^{n/2} \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-1}}$. Therefore f is gbent.

Conversely suppose that f is gbent. As observed above, for $\mathbf{u} \in \mathbb{V}_n$ we then have

$$\mathcal{H}_f^{(2^k)}(\mathbf{u}) = 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} - 2^{k-3}} + 2^{\frac{n-1}{2}} \zeta_{2^k}^{\rho_{\mathbf{u}} + 2^{k-3}}, \quad (14)$$

for some $0 \leq \rho_{\mathbf{u}} \leq 2^k - 1$ depending on \mathbf{u} . By the definition of $B_{\mathbf{u}}(\rho)$ we

moreover have

$$\begin{aligned}
\mathcal{H}_f^{(2^k)}(\mathbf{u}) &= |B_{\mathbf{u}}(0)| + |B_{\mathbf{u}}(1)|\zeta_{2^k} + \cdots + |B_{\mathbf{u}}(2^{k-1} - 1)|\zeta_{2^k}^{2^{k-1}-1} \\
&\quad + |B_{\mathbf{u}}(2^{k-1})|(-1) + |B_{\mathbf{u}}(2^{k-1} + 1)|\zeta_{2^k}^{2^{k-1}+1} + \cdots + |B_{\mathbf{u}}(2^k - 1)|\zeta_{2^k}^{2^k-1} \\
&= (|B_{\mathbf{u}}(0)| - |B_{\mathbf{u}}(2^{k-1})|) + (|B_{\mathbf{u}}(1)| - |B_{\mathbf{u}}(2^{k-1} + 1)|)\zeta_{2^k} + \cdots \\
&\quad + (|B_{\mathbf{u}}(2^{k-1} - 1)| - |B_{\mathbf{u}}(2^k - 1)|)\zeta_{2^k}^{2^{k-1}-1}. \tag{15}
\end{aligned}$$

Since $\{1, \zeta_{2^k}, \dots, \zeta_{2^k}^{2^{k-1}-1}\}$ is a basis of $\mathbb{Q}(\zeta_{2^k})$, the conditions in the proposition follow from equations (14) and (15). \square

Let us now explain how to deduce from Proposition 4.4 a first result. We include the hyperbent condition only in the first part of the proof of the following proposition. As we will see, including this condition does not change the arguments, hence we will omit it in the further, although the decomposition results also hold for g-hyperbent functions.

Proposition 4.5. *Let $k \geq 2t$, and let $f : \mathbb{F}_{2^n} \rightarrow \mathbb{Z}_{2^k}$ be a g-hyperbent function given as*

$$f(x) = a_1(x) + 2a_2(x) + \cdots + 2^{k-1}a_k(x) = g(x) + 2^t h(x)$$

for some Boolean functions $a_i : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$, $1 \leq i \leq k$, and

$$\begin{aligned}
g(x) &= a_1(x) + 2a_2(x) + \cdots + 2^{t-1}a_t(x) \in \mathcal{GB}_n^{2^t}, \\
h(x) &= a_{t+1}(x) + 2a_{t+2}(x) + \cdots + 2^{k-t-1}a_k(x) \in \mathcal{GB}_n^{2^{k-t}}.
\end{aligned}$$

If n is even or $k \geq 3$, then the functions $h(x)$ and $h(x) + 2^{k-2t}g(x)$ are g-hyperbent functions in $\mathcal{GB}_n^{2^{k-t}}$.

Proof. For an integer i , $\gcd(i, 2^n - 1) = 1$, and an element $u \in \mathbb{V}_n = \mathbb{F}_{2^n}$, let $f_{u,i}(x) = f(x) + 2^{k-1}\text{Tr}_n(ux^i)$, $h_{u,i}(x) = h(x) + 2^{k-t-1}\text{Tr}_n(ux^i)$, and for $0 \leq e \leq 2^t - 1$, $0 \leq r \leq 2^{k-t} - 1$, denote by $S^{(u,i)}(e, r)$ the set

$$S^{(u,i)}(e, r) = \{x : f_{u,i}(x) = e + 2^t r\} = \{x : g(x) = e, h_{u,i}(x) = r\}.$$

First we suppose that n is even. Then, since f is g-hyperbent, by an obvious version of Lemma 2.1 for g-hyperbent functions, for $0 \leq e \leq 2^t - 1$ and $0 \leq \tilde{r} \leq 2^{k-t-1} - 1$ we have

$$|S^{(u,i)}(e, \tilde{r})| = |S^{(u,i)}(e, \tilde{r} + 2^{k-t-1})|$$

for all but one pair, say the pair $(e, \tilde{r}) = (\epsilon_{u,i}, \rho_{u,i})$, for which we have

$$|S^{(u,i)}(\epsilon_{u,i}, \rho_{u,i} + 2^{k-t-1})| = |S^{(u,i)}(\epsilon_{u,i}, \rho_{u,i})| \pm 2^{n/2}.$$

Consequently,

$$\begin{aligned} \mathcal{H}_{h,i}^{(2^{k-t})}(u) &= \sum_{x \in \mathbb{V}_n} \zeta_{2^{k-t}}^{h(x) + 2^{k-t-1} \text{Tr}_n(ux^i)} = \sum_{x \in \mathbb{V}_n} \zeta_{2^{k-t}}^{h_{u,i}(x)} \\ &= \sum_{\substack{0 \leq e \leq 2^t - 1 \\ 0 \leq r \leq 2^{k-t} - 1}} |S^{(u,i)}(e, r)| \zeta_{2^{k-t}}^r \\ &= \sum_{\substack{0 \leq e \leq 2^t - 1 \\ 0 \leq \tilde{r} \leq 2^{k-t-1} - 1}} \left[|S^{(u,i)}(e, \tilde{r})| - |S^{(u,i)}(e, \tilde{r} + 2^{k-t-1})| \right] \zeta_{2^{k-t}}^{\tilde{r}} \\ &= \pm 2^{n/2} \zeta_{2^{k-t}}^{\rho_{u,i}}, \end{aligned}$$

hence h is g -hyperbent. For $h + 2^{k-2t}g$ we have

$$\begin{aligned} \mathcal{H}_{h+2^{k-2t}g,i}^{(2^{k-t})}(u) &= \sum_{x \in \mathbb{V}_n} \zeta_{2^{k-t}}^{h_{u,i}(x) + 2^{k-2t}g(x)} \\ &= \sum_{\substack{0 \leq e \leq 2^t - 1 \\ 0 \leq \tilde{r} \leq 2^{k-t-1} - 1}} \left[|S^{(u,i)}(e, \tilde{r})| - |S^{(u,i)}(e, \tilde{r} + 2^{k-t-1})| \right] \zeta_{2^{k-t}}^{\tilde{r} + 2^{k-2t}e} \\ &= \pm 2^{n/2} \zeta_{2^{k-t}}^{\rho_{u,i} + 2^{k-2t}\epsilon_u}, \end{aligned}$$

and hence $h + 2^{k-2t}g$ is g -hyperbent.

Now suppose that n is odd and $k \geq 3$. Let $f_u(x) = f(x) + 2^{k-1} \text{Tr}_n(ux)$, $h_u(x) = h(x) + 2^{k-t-1} \text{Tr}_n(ux)$, $S^{(u)}(e, r) = \{x : f_u(x) = e + 2^t r\} = \{x : g(x) = e, h_u(x) = r\}$. If f is g bent, by Proposition 4.4 there exist two integers

$$\begin{aligned} \rho_u^{(1)} &= \epsilon_{u,1} + 2^t \rho_{u,1} = \rho_u - 2^{k-3}, \\ \rho_u^{(2)} &= \epsilon_{u,2} + 2^t \rho_{u,2} = \rho_u + 2^{k-3}, \end{aligned}$$

where $0 \leq \epsilon_{u,j} \leq 2^t - 1$, $0 \leq \rho_{u,j} \leq 2^{k-t-1} - 1$, $j = 1, 2$, such that

$$|S^u(\epsilon_{u,j}, \rho_{u,j} + 2^{k-t-1})| = |S^u(\epsilon_{u,j}, \rho_{u,j})| \pm 2^{\frac{n-1}{2}}, \quad j = 1, 2.$$

For $(e, r) \neq (\epsilon_{u,j}, \rho_{u,j})$ we have

$$|S^u(e, r + 2^{k-t-1})| = |S^u(e, r)|.$$

Observe that $\rho_u^{(2)} - \rho_u^{(1)} = \epsilon_{u,2} - \epsilon_{u,1} + 2^t(\rho_{u,2} - \rho_{u,1}) = 2^{k-2}$, therefore $2^t |(\epsilon_{u,2} - \epsilon_{u,1})|$, and consequently $\epsilon_{u,2} = \epsilon_{u,1}$ and $\rho_{u,2} - \rho_{u,1} = 2^{k-t-2}$. For the generalized Walsh-Hadamard transform of h we then get

$$\begin{aligned} \mathcal{H}_h^{(2^{k-t})}(u) &= \sum_{x \in \mathbb{V}_n} \zeta_{2^{k-t}}^{h_u(x)} = \sum_{\substack{0 \leq e \leq 2^t - 1 \\ 0 \leq r \leq 2^{k-t} - 1}} |S^{(u)}(e, r)| \zeta_{2^{k-t}}^r = 2^{\frac{n-1}{2}} (\pm \zeta_{2^{k-t}}^{\rho_{u,1}} \pm \zeta_{2^{k-t}}^{\rho_{u,2}}) \\ &= 2^{\frac{n-1}{2}} (\pm \zeta_{2^{k-t}}^{\rho_{u,1}} \pm \zeta_{2^{k-t}}^{\rho_{u,1}} \zeta_{2^{k-t}}^{2^{k-t-2}}) = 2^{\frac{n-1}{2}} \zeta_{2^{k-t}}^{\rho_{u,1}} (\pm 1 \pm i), \end{aligned}$$

hence h is gbent. For $h + 2^{k-2t}g$, using that $\epsilon_{u,2} = \epsilon_{u,1} := \epsilon_u$ we obtain

$$\begin{aligned} \mathcal{H}_{h+2^{k-2t}g}^{(2^{k-t})}(u) &= \sum_{x \in \mathbb{V}_n} \zeta_{2^{k-t}}^{h_u(x) + 2^{k-2t}g(x)} \\ &= 2^{\frac{n-1}{2}} (\pm \zeta_{2^{k-t}}^{\rho_{u,1} + 2^{k-2t}\epsilon_u} \pm \zeta_{2^{k-t}}^{\rho_{u,2} + 2^{k-2t}\epsilon_u}) \\ &= 2^{\frac{n-1}{2}} \zeta_{2^{k-t}}^{\rho_{u,1} + 2^{k-2t}\epsilon_u} (\pm 1 \pm i), \end{aligned}$$

and hence $h + 2^{k-2t}g$ is gbent. \square

With Proposition 4.5 we can conclude the equivalence of the conditions in Theorem 2.5 also for odd n . We use multivariate notation, but keep in mind that many results also apply to g-hyperbent functions, which are only defined when $\mathbb{V}_n = \mathbb{F}_{2^n}$.

Corollary 4.6. *Let $f \in \mathcal{GB}_n^{2^k}$ with $f(\mathbf{x}) = g(\mathbf{x}) + 2h(\mathbf{x})$, $g \in \mathcal{B}_n$, $h \in \mathcal{GB}_n^{2^{k-1}}$. Let n be even or $k \geq 3$, 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 $\mathbf{u} \in \mathbb{V}_n$.

Proof. For even n , the corollary is Theorem 2.5. By Remark 2.6, for odd n it suffices to show that h and $h + 2^{k-2}g$ are both gbent in $\mathcal{GB}_n^{2^{k-1}}$ if f is gbent in $\mathcal{GB}_n^{2^k}$. This follows for $k \geq 3$ from Proposition 4.5 with $t = 1$. \square

We can now show one of our main theorems about the decomposition of g-(hyper)bent functions. Proposition 2.3(i), that is, Theorem 18 in [8], will also follow from this theorem as a special case.

Theorem 4.7. Let $f \in \mathcal{GB}_n^{2^k}$, $k \geq 2$, with $f(\mathbf{x}) = a_1(\mathbf{x}) + 2a_2(\mathbf{x}) + \cdots + 2^{k-1}a_k(\mathbf{x})$, $a_i \in \mathcal{B}_n$, $1 \leq i \leq k$, be a gbent function. Let $1 \leq s \leq k$, and let $\mathbf{c} \in \mathbb{F}_2^{s-1}$. The function

$$g_{\mathbf{c}}(x) = a_s + 2a_{s+1} + \cdots + 2^{k-s} \left(\bigoplus_{i=1}^{s-1} c_i a_i \oplus a_k \right)$$

is a gbent function in $\mathcal{GB}_n^{2^{k-s+1}}$ if

- n is even,
- n is odd and $s < k$.

Moreover, for $\mathbf{c}_0 = (c_1, \dots, c_{s-2}, 0)$, $\mathbf{c}_1 = (c_1, \dots, c_{s-2}, 1)$ we have

$$\mathcal{H}_{g_{\mathbf{c}_1}}(\mathbf{u}) = \pm \mathcal{H}_{g_{\mathbf{c}_0}}(\mathbf{u}),$$

for all $\mathbf{u} \in \mathbb{V}_n$.

If n is odd and $s = k$ (hence $g_{\mathbf{c}}$ is Boolean), then $g_{\mathbf{c}}$ is semibent.

Proof. We show the result by induction. If $s = 1$, the claim is obvious. If $s = 2$, by taking $g := a_1$, $h := a_2 + 2a_3 + \cdots + 2^{k-2}a_k$, the claim follows from Corollary 4.6, since then f is gbent if and only if both $h = a_2 + 2a_3 + \cdots + 2^{k-2}a_k$, $h + 2^{k-2}g = a_2 + 2a_3 + \cdots + 2^{k-2}(a_1 \oplus a_k)$ are gbent and $\mathcal{H}_h(\mathbf{u}) = \pm \mathcal{H}_{h+2^{k-2}g}(\mathbf{u})$, for all \mathbf{u} . Assume the result is true for some $s \leq k-1$, i.e., $g_{\mathbf{c}}(\mathbf{x}) = a_s + 2a_{s+1} + \cdots + 2^{k-s} \left(\bigoplus_{i=1}^{s-1} c_i a_i \oplus a_k \right)$ is a gbent function in $\mathcal{GB}_n^{2^{k-s+1}}$ for all $\mathbf{c} = (c_1, \dots, c_{s-1}) \in \mathbb{F}_2^{s-1}$. We show that it then also holds for $s+1$. We apply Corollary 4.6 to $g_{\mathbf{c}} \in \mathcal{GB}_n^{2^{k-s+1}}$. Note that we therefore require $k-s+1 \geq 3$, i.e., $s \leq k-2$, if n is odd. We obtain that for $(\mathbf{c}, 0)$ and $(\mathbf{c}, 1)$ in \mathbb{F}_2^{s-1} , both

$$g_{(\mathbf{c},0)} = a_{s+1} + 2a_{s+2} + \cdots + 2^{k-s-1} \left(\bigoplus_{i=1}^{s-1} c_i a_i \oplus a_k \right)$$

and

$$g_{(\mathbf{c},1)} = a_{s+1} + 2a_{s+2} + \cdots + 2^{k-s-1} \left(\bigoplus_{i=1}^{s-1} c_i a_i \oplus a_s \oplus a_k \right)$$

are gbent functions in $\mathcal{GB}_n^{2^{k-s}}$. Therefore $g_{\mathbf{c}} \in \mathcal{GB}_n^{2^{k-s}}$ is gbent for every $\mathbf{c} \in \mathbb{F}_2^s$, $1 \leq s \leq k$ when n is even, and $1 \leq s \leq k-1$ when n is odd. Moreover, again applying Corollary 4.6, we get

$$\mathcal{H}_{g_{(\mathbf{c},1)}}(\mathbf{u}) = \pm \mathcal{H}_{g_{(\mathbf{c},0)}}(\mathbf{u}),$$

for all $\mathbf{u} \in \mathbb{V}_n$. By Theorem 4.3, if n is odd and $s = k$ then for every $\mathbf{c} \in \mathbb{F}_2^{s-1}$ the Boolean function $g_{\mathbf{c}}$ is semibent. \square

Remark 4.8. *If, conversely, $\mathcal{H}_{g(\mathbf{c},1)}(\mathbf{u}) = \pm \mathcal{H}_{g(\mathbf{c},0)}(\mathbf{u})$ holds for all $\mathbf{u} \in \mathbb{V}_n$ and $\mathbf{c} \in \mathbb{F}_2^{s-1}$, by Corollary 4.6, all functions $g_{\mathbf{c}}(\mathbf{x}) = a_s(\mathbf{x}) + 2a_{s+1}(\mathbf{x}) + \dots + 2^{k-s} \left(\bigoplus_{i=1}^{s-1} c_i a_i(\mathbf{x}) \oplus a_k(\mathbf{x}) \right) \in \mathcal{GB}_n^{2^{k-s+1}}$ are gbent. However, we have to impose the analog property for this set of gbent functions for the next step.*

We finish with a decomposition of gbent functions in $\mathcal{GB}_n^{2^t}$ into gbent functions in $\mathcal{GB}_n^{2^t}$. The following theorem generalizes both, Proposition 2.3(i), [8, Theorem 12] and partially Theorem 4.1. To this end, let us introduce additional notation and present some facts that shall help us in our analysis. The core of the proof of Theorem 4.1 is (6) which simply expresses the following decomposition of $\zeta_{2^k}^{2^j \alpha}$ for $\alpha \in \{0, 1\}$ with respect to $\{1, \zeta_2 = -1\}$. In fact, equation (6) is simply a particular case. Indeed, one can express more generally $\zeta_{2^k}^{2^j \alpha}$, $\alpha \in \mathbb{Z}_{2^t}$, with respect to $\{1, \dots, \zeta_{2^t}\}$ if t is a divisor of k . Let $\mathcal{V}_{2^t}(\zeta_{2^t})$ and $\mathcal{V}_{2^t}(\zeta_{2^t}^{-1})$ be the $2^t \times 2^t$ Vandermonde matrices :

$$\mathcal{V}_{2^t}(\zeta_{2^t}) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \zeta_{2^t} & & \zeta_{2^t}^{2^t-1} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta_{2^t}^{2^t-1} & & \zeta_{2^t}^{(2^t-1)(2^t-1)} \end{pmatrix}$$

and

$$\mathcal{V}_{2^t}(\zeta_{2^t}^{-1}) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \zeta_{2^t}^{-1} & & \zeta_{2^t}^{-(2^t-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \zeta_{2^t}^{-(2^t-1)} & & \zeta_{2^t}^{-(2^t-1)(2^t-1)} \end{pmatrix}.$$

Observe that

$$\mathcal{V}_{2^t}(\zeta_{2^t}) \mathcal{V}_{2^t}(\zeta_{2^t}^{-1}) = 2^t \mathbf{I}_{2^t}, \quad (16)$$

where \mathbf{I}_{2^t} stands for the identity matrix of size 2^t . Define now a collection of maps from \mathbb{C} to itself by setting

$$\begin{pmatrix} h_0(z) \\ h_1(z) \\ \vdots \\ h_{2^t-1}(z) \end{pmatrix} = \mathcal{V}_{2^t}(\zeta_{2^t}^{-1}) \begin{pmatrix} 1 \\ z \\ \vdots \\ z^{2^t-1} \end{pmatrix}$$

or equivalently, for any $\alpha \in \mathbb{Z}_{2^t}$,

$$h_\alpha(z) = \sum_{\beta \in \mathbb{Z}_{2^t}} \zeta_{2^t}^{-\alpha\beta} z^\beta. \quad (17)$$

Furthermore, according to (16), one has, for any $z \in \mathbb{C}$,

$$\begin{pmatrix} 1 \\ z \\ \vdots \\ z^{2^t-1} \end{pmatrix} = \frac{1}{2^t} \mathcal{V}_{2^t}(\zeta_{2^t}) \begin{pmatrix} h_0(z) \\ h_1(z) \\ \vdots \\ h_{2^t-1}(z) \end{pmatrix} \quad (18)$$

that is, for $\beta \in \mathbb{Z}_{2^t}$,

$$z^\beta = \frac{1}{2^t} \sum_{\alpha \in \mathbb{Z}_{2^t}} \zeta_{2^t}^{\alpha\beta} h_\alpha(z). \quad (19)$$

Then, we show the next theorem.

Theorem 4.9. *Let n be even. Let $k = lt$ and let $f \in \mathcal{GB}_n^{2^k}$ be a g -hyperbent function given as*

$$f(\mathbf{x}) = b_1(\mathbf{x}) + 2^t b_2(\mathbf{x}) + \cdots + 2^{(l-1)t} b_l(\mathbf{x}),$$

for some functions $b_i \in \mathcal{GB}_n^{2^t}$, $1 \leq i \leq l$. If n is even or $t \geq 2$, then for every $\mathbf{c} = (c_1, c_2, \dots, c_{l-1}) \in \mathbb{Z}_{2^t}^{l-1}$, the function

$$g_{\mathbf{c}}(\mathbf{x}) = c_1 b_1(\mathbf{x}) + \cdots + c_{l-1} b_{l-1}(\mathbf{x}) + b_l(\mathbf{x}) \in \mathcal{GB}_n^{2^t}$$

is g -hyperbent.

Proof. The extended Hadamard-Walsh transform of f is :

$$\mathcal{H}_{f,i}^{(2^k)}(a) = \sum_{x \in \mathbb{F}_{2^n}} \zeta_{2^k}^{f(x)} (-1)^{\text{Tr}_n(ax^i)}. \quad (20)$$

Using (17) and (19), one gets

$$\begin{aligned} \zeta_{2^k}^{f(x)} &= \zeta_{2^t}^{b_l(x)} \prod_{j=1}^{l-1} \zeta_{2^k}^{2^{(j-1)t} b_j(x)} = \zeta_{2^t}^{b_l(x)} \prod_{j=1}^{l-1} \left(\frac{1}{2^t} \sum_{c_j \in \mathbb{Z}_{2^t}} \zeta_{2^t}^{c_j b_j(x)} h_{c_j} \left(\zeta_{2^k}^{2^{(j-1)t}} \right) \right) \\ &= \zeta_{2^t}^{b_l(x)} \prod_{j=1}^{l-1} \left(\frac{1}{2^t} \sum_{c_j \in \mathbb{Z}_{2^t}} \zeta_{2^t}^{c_j b_j(x)} \sum_{d_j \in \mathbb{Z}_{2^t}} \zeta_{2^t}^{-c_j d_j} \zeta_{2^k}^{2^{(j-1)t} d_j} \right) \\ &= \zeta_{2^t}^{b_l(x)} \prod_{j=1}^{l-1} \left(\frac{1}{2^t} \sum_{(c_j, d_j) \in \mathbb{Z}_{2^t}^2} \zeta_{2^t}^{c_j (b_j(x) - d_j)} \zeta_{2^k}^{2^{(j-1)t} d_j} \right). \end{aligned}$$

Therefore,

$$\begin{aligned}\zeta_{2^k}^{f(x)} &= \zeta_{2^t}^{b_l(x)} \times \frac{1}{2^{k-t}} \sum_{(c,d) \in \mathbb{Z}_{2^t}^{l-1} \times \mathbb{Z}_{2^t}^{l-1}} \zeta_{2^k}^{\sum_{j=1}^{l-1} 2^{(j-1)t} d_j} \zeta_{2^t}^{\sum_{j=0}^{l-1} c_j (b_j(x) - d_j)} \\ &= \frac{1}{2^{k-t}} \sum_{(c,d) \in \mathbb{Z}_{2^t}^{l-1} \times \mathbb{Z}_{2^t}^{l-1}} \zeta_{2^k}^{\sum_{j=1}^{l-1} 2^{(j-1)t} d_j} \zeta_{2^t}^{g_c(x) - c \cdot d},\end{aligned}$$

where $c \cdot d = \sum_{j=1}^{l-1} c_j d_j$. If we use the above relation in (20), then

$$\mathcal{H}_{f,i}^{(2^k)}(a) = \frac{1}{2^{k-t}} \sum_{(c,d) \in \mathbb{Z}_{2^t}^{l-1} \times \mathbb{Z}_{2^t}^{l-1}} \zeta_{2^t}^{-c \cdot d} \zeta_{2^k}^{\sum_{j=1}^{l-1} 2^{(j-1)t} d_j} \mathcal{W}_{f_c, i}(a). \quad (21)$$

At this stage, observe that (21) generalizes (11) (which corresponds to $t = 1$). It is then quite straightforward to repeat the arguments of the proof of Theorem 4.1 to get Theorem 4.5. \square

5 Conclusion

In this paper we extend the concept of a hyperbent function to generalized Boolean functions from \mathbb{F}_{2^n} to \mathbb{Z}_{2^k} , and we present examples of generalized hyperbent functions obtained with partial spreads. We investigate decompositions of generalized (hyper)bent functions (gbent respectively g-hyperbent functions). We prove that g-(hyper)bent functions from \mathbb{F}_{2^n} to \mathbb{Z}_{2^k} decompose into g-(hyper)bent functions from \mathbb{F}_{2^n} to $\mathbb{Z}_{2^{k'}}$ for some $k' < k$. We show that when n is odd, then the Boolean functions associated to a generalized bent function form an affine space of semibent functions. This complements a result [8], where it is shown that for even n the associated Boolean functions are bent.

We finally remark that for a gbent function from \mathbb{V}_n to \mathbb{Z}_{2^k} , the function cf is in general not gbent when $c \in \mathbb{Z}_{2^k}$ is even. Functions for which cf is gbent for every nonzero c seem to be quite rare. Some examples obtained from partial spreads are in [9]. Such functions may be particularly interesting for future research as they yield relative difference sets (being bent). For a general discussion on relative difference sets and functions between arbitrary abelian groups we refer to [12].

Acknowledgement. The second author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

References

- [1] C. Carlet, *\mathbb{Z}_{2^k} -linear Codes*, IEEE Trans. Inf. Theory 44:4 (1998), 1543–1547.
- [2] C. Carlet, P. Gaborit, *Hyper-bent functions and cyclic codes*, J. Combin. Theory Ser A 113 (2006), 446–482.
- [3] C. Carlet, S. Mesnager, *Four decades of research on bent functions*, Des. Codes Cryptogr., 78:1 (2016), 5–50.
- [4] P. Charpin, G. Gong, *Hyperbent functions, Kloosterman sums, and Dickson polynomials*, IEEE Trans. Inform. Theory 54:9 (2008), 4230–4238.
- [5] T. W. Cusick, P. Stănică, *Cryptographic Boolean Functions and Applications*, Academic Press, San Diego, CA, 2009.
- [6] S. Gangopadhyay, E. Pasalic, P. Stănică, *A note on generalized bent criteria for Boolean functions*, IEEE Trans. Inform. Theory 59:5 (2013), 3233–3236.
- [7] S. Hodžić, E. Pasalic, *Generalized bent functions – Some general construction methods and related necessary and sufficient conditions*, Cryptogr. Commun. 7 (2015), 469–483.
- [8] T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, manuscript.
- [9] T. Martinsen, W. Meidl, P. Stănică, *Partial spread and vectorial generalized bent functions*, manuscript.
- [10] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, to appear.
- [11] M.G. Parker, A. Pott, *On Boolean functions which are bent and negabent*, In: Sequences, subsequences, and consequences, LNCS 4893, Springer, Berlin, 2007, 9–23.
- [12] A. Pott, *Nonlinear functions in abelian groups and relative difference sets*, Discrete Appl. Math. 138 (2004), 177–193.
- [13] P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, Prikl. Diskr. Mat. 1 (2009), 16–18 (see also, <http://eprint.iacr.org/2009/544.pdf>).

- [14] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, *Investigations on bent and negabent functions via the nega-Hadamard transform*, IEEE Trans. Inform. Theory 58:6 (2012), 4064–4072.
- [15] P. Stănică, T. Martinsen, S. Gangopadhyay, B.K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptogr. 69 (2013), 77–94.
- [16] [W. Su, A. Pott, X. Tang, *Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree*, IEEE Trans. Inform. Theory 59:6 \(2013\), 3387–3395.](#)
- [17] N. Tokareva, *Generalizations of bent functions: a survey of publications*, (Russian) Diskretn. Anal. Issled. Oper. 17 (2010), no. 1, 34–64; translation in J. Appl. Ind. Math. 5:1 (2011), 110–129.
- [18] [N. Tokareva, *Bent Functions, Results and Applications to Cryptography*, Academic Press, San Diego, CA, 2015.](#)
- [19] [A.M. Youssef, G. Gong, *Hyper-bent functions*, In: Adv. Crypt. – EUROCRYPT 2001, LNCS 2045, Springer, Berlin, 2001, 406–419.](#)