Decomposing generalized bent and hyperbent functions

Thor Martinsen[1], Wilfried Meidl[2], Sihem Mesnager[3], Pantelimon Stănică[1]

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

***Abstract*—In this paper we introduce generalized hyperbent functions from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_{2k}$, and investigate decompositions of generalized (hyper)bent functions. We show that generalized (hyper)bent functions f from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_{2k}$ consist of components which are generalized (hyper)bent functions from $\mathbb{F}_{2^n}$ to $\mathbb{Z}_{2k'}$ for some $k' < k$. For even n, most notably we show that the g-hyperbentness of f is equivalent to the hyperbentness of the components of f with some conditions on the Walsh-Hadamard coefficients. 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, semibent functions, hyperbent functions, generalized bent functions, cyclotomic fields.

I. Introduction

In the context of filtered LFSRs, Canteaut and Rotella [1] showed at the 2016 FSE conference that when considering fast correlation attacks, the relevant criterion should no longer be nonlinearity, but rather generalized nonlinearity. Indeed, Canteaut and Rotella showed that if $f + \mathrm{Tr_n}(\lambda x^k)$ (where "$\mathrm{Tr_n}$" stands for the absolute trace function over $\mathbb{F}_{2^n}$) is biased, then we can apply a fast correlation attack to recover x_0^k where x_0 denotes the initial state. If k is coprime to 2^n-1, then the attack recovers the initial state. Moreover, the case when k is not coprime to 2^n-1 also leads to another attack and a new criterion to evaluate the security of filtered LFSR. The new criterion given on filtered LFSRs has thus revived interest in the topic of hyperbent functions. This paper seeks to increase our knowledge of these functions.

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 $\Im(z) = \beta$ be the real and imaginary parts of a complex number $z = \alpha + \beta i$, respectively. For a *generalized Boolean function* $f : \mathbb{V}_n \to \mathbb{Z}_q$ 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 $\zeta_q = e^{\frac{2\pi\imath}{q}}$ 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 $\mathrm{Tr_n}(ux)$. Most of our results are in the vector space $\mathbb{V}_n = \mathbb{F}_2^n$, although, whenever applicable (for example, where we emphasize hyperbent properties) we require the finite field environment $\mathbb{V}_n = \mathbb{F}_{2^n}$. We use the notation as in [10], [11], [18] and denote the set of all generalized Boolean functions by $\mathcal{GB}_n^q$ and when $q = 2$, by $\mathcal{B}_n$. A function $f : \mathbb{V}_n \to \mathbb{Z}_q$ 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 a historical perspective, and making pertinent connections to designs, codes and cryptography is [4]. A book devoted especially to bent functions and containing a complete survey (including variations, generalizations and applications) is [13].

In Section II we recall some results which are of importance to our considerations and will be used in the following sections. In Section III we introduce generalized hyperbent functions, and show hyperbentness for classes of gbent functions introduced in [11], which can be seen as generalized Dillon's PS (Partial Spreads) functions. These canonical examples also guarantee the existence of generalized hyperbent functions. In Section IV 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 $k' < k$. In particular, for n even, we show that $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ is generalized hyperbent if and only if all components are hyperbent with some conditions on the Walsh-Hadamard coefficients. 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.

II. Preliminaries

We begin by collecting some results which we will subsequently use in the paper. We start with a lemma, which is Proposition 1 in [10] (here, $\mathbf{u}\cdot\mathbf{x}=\sum_{i=1}^{n}u_ix_i$ is the dot product, where $\mathbf{u}=(u_1,\ldots,u_n),\mathbf{x}=(x_1,\ldots,x_n)\in\mathbb{V}_n$).

Lemma 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*

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

In [10] 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. *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 $f^*\in\mathcal{GB}_n^{2^k}$, except for n odd and $k=2$, in which case we have

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

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

$$f(\mathbf{x})=a_0(\mathbf{x})+2a_1(\mathbf{x})+\cdots+2^{k-1}a_{k-1}(\mathbf{x})$$

for some Boolean functions a_i, $0\le i\le k-1$. We remark that this decomposition is very natural (and as we will see renders a lot of structure when f is gbent), since it comes from the binary representation of the elements in the image set $\mathbb{Z}_{2^k}$. 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 3. *Let $f(\mathbf{x})$ be a gbent function in $\mathcal{GB}_n^{2^k}$, $k>1$. We write*

$$f(\mathbf{x})=a_0(\mathbf{x})+2a_1(\mathbf{x})+\cdots+2^{k-2}a_{k-2}(\mathbf{x})+2^{k-1}a_{k-1}(\mathbf{x}),$$

for $a_i\in\mathcal{B}_n$, $0\le i\le k-1$, and for $\mathbf{c}=(c_0,c_1,\ldots,c_{k-2})\in\mathbb{F}_2^{k-1}$, let $g_{\mathbf{c}}$ be the Boolean function

$$g_{\mathbf{c}}(\mathbf{x})=c_0a_0(\mathbf{x})\oplus c_1a_1(\mathbf{x})\oplus\cdots\oplus c_{k-2}a_{k-2}(\mathbf{x})\oplus a_{k-1}(\mathbf{x}). \tag{1}$$

- (i) [10] *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) [10], [16], [17] *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.*

By Proposition 3 the set of the functions $g_{\mathbf{c}}$ defined as in (1) form an affine subspace of bent functions. As for linear spaces of bent functions, i.e. vectorial bent functions, we call the bent functions $g_{\mathbf{c}}$ the *component functions*.

Remark 4. *When n is even, then $a_0(\mathbf{x})+2a_1(\mathbf{x})\in\mathcal{GB}_n^4$ is gbent if and only if a_0 and $a_0\oplus a_1$ are bent (see* [16]*). Sufficient conditions on the gbentness of $f\in\mathcal{GB}_n^{2^k}$ have been published for $k=2$ when n is odd, and in general for $k=3,4$ (see* [10], [16], [17]*). We will generalize the previously known Proposition $3(ii)$ in Theorem* 11.

Another result about the decomposition of gbent functions is the following theorem of [10].

Theorem 5 ([10, 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).

Remark 6. *In the proof of* [10, Theorem 3] *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* 15 *we will show that (i) and (ii) in Theorem* 5 *are equivalent also when n is odd.*

III. Generalized hyperbent functions

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

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

Recall that f is called *hyperbent* if $|\mathcal{W}_{f,i}(u)|=2^{n/2}$, for all $1\le i\le n$ with $\gcd(2^n-1,i)=1$. For background on hyperbent functions we refer to the articles [3], [5], [23].

In this section we introduce the concept of hyperbent functions for generalized Boolean functions. For a function $f\in\mathcal{GB}_n^{2^k}$ and an integer $1\le i\le n$ 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

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

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

There are several reasons for studying hyperbent functions. In addition to fast correlation attacks already mentioned in the introduction, as observed in [23], the extended Walsh-Hadamard transform could be used to quantify the approximation of S-boxes via a bijective monomial, and the flatness of its (absolute) values can be regarded as resistance to such approximations; in [3], yet another connection was found,

and the authors showed that all hyperbent functions can be obtained from codewords of an extended cyclic code of small dimension. While we could not yet find that code theory connection for the generalized hyperbentness, we remark that a motivation for their study is simply found in the attempt to check when a composition of a gbent (in this case via a bijective monomial) is also gbent. This is nontrivial in the classical case, as well as in the generalized sense.

In [3] Carlet and Gaborit proved that all functions in the class of PS_{ap} are hyperbent. We similarly show the g-hyperbentness for a class of gbent functions from $\mathcal{GB}_{2n}^{2^k}$ presented in [11]. The functions, which are given in bivariate form, can be seen as functions in a generalized PS_{ap} class. We use the convention that $\frac{y'}{y} = 0$ if $y = 0$.

Theorem 7. *Let $g_j : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $0 \le j \le k-1$, 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 $f : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{Z}_{2^k}$ given by $f(y', y) = \sum_{j=0}^{k-1} 2^j g_j(y'/y)$ is g-hyperbent.*

Proof. We start the proof 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 $\mathrm{Tr_n}(y) = 0$ for $y \in \mathbb{F}_{2^{n/2}}$. With the inner product on $\mathbb{F}_{2^n}$ defined by $\langle y, y'\rangle = \mathrm{Tr_n}(yy')$, the subspace $\mathbb{F}_{2^{n/2}}$ is orthogonal to itself. Therefore,

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

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 $x := y' + \omega y$, $z := \frac{y'}{y}$)

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

With (2) we obtain

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

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

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

By [3, 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 $\mathrm{Tr_n}(a(z+\omega)^i y^i) = 0$, since $y^i \in \mathbb{F}_{2^{n/2}}$. Hence, the first term $\sum_z \zeta^{\sum_{j=0}^{k-1} 2^j g_j(z)} \sum_y (-1)^{\mathrm{Tr_n}(a(z+w)^i y^i)}$ 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 $\zeta^{\sum_j 2^j g_j(0) \oplus \mathrm{Tr_n}(ay'^i)}$ 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. □

IV. 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.

First, for a function $f : \mathbb{F}_{2^n} \to \mathbb{Z}_{2^k}$ we consider its standard decomposition $f(x) = \sum_{j=0}^{k-1} 2^j a_j(x)$, where the a_j's are Boolean functions. Recall from Proposition 3 that, when n is even, if f is gbent then all its components $f_{\mathbf{c}}(x) = c_0 a_0(x) \oplus c_1 a_1(x) \oplus \cdots \oplus c_{k-2} a_{k-2}(x) \oplus a_{k-1}(x)$ are bent functions for each $\mathbf{c} \in \mathbb{F}_2^{k-1}$. We extend this results to g-hyperbent functions by showing that g-hyperbent functions have hyperbent components. Moreover, we will see that a function $f \in \mathcal{GB}_n^{2^k}$ for which all components are hyperbent along with some conditions on the Walsh-Hadamard coefficients, is also g-hyperbent.

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

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

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 $k \ge 3$,

$$\mathcal{H}_{f,i}^{(2^k)}(a) = 2^{\frac{n}{2}} \zeta_{2^k}^{\rho} \tag{3}$$

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

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

Set

$$Q(X_1,\dots,X_{k-1}) = \prod_{j=0}^{k-1}\left(\frac{1+\zeta_{2^k}^{2^j}}{2}+\frac{1-\zeta_{2^k}^{2^j}}{2}X_j\right)$$
$$= 2^{-k}\prod_{j=0}^{k-1}\sum_{c\in\mathbb{F}_2}\left(\left(1+\zeta_{2^k}^{2^j+c2^{k-1}}\right)X_j^c\right)$$
$$= 2^{-k}\sum_{c\in\mathbb{F}_2^k}\left(\prod_{j=0}^{k-1}\left(1+\zeta_{2^k}^{2^j+c_j2^{k-1}}\right)\right)\prod_{j=0}^{k-1}X_j^{c_j}.$$

Set $A_{\mathbf{c}} = 2^{-k}\prod_{j=0}^{k-1}\left(1+\zeta_{2^k}^{2^j+c_j2^{k-1}}\right)$, where $\mathbf{c} = (c_0,\dots,c_{k-1})$. Then

$$\zeta_{2^k}^{f(x)} = Q\left((-1)^{a_0(x)},\dots,(-1)^{a_{k-1}(x)}\right) = \sum_{\mathbf{c}\in\mathbb{F}_2^k}A_{\mathbf{c}}(-1)^{\sum_{j=0}^{k-1}c_ja_j(x)}. \tag{4}$$

Define the "canonical injection" $\iota:\mathbb{F}_2^{k-1}\to\mathbb{Z}_{2^{k-1}}$ by $\iota(\mathbf{c}) = \sum_{j=0}^{k-2}c_j2^j$ where $\mathbf{c} = (c_0,c_1,\dots,c_{k-2})$. It is obvious that, in fact, ι is a bijection. Then, we have the following theorem (we remark that in [20], independently, the authors also obtain the characterization of generalized bent functions in terms of their components, for both n even and odd, see our Theorems 8 and 11).

Theorem 8. *Let $f:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^k}$, n even. Then f is a g-hyperbent function given as $f(x) = a_0(x)+2a_1(x)+\cdots+2^{k-1}a_{k-1}(x)$ if and only if, for each $\mathbf{c}\in\mathbb{F}_2^{k-1}$, the Boolean function $f_{\mathbf{c}}$ defined as*

$$f_{\mathbf{c}}(x) = c_0a_0(\mathbf{x})\oplus c_1a_1(x)\oplus\cdots\oplus c_{k-2}a_{k-2}(x)\oplus a_{k-1}(x)$$

is a hyperbent function, such that $\mathcal{W}_{f_{\mathbf{c}},i}(a) = (-1)^{\mathbf{c}\cdot\iota^{-1}(g_i(a))+s_i(a)}2^{\frac{n}{2}}$, for some $g_i:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^{k-1}}$, $s_i:\mathbb{F}_{2^n}\to\mathbb{F}_2$, for all $\gcd(i,2^n-1)=1$.

Proof. First, we compute

$$2^kA_{\mathbf{c}} = \prod_{j=0}^{k-1}\sum_{d\in\mathbb{Z}_2}\zeta_{2^k}^{d2^j+dc_j2^{k-1}} = \sum_{\mathbf{d}\in\mathbb{F}_2^k}\zeta_{2^k}^{\sum_{j=0}^{k-1}\left(d_j2^j+d_jc_j2^{k-1}\right)}$$
$$= \sum_{\mathbf{d}\in\mathbb{F}_2^k}\zeta_{2^k}^{\sum_{j=0}^{k-1}d_j2^j}(-1)^{\sum_{j=0}^{k-1}d_jc_j}$$
$$= \sum_{\mathbf{d}\in\mathbb{F}_2^k}\zeta_{2^k}^{\sum_{j=0}^{k-2}d_j2^j+2^{k-1}d_{k-1}}(-1)^{\sum_{j=0}^{k-1}d_jc_j}$$
$$= \left(\sum_{d_{k-1}\in\mathbb{F}_2}(-1)^{d_{k-1}+c_{k-1}d_{k-1}}\right)\cdot\sum_{(d_0,\dots,d_{k-2})\in\mathbb{F}_2^{k-1}}\zeta_{2^k}^{\sum_{j=0}^{k-2}d_j2^j}(-1)^{\sum_{j=0}^{k-2}d_jc_j}$$

which is 0 if $c_{k-1}=0$, and $2\sum_{(d_0,\dots,d_{k-2})\in\mathbb{F}_2^{k-1}}\zeta_{2^k}^{\sum_{j=0}^{k-2}d_j2^j}(-1)^{\sum_{j=0}^{k-2}d_jc_j}$, if $c_{k-1}=1$. Next, we let i be coprime with 2^n-1. Using (4) and the previous computation, we infer that

$$\mathcal{H}_{f,i}^{(2^k)}(a) = \sum_{x\in\mathbb{F}_{2^n}}\sum_{\mathbf{c}\in\mathbb{F}_2^k}A_{\mathbf{c}}(-1)^{\sum_{j=0}^{k-1}c_ja_j(x)+\mathrm{Tr_n}(ax^i)} = \sum_{\mathbf{c}\in\mathbb{F}_2^k,c_{k-1}=1}A_{\mathbf{c}}\mathcal{W}_{f_{\mathbf{c}},i}(a).$$

Define a "dot product" over $\mathbb{F}_2^{k-1}$ by setting $\mathbf{c}\cdot\mathbf{d} = \sum_{j=0}^{k-2}c_jd_j$ for $\mathbf{c} = (c_0,c_1,\dots,c_{k-2})\in\mathbb{F}_2^{k-1}$ and $\mathbf{d} = (d_0,d_1,\dots,d_{k-2})\in\mathbb{F}_2^{k-1}$. Then

$$\mathcal{H}_{f,i}^{(2^k)}(a) = \frac{1}{2^{k-1}}\sum_{(\mathbf{c},\mathbf{d})\in\mathbb{F}_2^{k-1}\times\mathbb{F}_2^{k-1}}(-1)^{\mathbf{c}\cdot\mathbf{d}}\zeta_{2^k}^{\iota(\mathbf{d})}\,\mathcal{W}_{f_{\mathbf{c}},i}(a). \tag{5}$$

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

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

for some $f_i^\star:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^k}$. Fix i coprime with 2^n-1 and decompose $f_i^\star$ as $f_i^\star = g_i+2^{k-1}s_i$ with $g_i:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^{k-1}}$ and $s_i:\mathbb{F}_{2^n}\to\mathbb{F}_2$ so that

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

Then,

$$\sum_{\mathbf{d}\in\mathbb{F}_2^{k-1}}\left(\frac{1}{2^{k-1}}\sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}}(-1)^{\mathbf{c}\cdot\mathbf{d}}\mathcal{W}_{f_{\mathbf{c}},i}(a)\right)\zeta_{2^k}^{\iota(\mathbf{d})} - 2^{\frac{n}{2}}(-1)^{s_i(a)}\zeta_{2^k}^{g_i(a)} = 0. \tag{6}$$

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

$$\frac{1}{2^{k-1}}\sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}}(-1)^{\mathbf{c}\cdot\mathbf{d}}\mathcal{W}_{f_{\mathbf{c}},i}(a) = \begin{cases}0 & \text{if } \iota(\mathbf{d})\neq g_i(a)\\ 2^{\frac{n}{2}}(-1)^{s_i(a)} & \text{if } \iota(\mathbf{d}) = g_i(a).\end{cases} \tag{7}$$

Now, let us invert (7). We have for any $\mathbf{c}\in\mathbb{F}_2^{k-1}$

$$\mathcal{W}_{f_{\mathbf{c}},i}(a) = \frac{1}{2^{k-1}}\sum_{(\mathbf{u},\mathbf{v})\in\mathbb{F}_2^{k-1}}(-1)^{(\mathbf{u}+\mathbf{c})\cdot\mathbf{v}}\mathcal{W}_{f_{\mathbf{u}},i}(a)$$
$$= \sum_{\mathbf{v}\in\mathbb{F}_2^{k-1}}(-1)^{\mathbf{c}\cdot\mathbf{v}}\left(\frac{1}{2^{k-1}}\sum_{\mathbf{u}\in\mathbb{F}_2^{k-1}}(-1)^{\mathbf{u}\cdot\mathbf{v}}\mathcal{W}_{f_{\mathbf{u}},i}(a)\right)$$
$$= (-1)^{\mathbf{c}\cdot\iota^{-1}(g_i(a))+s_i(a)}2^{\frac{n}{2}},$$

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

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

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

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

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

proving that f is g-hyperbent. □

Example 9. *In* [9] *several classes of hyperbent functions are constructed. In particular, examples of hyperbent functions $f:\mathbb{F}_{2^n}\to\mathbb{F}_2$ of the form $(n=2m)$ $F(x)=\mathrm{Tr_n}\left(\beta_1 x^{2^m-1}+\beta_3 x^{3(2^m-1)}\right)$ are provided ($\beta_i\in\mathbb{F}_{2^m}$). Let two such functions, F_1, F_2 be given. It is shown in* [9] *that the extended Walsh–Hadamard transform of such functions (if hyperbent) are given by*

$$\mathcal{W}_{F_1,i}(a)=2^m(-1)^{F_1(a^{\frac{2^m-1}{2i}})},$$
$$\mathcal{W}_{F_2,i}(a)=2^m(-1)^{F_2(a^{\frac{2^m-1}{2i}})}.$$

Then the generalized Boolean function $f:\mathbb{F}_{2^n}\to\mathbb{Z}_4$ given by $f=a_0+2a_1$, where $a_1:=F_1, a_0=F_1\oplus F_2$, satisfies the conditions of our Theorem 8 *with $s_i(a)=F_1(a^{\frac{2^m-1}{2i}})$ and $g_i(a)=F_1(a^{\frac{2^m-1}{2i}})\oplus F_2(a^{\frac{2^m-1}{2i}})$.*

Remark 10. *Note that in the proof of Theorem* 8*, 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* 8 *proposes therefore an alternate proof of Proposition 3(i).*

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

Theorem 11. *Let $f:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^k}$, n odd, be a gbent function given as $f(x)=a_0(x)+2a_1(x)+\cdots+2^{k-1}a_{k-1}(x)$. Then f is gbent if and only if for each $\mathbf{c}\in\mathbb{F}_2^{k-1}$, the Boolean function $f_\mathbf{c}$ defined as*

$$f_\mathbf{c}(x)=c_1a_1(x)\oplus c_2a_2(x)\oplus\cdots\oplus c_{k-2}a_{k-2}(x)\oplus a_{k-1}(x)$$

is a semibent function with the Walsh transform $\mathcal{W}_{f_\mathbf{c}}(a)=\left((-1)^{\mathbf{c}\cdot\iota^{-1}(g_1(a))+s_1(a)}-(-1)^{\mathbf{c}\cdot\iota^{-1}(g_2(a))+s_2(a)}\right)2^{\frac{n+1}{2}}$, for some $g_j:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^{k-1}}, s_j:\mathbb{F}_{2^n}\to\mathbb{F}_2$, $j=1,2$, where $g_2(a)-g_1(a)+2^{k-1}(s_2(a)-s_1(a))=2^{k-2}$ in $\mathbb{Z}_{2^k}$.

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

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

for some map $f^\star:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^k}$. 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,

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

Write $f^\star(a)+2^{k-3}=g_1(a)+2^{k-1}s_1(a)+2^kt_1(a)$ and $f^\star(a)+3\cdot 2^{k-3}=g_2(a)+2^{k-1}s_2(a)+2^kt_2(a)$ 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 8, 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 (5) and recall that ι is the "canonical" injection from $\mathbb{F}_2^{k-1}$ to $\mathbb{Z}_{2^{k-1}}$ which sends $(c_0,\ldots,c_{k-2})$ to $\sum_{j=0}^{k-2}c_j2^j$), namely,

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

Then, one has

$$\begin{aligned}&\frac{1}{2^{k-1}} \sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{\mathbf{c}\cdot\mathbf{d}}\mathcal{W}_{f_\mathbf{c}}(a)\\ &\quad= \begin{cases}0 & \text{if } \iota(\mathbf{d})\notin\{g_1(a),g_2(a)\}\\ 2^{\frac{n-1}{2}}(-1)^{s_1(a)} & \text{if } \iota(\mathbf{d})=g_1(a)\\ -2^{\frac{n-1}{2}}(-1)^{s_2(a)} & \text{if } \iota(\mathbf{d})=g_2(a).\end{cases}\end{aligned} \tag{8}$$

Thus,

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

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

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

for every $a\in\mathbb{F}_{2^n}$, along with the conditions on the Walsh spectrum.

Conversely, assume that for all $\mathbf{c}\in\mathbb{F}_{2^{k-1}}$, $f_\mathbf{c}$ are semibent and their Walsh transform are of the form

$$\mathcal{W}_{f_\mathbf{c}}(a)=\left((-1)^{\mathbf{c}\cdot\iota^{-1}(g_1(a))+s_1(a)}-(-1)^{\mathbf{c}\cdot\iota^{-1}(g_2(a))+s_2(a)}\right)2^{\frac{n+1}{2}},$$

for some $g_j:\mathbb{F}_{2^n}\to\mathbb{Z}_{2^{k-1}}, s_j:\mathbb{F}_{2^n}\to\mathbb{F}_2$, $j=1,2$, with

$g_2(a) - g_1(a) + 2^{k-1}(s_2(a) - s_1(a)) = 2^{k-2}$ in $\mathbb{Z}_{2^k}$. Then

$$\begin{aligned}
\mathcal{H}_f^{(2^k)}(a) &= \frac{1}{2^{k-1}} \sum_{(\mathbf{c},\mathbf{d})\in\mathbb{F}_2^{k-1}\times\mathbb{F}_2^{k-1}} (-1)^{\mathbf{c}\cdot\mathbf{d}} \zeta_{2^k}^{\iota(\mathbf{d})} . \mathcal{W}_{f_\mathbf{c}}(a) \\
&= 2^{\frac{n+1}{2}-k} \sum_{\mathbf{d}\in\mathbb{F}_2^{k-1}} \zeta_{2^k}^{\iota(\mathbf{d})} \left(\sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{\mathbf{c}\cdot(\mathbf{d}\oplus\iota^{-1}(g_1(a))+s_1(a)} \right. \\
&\qquad \left. - \sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{\mathbf{c}\cdot(\mathbf{d}\oplus\iota^{-1}(g_2(a))+s_2(a)} \right) \\
&= 2^{\frac{n+1}{2}-k} \sum_{\mathbf{d}\in\mathbb{F}_2^{k-1}} \zeta_{2^k}^{\iota(\mathbf{d})} \\
&\quad \cdot \begin{cases} 0 & \text{if } \iota(\mathbf{d}) \notin \{g_1(a), g_2(a)\} \\ 2^{k-1}(-1)^{s_1(a)} & \text{if } \iota(\mathbf{d}) = g_1(a) \neq g_2(a) \\ -2^{k-1}(-1)^{s_2(a)} & \text{if } \iota(\mathbf{d}) = g_2(a) \neq g_1(a) \\ 2^{k-1}\left((-1)^{s_1(a)} - (-1)^{s_2(a)}\right) & \text{if } \iota(\mathbf{d}) = g_1(a) = g_2(a) \end{cases} \\
&= 2^{\frac{n-1}{2}} \left((-1)^{s_1(a)} \zeta_{2^k}^{g_1(a)} - (-1)^{s_2(a)} \zeta_{2^k}^{g_2(a)} \right) \\
&= 2^{\frac{n-1}{2}} (-1)^{s_1(a)} \zeta_{2^k}^{g_1(a)} \left(1 - \zeta_{2^k}^{g_2(a)-g_1(a)+2^{k-1}(s_2(s)-s_1(a))} \right) \\
&= 2^{\frac{n-1}{2}} (-1)^{s_1(a)} \zeta_{2^k}^{g_1(a)} (1 - \zeta_{2^k}^{2^{k-2}}) = s^{\frac{n}{2}} (-1)^{s_1(a)} \zeta_{2^k}^{g_1(a)} \zeta_8,
\end{aligned}$$

and so, $2^{-\frac{n}{2}} \mathcal{H}_f^{(2^k)}(a)$ is a root of unity, showing that f is gbent. □

By our previous theorems, we can identify a gbent function $f = a_0 + 2a_1 + \cdots + a_{k-2}2^{k-2} + a_{k-1}2^{k-1} \in \mathcal{GB}_n^{2^k}$ with the affine space of (semi)bent functions $a_{k-1} + \langle a_0, a_1, \ldots, a_{k-2}\rangle$ (with some additional properties on the Walsh spectrum). However, one would ask whether the functions a_i, $0 \leq i \leq k-3$, themselves have interesting properties. In our next result we show such a property, and as a byproduct, we obtain a description of the functions g_i, s_i that occur in Theorem 8 and 11.

Theorem 12. *Let $f \in \mathcal{GB}_n^{2^k}$ be a g-hyperbent function, written as $f = a_0 + 2a_1 + \cdots + a_{k-2}2^{k-2} + a_{k-1}2^{k-1}$, for some $a_i \in \mathcal{B}_n$. If n is even, then (identifying $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$)*

$$\begin{aligned}
(-1)^{s_i(\mathbf{a})} &= 2^{-\frac{n}{2}} \mathcal{W}_{a_{k-1},i}(\mathbf{a}) \\
(-1)^{g_{ij}(\mathbf{a})} &= \frac{\mathcal{W}_{a_j\oplus a_{k-1},i}(\mathbf{a})}{\mathcal{W}_{a_{k-1},i}(\mathbf{a})},
\end{aligned}$$

and further, $\mathcal{W}_{a_j,i}(\mathbf{a}) = C_{g_{ij}\oplus s_i,s_i}(\mathbf{a})$, where $C_{f,g}(\mathbf{a}) = \sum_{\mathbf{v}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{v})+g(\mathbf{a}\oplus\mathbf{v})}$ is the crosscorrelation of f, g, and s_i, g_i are as in Theorem 8 with $g_{ij} = (0, \ldots, 1, \ldots, 0)\cdot\iota^{-1}(g_i)$ (1 occurs in position j). If n is odd, with $\lambda(\mathbf{a}) := \zeta^{g_1(\mathbf{a})-g_2(\mathbf{a})}$, where s_i, g_i, $i = 1, 2$, are as in Theorem 11, then

$$\begin{aligned}
(-1)^{s_1(\mathbf{a})} &= 2^{-\frac{n+1}{2}} \frac{\mathcal{W}_{a_{k-1}}(\mathbf{a})}{1 - \imath\cdot\lambda(\mathbf{a})} \\
(-1)^{s_2(\mathbf{a})} &= \imath(-1)^{s_1(\mathbf{a})}\cdot\lambda(\mathbf{a}) = 2^{-\frac{n+1}{2}} \frac{\imath\lambda(\mathbf{a})\mathcal{W}_{a_{k-1}}(\mathbf{a})}{1 - \imath\cdot\lambda(\mathbf{a})} \\
(-1)^{g_{1j}(\mathbf{a})} - \imath(-1)^{g_{2j}(\mathbf{a})}\lambda(\mathbf{a}) &= (1 - \imath\cdot\lambda(\mathbf{a})) \frac{\mathcal{W}_{a_j\oplus a_{k-1}}(\mathbf{a})}{\mathcal{W}_{a_{k-1}}(\mathbf{a})}.
\end{aligned}$$

Proof. We show the first claim, for n even, since the second case, for n odd, is similar (using the identity $(-1)^{s_2(\mathbf{a})-s_1(\mathbf{a})} = \imath\cdot\lambda(\mathbf{a})$). By Theorem 8, every component function $f_\mathbf{c}$ is hyperbent and $\mathcal{W}_{f_\mathbf{c},i}(a) = (-1)^{\mathbf{c}\cdot\iota^{-1}(g_i(a))+s_i(a)} 2^{\frac{n}{2}}$, for some $g_i : \mathbb{F}_{2^n} \to \mathbb{Z}_{2^{k-1}}$, $s_i : \mathbb{F}_{2^n} \to \mathbb{F}_2$, for all $\gcd(i, 2^n - 1) = 1$. To make things easier, without loss of generality, we let $i = 1$. Let now, $\mathbf{c}_0 = (0, \ldots, 0), \mathbf{c}_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ (the nonzero component of $\mathbf{c}_j$ occurs in position j), with both $\mathbf{c}_0, \mathbf{c}_j$ in $\mathbb{F}_2^{k-1}$. By our assumption, a_{k-1} and $a_j \oplus a_{k-1}$ are both bent and for all $\mathbf{a} \in \mathbb{F}_2^n$ (we identify naturally $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$),

$$\begin{aligned}
\mathcal{W}_{a_{k-1}}(\mathbf{a}) &= (-1)^{s_1(\mathbf{a})} 2^{n/2} \\
\mathcal{W}_{a_j\oplus a_{k-1}}(\mathbf{a}) &= (-1)^{g_{1j}(\mathbf{a})+s_1(\mathbf{a})} 2^{n/2} = (-1)^{g_{1j}(\mathbf{a})} \mathcal{W}_{a_{k-1}}(\mathbf{a}),
\end{aligned}$$

where g_1, s_1 are as in Theorem 8, and $g_{1j} = \mathbf{c}_j \cdot \iota^{-1}(g_1)$.

Now, since $a_j = (a_j \oplus a_{k-1}) \oplus a_{k-1}$, using [6, Theorem 2.17(5)], which states that if $h(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$, then

$$\mathcal{W}_h(\mathbf{a}) = 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathcal{W}_f(\mathbf{x}) \mathcal{W}_g(\mathbf{x} \oplus \mathbf{a}),$$

we obtain

$$\begin{aligned}
\mathcal{W}_{a_j}(\mathbf{a}) &= 2^{-n} \sum_{\mathbf{v}\in\mathbb{F}_2^n} \mathcal{W}_{a_{k-1}}(\mathbf{v})\, \mathcal{W}_{a_j\oplus a_{k-1}}(\mathbf{v} \oplus \mathbf{a}) \\
&= \sum_{\mathbf{v}\in\mathbb{F}_2^n} (-1)^{g_{1j}(\mathbf{v})+s_1(\mathbf{v})+s_1(\mathbf{v}\oplus\mathbf{a})} = C_{g_{1j}\oplus s_1,s_1}(\mathbf{a}),
\end{aligned}$$

and the theorem is shown. □

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 1. For instance the proof of Proposition 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 1 which is applicable to gbent functions in an odd number of variables. We emphasize that Lemma 1 and the following Proposition 13 are interesting by themselves. They describe the cardinalities of the preimages of $f_\mathbf{u}(\mathbf{x}) := f(\mathbf{x}) + 2^{k-1}(\mathbf{u}\cdot\mathbf{x})$ for gbent functions f, which gives a lot of information on the structure of gbent functions.

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 13. *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 $\rho_{\mathbf{u}}$, $0 \le \rho_{\mathbf{u}} \le 2^k - 1$, 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

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

(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

$$\mathcal{H}_f^{(2^k)}(\mathbf{u}) = 2^{\frac{n-1}{2}}\zeta_{2^k}^{\rho_{\mathbf{u}}-2^{k-3}} + 2^{\frac{n-1}{2}}\zeta_{2^k}^{\rho_{\mathbf{u}}+2^{k-3}}, \tag{9}$$

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

$$\begin{aligned}
&\mathcal{H}_f^{(2^k)}(\mathbf{u}) \\
&= |B_{\mathbf{u}}(0)| + |B_{\mathbf{u}}(1)|\zeta_{2^k} + \cdots + |B_{\mathbf{u}}(2^{k-1}-1)|\zeta_{2^k}^{2^{k-1}-1} \\
&+ |B_{\mathbf{u}}(2^{k-1})|(-1) + |B_{\mathbf{u}}(2^{k-1}+1)|\zeta_{2^k}^{2^{k-1}+1} \\
&+ \cdots + |B_{\mathbf{u}}(2^k-1)|\zeta_{2^k}^{2^k-1} \\
&= (|B_{\mathbf{u}}(0)| - |B_{\mathbf{u}}(2^{k-1})|) + (|B_{\mathbf{u}}(1)| - |B_{\mathbf{u}}(2^{k-1}+1)|)\zeta_{2^k} \\
&+ \cdots + (|B_{\mathbf{u}}(2^{k-1}-1)| - |B_{\mathbf{u}}(2^k-1)|)\zeta_{2^k}^{2^{k-1}-1}.
\end{aligned} \tag{10}$$

Since $\{1, \zeta_{2^k}, \ldots, \zeta_{2^k}^{2^{k-1}-1}\}$ is a basis of $\mathbb{Q}(\zeta_{2^k})$, the conditions in the proposition follow from equations (9) and (10). □

We next apply Lemma 1 and Proposition 13 to show that we can decompose every g-(hyper)bent function into two (hyper)bent functions in smaller dimension in various ways.

Proposition 14. *Let $k \ge 2t$, and let $f : \mathbb{F}_{2^n} \to \mathbb{Z}_{2^k}$ be a g-hyperbent function given as*

$$f(x) = a_0(x) + 2a_1(x) + \cdots + 2^{k-1}a_{k-1}(x) = g(x) + 2^t h(x)$$

for some Boolean functions $a_i : \mathbb{F}_{2^n} \to \mathbb{F}_2$, $0 \le i \le k-1$, and

$$\begin{aligned}
g(x) &= a_0(x) + 2a_1(x) + \cdots + 2^{t-1}a_{t-1}(x) \in \mathcal{GB}_n^{2^t}, \\
h(x) &= a_t(x) + 2a_{t+1}(x) + \cdots + 2^{k-t-1}a_{k-1}(x) \in \mathcal{GB}_n^{2^{k-t}}.
\end{aligned}$$

If n is even or $k \ge 3$, 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 $f_{u,i}(x) = f(x) + 2^{k-1}\mathrm{Tr}_n(ux^i)$, $h_{u,i}(x) = h(x) + 2^{k-t-1}\mathrm{Tr}_n(ux^i)$, and for $0 \le e \le 2^t - 1$, $0 \le r \le 2^{k-t} - 1$, denote by $S^{(u,i)}(e,r)$ the set

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

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

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

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

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

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

Now suppose that n is odd and $k \ge 3$. Let $f_u(x) = f(x) + 2^{k-1}\mathrm{Tr}_n(ux)$, $h_u(x) = h(x) + 2^{k-t-1}\mathrm{Tr}_n(ux)$, $S^{(u)}(e,r) = \{x : f_u(x) = e + 2^t r\} = \{x : g(x) = e, h_u(x) = r\}$. If f is gbent, by Proposition 13 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 $0 \le \epsilon_{u,j} \le 2^t - 1$, $0 \le \rho_{u,j} \le 2^{k-t-1} - 1$, $j = 1, 2$, such that

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

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

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

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

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

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

With Proposition 14 we can conclude the equivalence of the conditions in Theorem 5, also for odd n.

Corollary 15. *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 $k \ge 3$, 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 $\mathcal{H}_{h+2^{k-2}g}^{(2^{k-1})}(\mathbf{u}) = \pm \mathcal{H}_h^{(2^{k-1})}(\mathbf{u})$ for all $\mathbf{u} \in \mathbb{V}_n$.

Proof. For even n, the corollary is Theorem 5. By Remark 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 $k \ge 3$ from Proposition 14 with $t = 1$. □

V. 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 $k' < k$. In particular, for n even we show that $f \in \mathcal{GB}_n^{2^k}$ is g-hyperbent if and only if all its Boolean components are hyperbent functions with some conditions on the Walsh-Hadamard coefficients. For n odd, we show that these Boolean functions associated to a generalized bent function form an affine space of semibent functions. This complements a result published in [10], where it is shown that for even n the Boolean component 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 may be particularly interesting for future research as - being bent - they yield relative difference sets (for a general discussion on relative difference sets and functions between arbitrary abelian groups we refer to [15]). The standard example corresponds to difference sets from spreads. However, the vast majority of the gbent functions obtained from spreads described as in [11] do not correspond to relative difference sets. One example of a gbent function from $\mathbb{V}_n$ to $\mathbb{Z}_8$, which gives a difference set and does not obviously come from a spread, is the function in [12, Corollary 3]. To the best of our knowledge all other examples in the literature also do not yield relative difference sets.

Acknowledgement. The authors are grateful to the Assoc. Edit. Prof. Tang and the anonymous reviewers for their valuable comments which have highly improved the manuscript. The second author is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

References

[1] A. Canteaut, Y. Rotella, *Attacks Against Filter Generators Exploiting Monomial Mappings*, Fast Software Encryption - 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers (2016), 78–98.

[2] C. Carlet, *$\mathbb{Z}_{2^k}$-linear Codes*, IEEE Trans. Inf. Theory 44:4 (1998), 1543–1547.

[3] C. Carlet, P. Gaborit, *Hyper-bent functions and cyclic codes*, J. Combin. Theory Ser A 113 (2006), 446–482.

[4] C. Carlet, S. Mesnager, *Four decades of research on bent functions*, Des. Codes Cryptogr. 78:1 (2016), 5–50.

[5] P. Charpin, G. Gong, *Hyperbent functions, Kloosterman sums, and Dickson polynomials*, IEEE Trans. Inform. Theory 54:9 (2008), 4230–4238.

[6] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications, 2nd Ed. (Academic Press, San Diego, CA, 2017); 1st Ed., 2009.

[7] S. Gangopadhyay, E. Pasalic, P. Stănică, *A note on generalized bent criteria for Boolean functions*, IEEE Trans. Inform. Theory 59:5 (2013), 3233–3236.

[8] S. Hodžić, E. Pasalic, *Generalized bent functions – Some general construction methods and related necessary and sufficient conditions*, Cryptogr. Commun. 7 (2015), 469–483.

[9] P. Lisoněk, *An Efficient Characterization of a Family of Hyperbent Functions*, IEEE Trans. Inform. Theory 57:9 (2011), 6010–6014.

[10] T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, In: Duquesne S., Petkova-Nikova S. (eds) Arithmetic of Finite Fields. WAIFI 2016, LNCS 10064. Springer, 160–173.

[11] T. Martinsen, W. Meidl, P. Stănică, *Partial spread and vectorial generalized bent functions*, Designs, Codes & Cryptogr. 85:1 (2017), 1–13.

[12] W. Meidl, *A secondary construction of bent functions, octal gbent functions and their duals*, to appear in Mathematics and Computers in Simulation, 2017.

[13] S. Mesnager, *Bent functions: fundamentals and results*, Springer Verlag, 2016.

[14] 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.

[15] A. Pott, *Nonlinear functions in abelian groups and relative difference sets*, Discrete Appl. Math. 138 (2004), 177–193.

[16] 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).

[17] 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.
[18] P. Stănică, T. Martinsen, S. Gangopadhyay, B.K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptogr. 69 (2013), 77–94.
[19] 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.
[20] C. Tang, C. Xiang, Y. Qi, K. Feng, *Complete characterization of generalized bent and 2^k-bent Boolean functions*, IEEE Trans. Inform. Theory 63:7 (2017), 4668–4674.
[21] 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.
[22] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.
[23] A. M. Youssef, G. Gong, *Hyper-bent functions*, In: Adv. Crypt. – EUROCRYPT 2001, LNCS 2045, Springer, Berlin, 2001, 406–419.

Thor Martinsen is a commander in the United States Navy. He currently serves as a Permanent Military Professor of applied mathematics at the Naval Postgraduate School. He has over 25 years of military experience and has served in key cryptologic, signals intelligence, electronic warfare and information operations assignments ashore and afloat, including positions as commanding officer, strike group deputy information warfare commander and cryptologic resource coordinator. He is also a senior member of IEEE and has earned Ph.D. and M.S. degrees in applied mathematics and an M.S. degree in Computer Science from the Naval Postgraduate School. His research interest are in the fields of cryptography, computer and communications security as well as electronic and cyber warfare.

Wilfried Meidl received the Ph.D. degree from Klagenfurt University, Austria, in 1998. From 2000 to 2002 he was with the Institute of Discrete Mathematics, OEAW, Vienna, Austria. From 2002–2004 he was with Temasek Labs, National University of Singapore, and from 2005–2014 he was with SabancıUniversity, Istanbul, Turkey. He is now with RICAM, OEAW, Linz, Austria. His research interests include sequences, permutation polynomials, finite fields and their applications, Boolean functions, bent functions.

Sihem Mesnager received the Ph.D. degree in Mathematics from the University of Pierre et Marie Curie (Paris VI), Paris, France, in 2002 and the Habilitation to Direct Theses (HDR) in Mathematics from the University of Paris VIII, France, in 2012. Currently, she is an associate Professor in Mathematics at the University of Paris VIII (France) in the laboratory LAGA (Laboratory of Analysis, Geometry and Applications), University of Paris XIII and CNRS. She is also a Professor adjoint to Telecom ParisTech (France), research group MIC2 in mathematics of the department INFERES, Telecom ParisTech (ex. National high school of telecommunications). Her research interests include Discrete Mathematics, Boolean functions, Bent functions, Cryptology (special cryptographic functions, symmetric ciphers, secret sharing), Coding theory (Reed-Muller codes, Identifying codes, minimal linear codes), Commutative Algebra and Computational Algebraic Geometry. She is Editor In-Chief of the International Journal of Information and Coding Theory (IJOCT) and an Associate Editor for the international journal IEEE Transactions on information Theory (IEEE-IT). She also serves on the editorial board of the international journal Advances in Mathematics of Communications (AMC), the international journal Cryptography and Communications Discrete Structures, Boolean Functions and Sequences (CCDS) and the international journal RAIRO ITA (Theoretical Informatics and Applications). She was a program co-chair for three International Workshops and served on the board off program committees of fourteen international conferences and workshops. She is (co)-author for 80 articles, 2 books and gave approx. 75 national and international conferences. Since 2016, she is president of the French Chapter of IEEE in information theory and the facilitator at AMIES (Agency for Interaction in Mathematics with Business and Society) in France for the coding theory and cryptography.

Pantelimon Stănică received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. He also holds a Doctorate in Mathematics from the Institute of Mathematics "Simion Stoilow" of the Romanian Academy (1998). Currently, he is a Professor and Associate Chair for Research at the Naval Postgraduate School, in Monterey, California. His research interests are in Cryptology, Number Theory and Discrete Mathematics.