Noname manuscript No.
(will be inserted by the editor)

Multiple characters transforms and generalized Boolean functions

Sihem Mesnager, Constanza Riera, Pantelimon Stănică

Received: date / Accepted: date

Abstract In this paper we investigate generalized Boolean functions whose spectrum is flat with respect to a set of Walsh-Hadamard transforms defined using various complex primitive roots of 1. We also study some differential properties of the generalized Boolean functions in even dimension defined in terms of these different characters. We show that those functions have similar properties to the vectorial bent functions. We next clarify the case of gbent functions in odd dimension. As a by-product of our proofs, more generally, we also provide several results about plateaued functions. Furthermore, we find characterizations of plateaued functions with respect to different characters in terms of second derivatives and fourth moments.

Keywords Generalized Boolean functions · characters · bent · plateaued

1 Introduction

Recently generalized Boolean functions have become an active area of research [8, 11, 12, 19–21, 24]. In this paper we show that there is a close connection between generalized Boolean functions and vectorial Boolean functions. We define, appropriately, the $\mathbb{Z}_{2^k}$-bent concept, which can be interpreted as the vectorial bent concept.

S. Mesnager
Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France; also, University of Paris XIII, CNRS, LAGA UMR 7539, Sorbonne Paris Cité, 93430 Villetaneuse, France; also with Telecom ParisTech, 75013 Paris, France; E-mail: smesnager@univ-paris8.fr

C. Riera
Department of Computing, Mathematics, and Physics,
Western Norway University of Applied Sciences, 5020 Bergen, Norway; E-mail: csr@hvl.no

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

Let $\mathbb{V}_n$ be an n-dimensional vector space over the binary field $\mathbb{F}_2$ (here, we consider both $\mathbb{F}_2^n$ and the finite field $\mathbb{F}_{2^n}$) and, for an integer q, let $\mathbb{Z}_q$ be the ring of integers modulo q. By '+' and '−' we respectively denote addition and subtraction in the appropiate environment (it will be obvious from the context). We call a function from $\mathbb{V}_n$ to $\mathbb{Z}_q$ ($q \geq 2$) a *generalized Boolean function* on n variables, and denote the set of all generalized Boolean functions by $\mathcal{GB}_n^q$ and, when $q = 2$, by $\mathcal{B}_n$. If $q = 2^k$ for some $k \geq 1$, we can associate to any $f \in \mathcal{GB}_n^q$ a unique sequence of Boolean functions $a_i \in \mathcal{B}_n$ ($i = 0, 1, \ldots, k-1$) such that

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{V}_n.$$

The (*Hamming*) *weight* of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{V}_n$ is denoted by $wt(\mathbf{x})$ and equals $\sum_{i=1}^n x_i$ (the Hamming weight of a function is the weight of its truth table, that is, the weight of its output vector). The cardinality of a set S is denoted by $|S|$.

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 $\zeta_q = e^{\frac{2\pi i}{q}}$ and $\langle \mathbf{u}, \mathbf{x} \rangle$ denotes a (nondegenerate) inner product on $\mathbb{V}_n$ (for easy writing, we sometimes 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*

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

For $f \in \mathcal{B}_n$, the map $\mathcal{F}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} f(\mathbf{x})(-1)^{\langle \mathbf{u}, \mathbf{x} \rangle}$ is the Fourier transform of f.

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 $\langle \mathbf{u}, \mathbf{x} \rangle$. If $\mathbb{V}_n = \mathbb{F}_{2^n}$, the standard inner product of $u, x \in \mathbb{F}_{2^n}$ is $\mathrm{Tr_n}(ux)$, where $\mathrm{Tr_n}(z)$ denotes the absolute trace of $z \in \mathbb{F}_{2^n}$.

The sum

$$\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x}+\mathbf{z}) - g(\mathbf{x})}$$

is the *crosscorrelation* of f and g at $\mathbf{z} \in \mathbb{V}_n$. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{V}_n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$ (also denoted as $\Delta_f(\mathbf{u})$). The following result was shown in [21] (modified for unnormalized Walsh-Hadamard).

Lemma 1 *If $f, g \in \mathcal{GB}_n^q$, then*

$$\begin{aligned} \sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{C}_{f,g}(\mathbf{u})(-1)^{\langle \mathbf{u}, \mathbf{x} \rangle} &= \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}, \\ \mathcal{C}_{f,g}(\mathbf{u}) &= 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}(-1)^{\langle \mathbf{u}, \mathbf{x} \rangle}. \end{aligned} \quad (1)$$

In particular, if $f = g$, then

$$\mathcal{C}_f(\mathbf{u}) = 2^{-n} \sum_{\mathbf{x}\in\mathbb{V}_n} |\mathcal{H}_f(\mathbf{x})|^2(-1)^{\langle \mathbf{u},\mathbf{x}\rangle}.$$

Given a generalized Boolean function f, the derivative $D_{\mathbf{a}}f$ of f with respect to a vector $\mathbf{a} \in \mathbb{V}_n$, is the generalized Boolean function defined by

$$D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{V}_n. \tag{2}$$

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 $f \in \mathcal{B}_n$ for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$ is a *bent* function, which only exists for even n. Further recall that $f \in \mathcal{B}_n$ is called *plateaued* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$ for a fixed integer s depending on f (we also call f then *s-plateaued*). If $s = 1$ (n must then be odd), or $s = 2$ (n must then be even), we call f *semibent*.

For $f \in \mathcal{GB}_n^{2^k}$, $c \in \mathbb{Z}_{2^k}, \mathbf{u} \in \mathbb{V}_n$, we now consider the generalized Walsh-Hadamard c-transform

$$\mathcal{H}_{cf}^{(2^k)}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^k}^{cf(\mathbf{x})}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle}.$$

When k is fixed, as before, we will often write $\mathcal{H}_{cf}(\mathbf{u})$ instead of $\mathcal{H}_{cf}^{(2^k)}(\mathbf{u})$. We say that f is *generalized c-gbent* if and only if $|\mathcal{H}_{cf}^{(2^k)}(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u}$. If f is c-gbent with respect to all nonzero c, then we call it *$\mathbb{Z}_{2^k}$-bent* (or strongly gbent) (as pointed out in [10], one could call such a function, simply bent, since the bent notion exists from a group A to another group B, but here, we preferred to insert "$\mathbb{Z}_{2^k}$-" just to differentiate it from a single character notion and to also specify the output of our functions). We will prove later that, by imposing bentness with respect to all characters ζ_q^c (hence $\mathbb{Z}_{2^k}$-bent), we obtain a condition resembling the vectorial bent property.

Similarly, a function $f \in \mathcal{GB}_n^q$, with $q = 2^k$, $k > 1$, is called *generalized plateaued of level s* [14] if $|\mathcal{H}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$. If it has the same values with respect to the transform $\mathcal{H}_{cf}^{(2^k)}$ then we call f a (c, s)-plateaued (if the level s is not specified, we will write $(c, \cdot)$-plateaued). Furthermore, if f is (c, s)-plateaued with respect to all nonzero c, then we call f a *$\mathbb{Z}_{2^k}$-plateaued function of level s*.

If f is a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, and $1 \le i \le n$ is an integer, Youssef and Gong [23] defined the *extended Walsh-Hadamard transform $\mathcal{W}_{f,i}$* to be the integer valued function

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

and they called f *hyperbent* if $|\mathcal{W}_{f,i}(u)| = 2^{n/2}$, for all $u \in \mathbb{F}_{2^n}$, and $1 \le i \le n$ with $\gcd(2^n - 1, i) = 1$. For more on hyperbent functions we refer to [3–5, 13, 23].

The paper [9] introduced the concept of hyperbent functions for generalized Boolean functions. In the same vein here, using other characters, for a function $f \in \mathcal{GB}_n^{2^k}$, an integer $1 \le i \le n$, and for $c \in \mathbb{Z}_{2^k}$, we define the *extended generalized Walsh-Hadamard c-transform* $\mathcal{H}_{cf,i}^{(2^k)}$ by

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

and call f a (*generalized*) *c-hyperbent* function if $|\mathcal{H}_{cf,i}^{(2^k)}(u)| = 2^{n/2}$, for all $1 \le i \le n$ with $\gcd(2^n-1, i) = 1$. We shall call the function (*generalized*) (c,s)-*hyperplateaued* if $|\mathcal{H}_{cf,i}^{(2^k)}(u)| \in \{0, 2^{(n+s)/2}\}$, for all $u \in \mathbb{F}_{2^n}$, and $1 \le i \le n$, $\gcd(2^n-1, i) = 1$.

Remark 2 *Even though this paper only states the results for characteristic* 2*, similar results can be obtained for odd characteristic. These have not been included in the paper, for reasons of brevity and clarity.*

2 Characterization of bents and plateaueds with respect to multiple characters

Recall that a gbent function $f \in \mathcal{GB}_n^q$ is regular if $\mathcal{H}_f(u) = 2^{n/2}\zeta^{f^*(u)}$ for some function $f^* \in \mathcal{GB}_n^q$. First, we show that there is a close connection between the regularity of cf and the regularity of $2^t f$, where t is the 2-adic valuation of c. To this end, we introduce some notation relative to cyclotomic fields. Let $\mathcal{O}_K = \mathbb{Z}[\zeta_{2^k}]$ be the ring of integers in $K = \mathbb{Q}(\zeta_{2^k})$. The group of roots of unity in $\mathcal{O}_K$ is $W_k = \{\pm\zeta_{2^k}^i, 0 \le i \le 2^k - 1\}$. If $k \ge 2$, the field extension $\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}$ is a Galois extension of degree $\phi(2^k) = 2^{k-1}$ and Galois group $Gal(\mathbb{Q}(\zeta_{2^k})/\mathbb{Q}) = \{\sigma_a, 0 \le a \le 2^k - 1, \gcd(a, 2) = 1\}$, where the automorphism σ_a of K is defined by $\sigma_a(\zeta_{2^k}) = \zeta_{2^k}^a$. Furthermore, recall that $\sqrt{2} \in \mathbb{Q}(\zeta_{2^k})$ whenever $k \ge 3$ since $\sqrt{2} = \zeta_8 - \zeta_8^3 = \zeta_{2^k}^{2^{k-3}} - \zeta_{2^k}^{2^{k-2}+2^{k-3}}$. Now, note that $\zeta_8^4 = -1$. Hence, $\sigma_a(\sqrt{2}) = \sqrt{2}$ if $a = 1 \mod 8$ or $a = 7 \mod 8$, $\sigma_a(\sqrt{2}) = -\sqrt{2}$ if $a = 3 \mod 8$ or $a = 5 \mod 8$. Finally, the following lemma holds.

Lemma 3 *Suppose that $k \ge 2$, and let $c \in \mathbb{Z}_{2^k}^\star$. Let t be the 2-adic valuation of c. Then, f is c-gbent (respectively, (c,s)-plateaued) if and only if f is 2^t-bent (respectively, $(2^t, s)$-plateaued).*

Remark 4 *Note that, if $k = 2$, and f is c-gbent (respectively, (c,s)-plateaued), n must be even (respectively, $n+s$ must be even).*

Proof Let $c = 2^t a$ with $\gcd(a, 2) = 1$. Let $\mathbf{u} \in \mathbb{F}_2^n$. We have that $\mathcal{H}_{cf}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta_{2^k}^{a(2^t f(\mathbf{x}))} (-1)^{\langle \mathbf{u}, \mathbf{x} \rangle} = \sigma_a\left(\mathcal{H}_{2^t f}(\mathbf{u})\right)$. It has been shown in [15] that f is c-gbent if and only if $2^{-\frac{n}{2}} \mathcal{H}_{cf}(\mathbf{u}) \in W_K$ for any $\mathbf{u} \in \mathbb{F}_2^n$. Now, σ_a permutes W_K. Furthermore, if $k \ge 3$, $\sqrt{2} \in \mathbb{Q}(\zeta_{2^k})$ and $\sigma_a(\sqrt{2}) = \pm\sqrt{2}$. Hence, $2^{-\frac{n}{2}} \mathcal{H}_{cf}(\mathbf{u}) \in$

W_K if and only if $2^{-\frac{n}{2}}\mathcal{H}_{2^t f}(\mathbf{u}) \in W_K$, yielding that f is c-gbent if and only f is 2^t-bent (n must be even if $k=2$). We can similarly prove that f is $(c,\cdot)$-plateaued if and only if f is $(2^t,\cdot)$-plateaued (since $\sigma_a(0)=0$). □

The next result follows immediately from the preceding lemma.

Corollary 5 *f is $\mathbb{Z}_{2^k}$-bent (respectively, $\mathbb{Z}_{2^k}$-plateaued) if and only if f is 2^t-gbent (respectively, $(2^t,\cdot)$-plateaued) for any $0 \le t \le k-1$.*

Remark 6 *In view of the previous lemma, we shall use the notation $(2^t,s)$-plateaued instead of (c,s)-plateaued, where 2^t is the 2-valuation of c (that is, the largest power of 2 dividing c). In general, however, this simplification is not possible: it is not true that the spectrum of* any *generalized Boolean function is preserved in absolute value by the isomorphism σ_a (a odd), as the following example shows. Let $k=3$, $n=2$, $f=a_0+2a_1+4a_2$, where $a_0=x_1x_2, a_1=x_1, a_2=x_2$ all in $\mathcal{B}_2$. With $\zeta=e^{i\pi/4}$, we compute the spectra of f and $3f$, and obtain (we let $\alpha=\frac{\sqrt{2}}{2}$)*

$$\mathcal{H}_f(\mathbf{u}) = (\alpha+(1-\alpha)i, 2-\alpha+(1+\alpha)i, -\alpha+(-1+\alpha)i, 2+\alpha-(1+\alpha)i)$$
$$\mathcal{H}_{3f}(\mathbf{u}) = (-\alpha+(-1-\alpha)i, 2+\alpha+(-1+\alpha)i, \alpha+(1+\alpha)i, 2-\alpha+(1-\alpha)i)\,.$$

Both 1 and 3 have zero 2-adic valuation, but $\mathcal{H}_f(\mathbf{u})$ and $\mathcal{H}_{3f}(\mathbf{u})$ have different absolute values at any point.

Any function f from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$ can be (uniquely) decomposed as $f=\sum_{i=0}^{k-1} 2^i a_i$, where $a_i \in \mathcal{B}_n$. With this notation, $2^t f = 2^t \sum_{i=0}^{k-t-1} 2^i a_i$.

Furthermore, following this decomposition, we associate to $2^t f$ the Boolean functions $f_{t,\mathbf{d}} = a_{k-t-1} + \sum_{i=0}^{k-t-2} d_i a_i$, where $\mathbf{d}=(d_0,\dots,d_{k-t-2}) \in \mathbb{Z}_2^{k-t-1}$. There is a one-to-one correspondence between $\mathbb{Z}_2^{k-t-1}$ and $\mathbb{Z}_{2^{k-t-1}}$ which sends $\mathbf{d}=(d_0,\dots,d_{k-t-2}) \in \mathbb{Z}_2^{k-t-1}$ to $\sum_{i=0}^{k-t-2} 2^i d_i$. Hence, we shall sometimes use an integer value to denote an element of $\mathbb{Z}_2^{k-t-1}$. For instance, we shall write $\mathbf{2^i}$ to denote the element $\mathbf{d}$ of $\mathbb{Z}_2^{k-t-1}$ such that $d_i=1$ and $d_j=0$ if $j \ne i$.

Let us now show that there is a close connection between the generalized Walsh-Hadamard 2^t-transform $\mathcal{H}_{2^t f}$ and the Walsh-Hadamard transform $\mathcal{W}_{f_{t,\mathbf{d}}}$. For any $\mathbf{v}=(v_0,\dots,v_{k-t-2}) \in \mathbb{Z}_2^{k-t-1}$, introduce the set $P_{\mathbf{v}} = \{\mathbf{x} \in \mathbb{F}_2^n \mid a_i(\mathbf{x}) = v_i \text{ for any } 0 \le i \le k-t-2\}$ and the sum

$$S_{\mathbf{v}}^{(t)}(\mathbf{u}) = \sum_{\mathbf{x}\in P_{\mathbf{v}}} (-1)^{a_{k-t-1}(\mathbf{x})+\langle \mathbf{u},\mathbf{x}\rangle}. \tag{3}$$

Then, for any $\mathbf{u} \in \mathbb{F}_2^n$ and $\mathbf{d}=(d_0,\dots,d_{k-t-2}) \in \mathbb{Z}_2^{k-t-1}$,

$$\mathcal{H}_{2^t f}(\mathbf{u}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-t-1}} \zeta_{2^{k-t}}^{\sum_{i=0}^{k-t-2} 2^i v_i} S_{\mathbf{v}}^{(t)}(\mathbf{u})$$

and

$$\mathcal{W}_{f_{t,\mathbf{d}}}(\mathbf{u}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-t-1}} (-1)^{\sum_{i=0}^{k-t-2} d_i v_i} S_{\mathbf{v}}^{(t)}(\mathbf{u}). \tag{4}$$

Hence, $S_{\mathbf{v}}^{(t)}(\mathbf{u})$ is the coefficient of $\zeta_{2^{k-t}}^{\sum_{i=0}^{k-t-2} 2^i v_i}$ in the decomposition of $\mathcal{H}_{2^t f}(\mathbf{u})$ over the integral basis $\{\zeta_{2^{k-t}}^i, 0 \le i \le k-t-1\}$ of $\mathbb{Q}(\zeta_{2^{k-t}})$ viewed as a vector space over $\mathbb{Q}$. On the other hand, one can deduce from (4) that

$$S_{\mathbf{v}}^{(t)}(\mathbf{u}) = \frac{1}{2^{k-t-1}} \sum_{\mathbf{d}\in\mathbb{Z}_2^{k-t-1}} (-1)^{\sum_{i=0}^{k-t-2} d_i v_i} \mathcal{W}_{f_{t,\mathbf{d}}}(\mathbf{u}), \text{ for all } \mathbf{u}.$$

Let $\mathbf{u} \in \mathbb{F}_2^n$. Then, $\mathcal{H}_{2^t f}(\mathbf{u}) = \sum_{i=0}^{k-t-2} b_i \zeta_{2^{k-t}}^i$ if and only if, for any $\mathbf{d} \in \mathbb{Z}_2^{k-t-1}$, $\mathcal{W}_{f_{t,\mathbf{d}}}(\mathbf{u}) = \sum_{\mathbf{v}\in\mathbb{Z}_2^{k-t-1}} (-1)^{\sum_{i=0}^{k-t-2} d_i v_i} b_{i(\mathbf{v})}$, where the b_i's are integers, and $i(\mathbf{v}) = \sum_{j=0}^{k-t-2} 2^j v_j$.

2.1 The even case

In this section, we shall consider functions for which $|\mathcal{H}_{2^t f}(\mathbf{u})|$ is an integer. In the sequel, when considering bent functions, n is an even integer and, when considering plateaued functions with magnitude $2^{\frac{n+s}{2}}$, $n+s$ is an even integer.

In [11], it has been shown that, if $f \in \mathcal{GB}_n^{2^k}$ is gbent then f is regular, that is $\mathcal{H}_f(\mathbf{u}) = 2^{n/2}\zeta_{2^k}^{f^*(\mathbf{u})}$, for all $\mathbf{u} \in \mathbb{F}_2^n$, for some $f^* \in \mathcal{GB}_n^{2^k}$, which is the dual of f. Going through the argument of [11], we can see that in fact, every 2^t-gbent is regular. In fact, one can prove that generalized plateaued functions (see [15]), or even the newly introduced landscape functions (see [17]) are all "regular".

Lemma 7 *Let $\mathbf{u} \in \mathbb{F}_2^n$. Let s be a nonnegative integer such that $n+s$ is even. If $|\mathcal{H}_{2^t f}(\mathbf{u})| = 2^{\frac{n+s}{2}}$, then*

$$\mathcal{H}_{2^t f}(\mathbf{u}) = 2^{\frac{n+s}{2}} \zeta_{2^{k-t}}^{b_{t,\mathbf{u}}}, \tag{5}$$

for some $b_{t,\mathbf{u}} \in \mathbb{Z}_{2^{k-t}}$.

Then, the following result [11] holds.

Theorem 8 *Let $f = \sum_{i=0}^{k-1} 2^i a_i$ from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$. Let $0 \le t \le k-1$. Suppose that n is even (respectively, let s be a positive integer such that $n+s$ is even). Then f is 2^t-gbent (respectively, f is $(2^t, s)$-plateaued) if and only if, for any $\mathbf{d} \in \mathbb{Z}_2^{k-t-1}$, $f_{t,\mathbf{d}}$ is bent (respectively, s-plateaued) and*

$$\mathcal{W}_{f_{t,\mathbf{d}}}(\mathbf{u}) = \mathcal{W}_{a_{k-t-1}}(\mathbf{u})(-1)^{\sum_{i=0}^{k-t-2} d_i b_i(\mathbf{u})} \tag{6}$$

for some $\mathbf{b} = (b_0, \ldots, b_{k-t-2}) \in \mathbb{Z}_2^{k-t-1}$. If $2^t f$ is gbent, $b_i = a_{k-t-1}^\star + (a_{k-t-1} + a_i)^\star$, $0 \le i \le k-t-2$, where $g^\star$ stands for the dual function of g.

The next corollary gives, as a by-product, another proof of [7, Theorem 6].

Corollary 9 *Let $f = \sum_{i=0}^{k-1} 2^i a_i$ from $\mathbb{F}_2^n$ to $\mathbb{Z}_{2^k}$. Suppose that n is even (respectively, let s be a positive integer such that $n+s$ is even). Then f is $\mathbb{Z}_{2^k}$-bent (respectively, f is $\mathbb{Z}_{2^k}$-plateaued with magnitude $2^{\frac{n+s}{2}}$) if and only, for any $\mathbf{d} \in \mathbb{Z}_2^{k-1} \setminus \{\mathbf{0}\}$, $g_{\mathbf{d}} = \sum_{i=0}^{k-1} d_i a_i$ is bent (respectively, s-plateaued) and, for any $0 \le t \le k-1$, there exists $h^{(t)} = (h_0^{(t)}, \dots, h_{k-t-2}^{(t)})$ from $\mathbb{F}_2^n$ to $\mathbb{Z}_2^{k-t-1}$ such that, for $\mathbf{u} \in \mathbb{F}_2^n$,*

$$\mathcal{W}_{g_{\mathbf{d}}}(\mathbf{u}) = \mathcal{W}_{a_{k-t-1}}(\mathbf{u})(-1)^{\sum_{i=0}^{k-t-2} d_i h_i^{(t)}(\mathbf{u})}$$

if $d_{k-t-1} = 1$ and $d_i = 0$ for $i \ge k-t$.

Remark 10 *One can repeat the known proofs for Lemma 7, Theorem 8 and Corollary 9 and show these results for hyperbent functions with $S_{\mathbf{v}}^{(t)}(\mathbf{u}) = \sum_{\mathbf{x} \in P_{\mathbf{v}}} (-1)^{a_{k-t-1} + \langle \mathbf{u}, \mathbf{x}^e \rangle}$ and $\gcd(e, 2^n - 1) = 1$. Obviously, one has to be careful since some functions and vectors involved in those results could depend on e.*

But above, Corollary 9 says that $\mathbb{Z}_{2^k}$-bent functions are images of vectorial Boolean functions under the map which sends $(a_0, \dots, a_{k-1})$ to $\sum_{i=0}^{k-1} 2^i a_i$. Therefore, $\mathbb{Z}_{2^k}$-bent functions can exists only if $k \le \frac{n}{2}$ according to the Nyberg bound. Certainly, this is known for a much more general case, since there is no splitting $(2^n, 2^k, 2^n, 2^{n-k})$-relative difference set with abelian forbidden subgroup if $k > n/2$ [18]. Furthermore, recall the classical result that vectorial bent functions have all of their nonzero derivatives balanced. By definition, the derivatives of $\mathbb{Z}_{2^k}$-bent functions are balanced [16]. The c-gbent functions satisfy a weaker character sum condition, hence in general the derivatives will not all be balanced. In the following we will investigate the differential properties of gbent functions (or c-gbent functions).

In the spirit of [10], if $\mathbb{V}_n = \mathbb{F}_2^n$, $0 \le t \le k-1$, we say that $f \in \mathcal{GB}_n^{2^k}$ satisfies the (*generalized*) 2^t-*propagation criterion of order* ℓ ($1 \le \ell \le n$), denoted by 2^t-*gPC*(ℓ), if and only if the autocorrelation $\mathcal{C}_{2^t f}(\mathbf{v}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{v}) - f(\mathbf{x})} = 0$, for all vectors $\mathbf{v} \in \mathbb{F}_2^n$ of weight $0 < wt(\mathbf{v}) \le \ell$. If $\ell = 1$, we say that f satisfies the (*generalized*) 2^t-*strict avalanche criterion* (2^t-*gSAC*). It is not difficult to obtain that f is 2^t-gbent if and only if $\mathcal{C}_{2^t f}(\mathbf{v}) = 0$ for all $\mathbf{v} \ne \mathbf{0}$. Let $f \in \mathcal{GB}_n^{2^k}$ and $A_j^{(\mathbf{w})} = \{\mathbf{x} | f(\mathbf{x}+\mathbf{w}) - f(\mathbf{x}) = j\}$. Observe that $|A_0^{(\mathbf{0})}| = 2^n$, and $|A_j^{(\mathbf{0})}| = 0$, for $j > 0$. The following theorem is just a generalization (for c-gbent functions) of [10, Theorem 4]. We could restate the theorem using the truncation $2^t f$ (recall that we perform the operations in $\mathbb{Z}_{2^k}$), but we preferred to give the result in terms of the values of the non-truncated function f.

Theorem 11 *Let $f \in \mathcal{GB}_n^{2^k}$, $1 \le \ell \le n$, and $A_j^{(\mathbf{w})} = \{\mathbf{x} | f(\mathbf{x}+\mathbf{w}) - f(\mathbf{x}) = j\}$. Then f is 2^t-gPC(ℓ) (for $0 \le t < k$) if and only if*

$$\sum_{\substack{j \equiv s \pmod{2^{k-t}}}}^{2^{k-1}-1} \left| A_j^{(\mathbf{w})} \right| = \sum_{\substack{j \equiv s \pmod{2^{k-t}}}}^{2^{k-1}-1} \left| A_{j+2^{k-t-1}}^{(\mathbf{w})} \right|, 1 \le wt(\mathbf{w}) \le \ell,$$

for all $0 \le s \le 2^{k-t-1} - 1$.

Proof If $t = 0$, the result follows from [10, Corollary 3]. Assume now that $1 \le t \le k-1$. We first note that $\zeta_{2^k}^{2^t}$ is a 2^{k-t}-complex root of 1. We write

$$\begin{aligned}
&\mathcal{H}_{2^t f}(\mathbf{u})\overline{\mathcal{H}_{2^t f}(\mathbf{u})} \\
&= \sum_{j=0}^{2^{k-1}-1} \sum_{\mathbf{w}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{w}} \zeta_{2^k}^{2^t\cdot j} \left(|A_j^{(\mathbf{w})}| - |A_{j+2^{k-t-1}}^{(\mathbf{w})}|\right) \\
&= \sum_{s=0}^{2^{k-t-1}-1} \sum_{\mathbf{w}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{w}} \zeta_{2^{k-t}}^{s} \left(\left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_j^{(\mathbf{w})} \right| - \left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_{j+2^{k-t-1}}^{(\mathbf{w})} \right| \right).
\end{aligned} \tag{7}$$

Let $\mathbf{v} \ne \mathbf{0}$ be a fixed vector. Then, using (7) and [6, p.11], we write

$$\begin{aligned}
\mathcal{C}_{2^t f}(\mathbf{v}) &= 2^n \sum_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{H}_{2^t f}(\mathbf{u})|^2 (-1)^{\mathbf{u}\cdot\mathbf{v}} \\
&= 2^n \sum_{\mathbf{u}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{v}} \sum_{s=0}^{2^{k-t-1}-1} \sum_{\mathbf{w}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{w}} \zeta_{2^{k-t}}^{s} \\
&\quad \cdot \left(\left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_j^{(\mathbf{w})} \right| - \left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_{j+2^{k-t-1}}^{(\mathbf{w})} \right| \right) \\
&= 2^n \sum_{s=0}^{2^{k-t-1}-1} \zeta_{2^{k-t}}^{s} \sum_{\mathbf{w}\in\mathbb{F}_2^n} \left(\left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_j^{(\mathbf{w})} \right| - \left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_{j+2^{k-t-1}}^{(\mathbf{w})} \right| \right) \\
&\qquad \cdot \sum_{\mathbf{u}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot(\mathbf{v}+\mathbf{w})} \\
&= 2^{2n} \sum_{j=0}^{2^{k-t-1}-1} \zeta_{2^{k-t}}^{j} \left(\left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_j^{(\mathbf{v})} \right| - \left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_{j+2^{k-t-1}}^{(\mathbf{v})} \right| \right).
\end{aligned}$$

Since $|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0, j > 0$, if $\left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_j^{(\mathbf{v})} \right| = \left| \bigcup_{j\equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_{j+2^{k-t-1}}^{(\mathbf{v})} \right|$, $1 \le wt(\mathbf{v}) \le \ell$, for all $0 \le s \le 2^{k-t-1}-1$, then $\mathcal{C}_{2^t f}(\mathbf{v}) = 0$ for all $1 \le wt(\mathbf{v}) \le \ell$, and so, f is 2^t-$gPC(\ell)$.

Conversely, we assume that f is 2^t-$gPC(\ell)$, and so, $\mathcal{C}_{2^t f}(\mathbf{v}) = 0$, for all $1 \le wt(\mathbf{v}) \le \ell$. Now, since $|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0$, for all $j > 0$, then (7) becomes

$$\sum_{s=0}^{2^{k-t-1}-1} \zeta_{2^{k-t-1}}^{s} X_s^{(\mathbf{v})} = 0,$$

where

$$X_s^{(\mathbf{v})} := \left| \bigcup_{j \equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_j^{(\mathbf{v})} \right| - \left| \bigcup_{j \equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} A_{j+2^{k-t-1}}^{(\mathbf{v})} \right|.$$

Since the set $\{\zeta_{2^{k-t-1}}^s : 0 \le s \le 2^{k-t-1}-1\}$ is a basis for $\mathbb{Q}(\zeta_{2^{k-t}})$, we infer that $X_s^{(\mathbf{v})} = 0$, for all $1 \le wt(\mathbf{v}) \le \ell$, and the theorem is shown. $\square$

The following corollary is similar to [10, Corollary 3].

Corollary 12 *Let $f \in \mathcal{GB}_n^{2^k}$. Then, f is 2^t-gbent if and only if*

$$\sum_{j \equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} \left| A_j^{(\mathbf{v})} \right| = \sum_{j \equiv s \pmod{2^{k-t}}}^{2^{k-1}-1} \left| A_{j+2^{k-t-1}}^{(\mathbf{v})} \right|,$$

for all $\mathbf{v} \neq \mathbf{0}$.

2.2 The odd case

In this section, we are going to study the case where $|\mathcal{H}_{2^t f}(\mathbf{u})|$ is not necessarily an integer but is in $\mathbb{Z}[\sqrt{2}]$. If n is odd and $f \in \mathcal{GB}_n^{2^k}$ is 2^t-gbent, then $|\mathcal{H}_{2^t f}(\mathbf{u})| = 2^{\frac{n}{2}} = 2^{\frac{n-1}{2}}\sqrt{2}$, for any $\mathbf{u}$. If f is generalized $(2^t, s)$-plateaued with $n+s$ odd, then $|\mathcal{H}_{2^t f}(\mathbf{u})| = 2^{\frac{n+s}{2}} \in \{0, 2^{\frac{n+s-1}{2}}\sqrt{2}\}$. In that case, we have to consider separately the case where $k = 2$ and $k \ge 3$ since $\sqrt{2} \in \mathbb{Z}[\zeta_8] \setminus \mathbb{Z}[i]$. Furthermore, contrary to the even case, we are not going to apply directly the results of [9] when $k \ge 3$. To this end, let us indicate that Lemma 7 is true even if $n+s$ is odd if $k \ge 3$.

Lemma 13 *Suppose that $k \ge 3$. Let $\mathbf{u} \in \mathbb{F}_2^n$. Let s be an nonnegative integer such that $n+s$ is odd. If $|\mathcal{H}_{2^t f}(\mathbf{u})| = 2^{\frac{n+s}{2}}$, then*

$$\mathcal{H}_{2^t f}(\mathbf{u}) = 2^{\frac{n+s}{2}} \zeta_{2^{k-t}}^{b_{t,\mathbf{u}}}, \tag{8}$$

for some $b_{t,\mathbf{u}} \in \mathbb{Z}_{2^{k-t}}$.

Remark 14 *We exclude the case where $t = k-1$ because $2^{k-1}f = a_0$ is a Boolean function and $\mathcal{H}_{2^{k-1}f}(\mathbf{u}) = \mathcal{W}_{a_0}(u) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{a_0(\mathbf{x}) + \langle \mathbf{u}, \mathbf{x} \rangle} \in \mathbb{Z}$. Thus, $\mathcal{H}_{2^{k-1}f}(\mathbf{u})$ cannot be equal to $2^{\frac{n+s}{2}}$ if $n+s$ is odd. In other words, there is no $\mathbb{Z}_{2^k}$-plateaued functions such that $|\mathcal{H}_{2^t f}(\mathbf{u})| \in \{0, 2^{\frac{n+s}{2}}\}$ for any $0 \le t \le k-1$.*

Remark 15 *If $k = 2$, $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$ and $W_K = \{\pm 1, \pm i\}$. Let $\alpha = a + ib \in \mathcal{O}_K$ be of modulus $2^{\frac{n+s}{2}}$. Then, $a^2 + b^2 = 2^{n+s}$. Since $n+s$ is odd, this diophantine equation has solutions $a, b \in \{\pm 2^{\frac{n+s-1}{2}}\}$. Therefore, $\alpha = 2^{\frac{n+s-1}{2}}(\pm 1 \pm i) = 2^{\frac{n+s}{2}} \frac{\pm 1 \pm i}{\sqrt{2}}$, that is, $2^{-\frac{n+s}{2}}\alpha \notin W_K$.*

In [17], a similar result as in Theorem 8 has been established when $n+s$ is odd. In the sequel, we are going to get a more precise statement than that of [17]. For that, we deduce from the preceding lemma a result on the sums $S_{\mathbf{v}}^{(t)}(\mathbf{u})$ defined by (3). From now on, we shall sometimes use the symbol $\oplus$ to denote the addition modulo 2.

Lemma 16 *Suppose that $k \geq 3$. Let $0 \leq t \leq k-1$. Let $\mathbf{u} \in \mathbb{F}_2^n$. Let s be a nonnegative integer such that $n+s$ is odd. Suppose that $|\mathcal{H}_{2^t f}(\mathbf{u})| = 2^{\frac{n+s}{2}}$. Then, there exists $h = \sum_{i=0}^{k-t-1} 2^i b_i$ from $\mathbb{F}_2^n$ to $\mathbb{Z}_2^{k-t}$ such that, for $\mathbf{v} \in \mathbb{Z}_{k-t-1}$,*

$$S_{\mathbf{v}}^{(t)}(\mathbf{u}) = \begin{cases} (-1)^{b_{k-t-1}(\mathbf{u})+b_{k-t-2}(\mathbf{u})b_{k-t-3}(\mathbf{u})} 2^{\frac{n+s-1}{2}} & \text{if } \sum_{i=0}^{k-t-2} 2^i v_i = \nu(\mathbf{u}), \\ (-1)^{1+b_{k-t-1}(\mathbf{u})+b_{k-t-2}(\mathbf{u})+b_{k-3}(\mathbf{u})+b_{k-t-2}(\mathbf{u})b_{k-t-3}(\mathbf{u})} 2^{\frac{n+s-1}{2}} & \\ \qquad \text{if } \sum_{i=0}^{k-2} 2^i v_i = (\nu(\mathbf{u}) + 2^{k-2}) \mod 2^{k-1}, & \\ 0, \ \text{otherwise} & \end{cases}$$

where $\nu(\mathbf{u}) = \sum_{i=0}^{k-t-4} 2^i b_i(\mathbf{u}) + 2^{k-t-3}(b_{k-3}(\mathbf{u}) \oplus 1) + 2^{k-t-2}(b_{k-t-3}(\mathbf{u}) \oplus b_{k-t-2}(\mathbf{u}))$.

Proof According to Lemma 13, for any $\mathbf{u} \in \mathbb{F}_2^n$, $\mathcal{H}_{2^t f}(\mathbf{u}) = 2^{\frac{n+s}{2}} \zeta_{2^{k-t}}^{b_{t,\mathbf{u}}}$, for some $b_{t,\mathbf{u}} = \sum_{i=0}^{k-t-1} 2^i b_i(\mathbf{u}) \in \mathbb{Z}_{2^{k-t}}$. Hence, since $\sqrt{2} = \zeta_8 - \zeta_8^3$,

$$\begin{aligned} \mathcal{H}_{2^t f}(\mathbf{u}) &= (-1)^{b_{k-t-1}(\mathbf{u})} 2^{\frac{n+s-1}{2}} \sqrt{2}\, \zeta_{2^{k-t}}^{\sum_{i=0}^{k-t-2} 2^i b_i(\mathbf{u})} \\ &= (-1)^{b_{k-t-1}(\mathbf{u})} 2^{\frac{n+s-1}{2}} \left(\zeta_{2^{k-t}}^{2^{k-t-3}} - \zeta_{2^{k-t}}^{2^{k-t-3}+2^{k-t-2}} \right) \zeta_{2^{k-t}}^{\sum_{i=0}^{k-t-2} 2^i b_i(\mathbf{u})} \\ &= (-1)^{b_{k-t-1}(\mathbf{u})} 2^{\frac{n+s-1}{2}} \zeta_{2^{k-t}}^{\sum_{i=0}^{k-t-2} 2^i b_i(\mathbf{u}) + 2^{k-t-3}} \\ &\qquad + (-1)^{1+b_{k-t-1}(\mathbf{u})} 2^{\frac{n+s-1}{2}} \zeta_{2^{k-t}}^{\sum_{i=0}^{k-t-2} 2^i b_i(\mathbf{u}) + 2^{k-t-3} + 2^{k-t-2}}. \end{aligned}$$

Now, $a + b = (a \oplus b) + 2ab$ for a and b in $\mathbb{Z}_2$. Therefore,

$$\begin{aligned} &\sum_{i=0}^{k-t-2} 2^i b_i(\mathbf{u}) + 2^{k-t-3} \\ &\quad = \sum_{i=0}^{k-t-4} 2^i b_i(\mathbf{u}) + 2^{k-t-3}(b_{k-t-3}(\mathbf{u}) \oplus 1) + 2^{k-t-2}(b_{k-t-3}(\mathbf{u}) \oplus b_{k-t-2}(\mathbf{u})) \\ &\qquad + 2^{k-t-1} b_{k-t-3}(\mathbf{u}) b_{k-t-2}(\mathbf{u}) \\ &\sum_{i=0}^{k-t-2} 2^i b_i(\mathbf{u}) + 2^{k-t-3} + 2^{k-t-2} \\ &\quad = \sum_{i=0}^{k-t-4} 2^i b_i(\mathbf{u}) + 2^{k-t-3}(b_{k-t-3}(\mathbf{u}) \oplus 1) + 2^{k-t-2}(b_{k-t-3}(\mathbf{u}) \oplus b_{k-t-2}(\mathbf{u}) \oplus 1) \\ &\qquad + 2^{k-t-1}(b_{k-t-3}(\mathbf{u}) \oplus b_{k-t-2}(\mathbf{u}) \oplus b_{k-t-3}(\mathbf{u}) b_{k-t-2}(\mathbf{u})). \end{aligned}$$

Finally, we get

$$\mathcal{H}_{2^t f}(\mathbf{u}) = (-1)^{b_{k-t-1}(\mathbf{u})+b_{k-t-3}(\mathbf{u})b_{k-t-2}(\mathbf{u})} 2^{\frac{n+s-1}{2}} \zeta_{2^{k-t}}^{\nu(\mathbf{u})} + (-1)^{1+b_{k-t-1}(\mathbf{u})+b_{k-t-3}(\mathbf{u})+b_{k-t-2}(\mathbf{u})+b_{k-t-3}(\mathbf{u})b_{k-t-2}(\mathbf{u})} \times 2^{\frac{n+s-1}{2}} \zeta_{2^{k-t}}^{(\nu(\mathbf{u})+2^{k-t-2}) \bmod 2^{k-t-1}},$$

and the lemma is shown. □

One then rewrites the result of [17, Theorem 3.2] as follows.

Theorem 17 *Suppose that $k \geq 3$. Let $f = \sum_{i=0}^{k-1} 2^i a_i$. Let $0 \leq t \leq k-1$. Suppose that n is odd (respectively, let s be a positive integer such that $n+s$ is odd). Then, f is 2^t-gbent (respectively, f is generalized $(2^t, s)$-plateaued) if and only if, for any $\mathbf{d} \in \mathbb{Z}_2^{k-t-1}$, $f_{t,\mathbf{d}}$ is semibent (respectively, $(s+1)$-plateaued), $\mathcal{W}_{a_{k-t-1}}(\mathbf{u})\mathcal{W}_{a_{k-t-1}+a_{k-t-2}}(\mathbf{u}) = 0$ for any $\mathbf{u} \in \mathbb{F}_2^n$ and there exists $h = (h_0, \ldots, h_{k-t-3})$ from $\mathbb{F}_2^n$ to $\mathbb{Z}_2^{k-t-2}$ such that, for $\mathbf{u} \in \mathbb{F}_2^n$ and $\mathbf{d} \in \mathbb{Z}_2^{k-t-1}$,*

$$\mathcal{W}_{f_{t,\mathbf{d}}}(\mathbf{u}) = \mathcal{W}_{a_{k-t-1}+d_{k-t-2}a_{k-t-2}}(\mathbf{u})(-1)^{\sum_{i=0}^{k-t-3} d_i h_i(\mathbf{u})}. \quad (9)$$

Proof If we apply (4) and Lemma 16, we get

$$\mathcal{W}_{f_{t,\mathbf{d}}}(\mathbf{u}) = 2^{\frac{n+s-1}{2}} (-1)^{b_{k-t-1}(\mathbf{u})+b_{k-t-2}(\mathbf{u})b_{k-3}(\mathbf{u})} \left(1 - (-1)^{d_{k-2}+b_{k-t-2}(\mathbf{u})+b_{k-3}(\mathbf{u})}\right) \times (-1)^{\sum_{i=0}^{k-t-4} d_i b_i(\mathbf{u}) + d_{k-t-3}(b_{k-t-3} \oplus 1) + d_{k-t-2}(b_{k-t-2}(\mathbf{u}) \oplus b_{k-t-3}(\mathbf{u}))}.$$

Observe that

$$\mathcal{W}_{a_{k-t-1}}(\mathbf{u}) = \begin{cases} 0 & \text{if } b_{k-t-2}(\mathbf{u}) \oplus b_{k-t-3}(\mathbf{u}) = 0 \\ 2^{\frac{n+s+1}{2}} (-1)^{b_{k-t-1}(\mathbf{u})+b_{k-t-2}(\mathbf{u})b_{k-3}(\mathbf{u})} & \text{if } b_{k-t-2}(\mathbf{u}) \oplus b_{k-t-3}(\mathbf{u}) = 1 \end{cases}$$

and

$$\mathcal{W}_{a_{k-t-1}+a_{k-t-2}}(\mathbf{u}) = \begin{cases} 2^{\frac{n+s+1}{2}} (-1)^{b_{k-t-1}(\mathbf{u})+b_{k-t-2}(\mathbf{u})b_{k-3}(\mathbf{u})+b_{k-t-2}(\mathbf{u})+b_{k-3}(\mathbf{u})} \\ \qquad \text{if } b_{k-t-2}(\mathbf{u}) \oplus b_{k-t-3}(\mathbf{u}) = 0 \\ 0 \text{ if } b_{k-t-2}(\mathbf{u}) \oplus b_{k-t-3}(\mathbf{u}) = 1 \end{cases}$$

yielding (9) and that the Walsh supports of a_{k-t-1} and $a_{k-t-1} + a_{k-t-2}$ are disjoint. □

Let us now discuss the case where $k = 2$. In that case, one has only to consider the bentness of f. In that case, if $f = a_0 + 2a_1$,

$$\mathcal{H}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} i^{f(x)} (-1)^{\langle \mathbf{u}, \mathbf{x} \rangle} = S_0(\mathbf{u}) + iS_1(\mathbf{u}),$$

where, for $\epsilon \in \mathbb{Z}_2$,

$$S_\epsilon(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n : a_0(\mathbf{x}) = \epsilon} (-1)^{a_1(x) + \langle \mathbf{u}, \mathbf{x} \rangle}.$$

According to Remark 15, if f is gbent then $S_0(\mathbf{u}) + iS_1(\mathbf{u}) = 2^{\frac{n-1}{2}}(\pm 1 \pm i)$, that is, $S_0(\mathbf{u}) = \pm 2^{\frac{n-1}{2}}$ and $S_1(\mathbf{u}) = \pm 2^{\frac{n-1}{2}}$. Therefore, for any $d \in \mathbb{Z}_2$,

$$\mathcal{W}_{f_d}(\mathbf{u}) = S_0(\mathbf{u}) + (-1)^d S_1(\mathbf{u}) = 2^{\frac{n-1}{2}}(\pm 1 \pm (-1)^d) \in \{0, \pm 2^{\frac{n+1}{2}}\}.$$

That implies that f_0 and f_1 are semibent. But also, $\mathcal{W}_{f_0}(\mathbf{u})\mathcal{W}_{f_1}(\mathbf{u}) = S_0^2(\mathbf{u}) - S_1^2(\mathbf{u}) = 0$, that is, f_0 and f_1 have disjoint Walsh support. Conversely, suppose that f_0 and f_1 are semibent and have disjoint Walsh support. Then, $S_0(\mathbf{u}) = \frac{1}{2}(\mathcal{W}_{f_0}(\mathbf{u}) + \mathcal{W}_{f_1}(\mathbf{u}))$ and $S_1(\mathbf{u}) = \frac{1}{2}(\mathcal{W}_{f_0}(\mathbf{u}) - \mathcal{W}_{f_1}(\mathbf{u}))$ are in $\{0, \pm 2^{\frac{n-1}{2}}\}$. Therefore, $|\mathcal{H}_f(\mathbf{u})|^2 = S_0^2(\mathbf{u}) + S_1^2(\mathbf{u}) \in \{0, 2^{n-1}, 2^n\}$. Because of Parseval identity, that implies that $|\mathcal{H}_f(\mathbf{u})|^2 = 2^n$. Thus, we get an alternative proof of the following theorem (shown first in [20]).

Theorem 18 *Let $f = a_0 + 2a_1$ be a function from $\mathbb{F}_2^n$ to $\mathbb{Z}_4$. Then f is gbent if and only if a_1 and $a_0 + a_1$ are semibent with disjoint Walsh support.*

Remark 19 *If $f = a_0 + 2a_1$ is a generalized s-plateaued with $s > 0$, we can repeat the beginning of the previous argument, and prove that a_0 and a_1 are $(s+1)$-plateaued and have disjoint support. However, we get $|\mathcal{H}_f(\mathbf{u})|^2 = S_0^2(\mathbf{u}) + S_1^2(\mathbf{u}) \in \{0, 2^{n+s-1}, 2^{n+s}\}$ from which we cannot deduce from the Parseval identity that f is generalized s-plateaued.*

2.3 Characterizing plateauedness in terms of Fourier sums

We modify some proofs of [15,17] to find characterizations of $(2^t, \cdot)$-plateaued functions in terms of second derivatives and fourth moments.

Theorem 20 *Let $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ and $0 \le t \le k-1$. Then f is $(2^t, s)$-plateaued with respect to the transform $\mathcal{H}_{2^t f}$ if and only if $\sum_{\mathbf{a},\mathbf{b} \in \mathbb{V}_n} \zeta_{2^{k-t}}^{D_{\mathbf{b}} D_{\mathbf{a}} f(\mathbf{x})} = 2^{n+s}$, for all $\mathbf{x}$, if and only if $\sum_{\mathbf{d} \in \mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^4 = 2^{3n+s}$.*

Proof We follow [17] with the appropriate modifications. We fix $\mathbf{x} \in \mathbb{V}_n$ and observe that $\sum_{\mathbf{a},\mathbf{b} \in \mathbb{V}_n} \zeta_{2^k}^{2^t D_{\mathbf{b}} D_{\mathbf{a}} f(\mathbf{x})} = 2^{n+s}$ is equivalent to

$$\sum_{\mathbf{a},\mathbf{b} \in \mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}+\mathbf{b}) - f(\mathbf{x}+\mathbf{b}) - f(\mathbf{x}+\mathbf{a})} = 2^{n+s} \zeta_{2^{k-t}}^{-f(\mathbf{x})}.$$

This is further equivalent to the equality of the extended Fourier 2^t-transforms of $F_1(\mathbf{x}) := \sum_{\mathbf{a},\mathbf{b} \in \mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}+\mathbf{b}) - f(\mathbf{x}+\mathbf{b}) - f(\mathbf{x}+\mathbf{a})}$ and $F_2(\mathbf{x}) := 2^{n+s} \zeta_{2^{k-t}}^{-f(\mathbf{x})}$ at all $\mathbf{u} \in \mathbb{V}_n$, that is,

$$\sum_{\mathbf{x},\mathbf{a},\mathbf{b} \in \mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}+\mathbf{b}) - f(\mathbf{x}+\mathbf{b}) - f(\mathbf{x}+\mathbf{a})} (-1)^{\langle \mathbf{u},\mathbf{x} \rangle} = 2^{n+s} \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^{k-t}}^{-f(\mathbf{x})} (-1)^{\langle \mathbf{u},\mathbf{x} \rangle}. \tag{10}$$

The left hand side of (10), setting $\mathbf{a}_1 := \mathbf{x}+\mathbf{a}, \mathbf{b}_1 := \mathbf{x}+\mathbf{b}$, becomes (we use below the identity $\langle \mathbf{u},\mathbf{x}\rangle = \langle \mathbf{u},\mathbf{a}_1\rangle + \langle \mathbf{u},\mathbf{b}_1\rangle + \langle \mathbf{u},\mathbf{x}+\mathbf{a}_1+\mathbf{b}_1\rangle$)

$$\begin{aligned}
&\sum_{\mathbf{x},\mathbf{a},\mathbf{b}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}+\mathbf{b})-f(\mathbf{x}+\mathbf{b})-f(\mathbf{x}+\mathbf{a})}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle}\\
&= \sum_{\mathbf{x},\mathbf{a}_1,\mathbf{b}_1\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}_1+\mathbf{b}_1)-f(\mathbf{b}_1)-f(\mathbf{a}_1)}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle}\\
&= \sum_{\mathbf{b}_1\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{b}_1)}(-1)^{\langle \mathbf{u},\mathbf{b}_1\rangle} \sum_{\mathbf{a}_1\in\mathbb{V}_n} \zeta_{2^{k-t}}^{-f(\mathbf{a}_1)}(-1)^{\langle \mathbf{u},\mathbf{a}_1\rangle}\\
&\qquad\cdot \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}_1+\mathbf{b}_1)}(-1)^{\langle \mathbf{u},\mathbf{x}+\mathbf{a}_1+\mathbf{b}_1\rangle}\\
&= \overline{\mathcal{H}_{2^t f}(\mathbf{u})}\,\overline{\mathcal{H}_{2^t f}(\mathbf{u})}\,\mathcal{H}_f(\mathbf{u}) = |\mathcal{H}_{2^t f}(\mathbf{u})|^2\,\overline{\mathcal{H}_{2^t f}(\mathbf{u})}.
\end{aligned}$$

The right hand side of (10) is also

$$2^{n+s}\sum_{\mathbf{x}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{-f(\mathbf{x})}(-1)^{\langle \mathbf{u},\mathbf{x}\rangle} = 2^{n+s}\overline{\mathcal{H}_{2^t f}(\mathbf{u})},$$

therefore (10) is equivalent to $|\mathcal{H}_{2^t f}(\mathbf{u})|^2\,\overline{\mathcal{H}_{2^t f}(\mathbf{u})} = 2^{n+s}\,\overline{\mathcal{H}_{2^t f}(\mathbf{u})}$, which implies, $|\mathcal{H}_{2^t f}(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$.

Next, using [21, Theorem 1], we see that

$$\begin{aligned}
\sum_{\mathbf{a},\mathbf{b}\in\mathbb{V}_n} \zeta_{2^k}^{2^t D_{\mathbf{b}} D_{\mathbf{a}} f(\mathbf{x})} &= \sum_{\mathbf{a},\mathbf{b}\in\mathbb{V}_n} \zeta_{2^k}^{2^t(f(\mathbf{x}+\mathbf{a}+\mathbf{b})-f(\mathbf{x}+\mathbf{b})-f(\mathbf{x}+\mathbf{a})+f(\mathbf{x}))}\\
&= \sum_{\mathbf{a}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{a})} \sum_{\mathbf{b}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x}+\mathbf{a}+\mathbf{b})-f(\mathbf{x}+\mathbf{b})} \text{ setting } \mathbf{c} := \mathbf{x}+\mathbf{b}\\
&= \sum_{\mathbf{a}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{a})} \sum_{\mathbf{c}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{c}+\mathbf{a})-f(\mathbf{c})}\\
&= \sum_{\mathbf{a}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{a})}\mathcal{C}_f(\mathbf{a}), \text{ since } \mathcal{C}_f \text{ is always real}\\
&= 2^{-n}\sum_{\mathbf{a}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{a})} \sum_{\mathbf{d}\in\mathbb{V}_n} |\mathcal{H}_f(\mathbf{d})|^2(-1)^{\langle \mathbf{a},\mathbf{d}\rangle}\\
&= 2^{-n}\sum_{\mathbf{d}\in\mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^2 \sum_{\mathbf{a}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{a})}(-1)^{\langle \mathbf{a},\mathbf{d}\rangle}\\
&= 2^{-n}\sum_{\mathbf{d}\in\mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^2 \zeta_{2^{k-t}}^{f(\mathbf{x})}(-1)^{\langle \mathbf{x},\mathbf{d}\rangle} \sum_{\mathbf{c}\in\mathbb{V}_n} \zeta_{2^{k-t}}^{-f(\mathbf{c})}(-1)^{\langle \mathbf{c},\mathbf{d}\rangle}\\
&= 2^{-n}\sum_{\mathbf{d}\in\mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^2 \zeta_{2^{k-t}}^{f(\mathbf{x})}(-1)^{\langle \mathbf{x},\mathbf{d}\rangle}\overline{\mathcal{H}_{2^t f}(\mathbf{d})}.
\end{aligned}$$

Thus,

$$2^{2n+s} = \sum_{\mathbf{x},\mathbf{a},\mathbf{b}\in\mathbb{V}_n} \zeta_{2^k}^{2^t D_{\mathbf{b}} D_{\mathbf{a}} f(\mathbf{x})} = 2^{-n}2^{-n}\sum_{\mathbf{d}\in\mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^2 \zeta_{2^{k-t}}^{f(\mathbf{x})}(-1)^{\langle \mathbf{x},\mathbf{d}\rangle}\overline{\mathcal{H}_{2^t f}(\mathbf{d})}$$

$$= 2^{-n} \sum_{\mathbf{d} \in \mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^2 \overline{\mathcal{H}_{2^t f}(\mathbf{d})} \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta_{2^{k-t}}^{f(\mathbf{x})} (-1)^{\langle \mathbf{x}, \mathbf{d} \rangle} = 2^{-n} \sum_{\mathbf{d} \in \mathbb{V}_n} |\mathcal{H}_{2^t f}(\mathbf{d})|^4,$$

and the second claim is shown. □

3 Conclusion

In this paper, we present a deeper study of generalized bent and, more generally, generalized plateaued functions in characteristic 2 than those presented in the previous literature. We clarify and simplify statements of several results of [9, 11]. In those papers, the bentness is defined according to a particular character of $\mathbb{Z}_{2^k}$. In even dimension, we characterize bent functions according to any other character of $\mathbb{Z}_{2^k}$. We notably show that those functions have similar properties to vectorial bent functions. We next clarify the case of gbent functions in odd dimension. As a by-product of our proofs, more generally, we also provide several results about plateaued functions. Furthermore, we find characterizations of 2^t-plateaued functions in terms of second derivatives and fourth moments. Even though this paper only states the results for characteristic 2, similar results can be obtained for odd characteristic. These have not been included in the paper, for reasons of brevity and clarity.

Acknowledgements: The authors deeply thank the Assoc. Edit. and the anonymous reviewers for their valuable comments, which have highly improved the manuscript.

References

1. C. Bey, G. Kyureghyan, *On Boolean functions with the sum of every two of them being bent* Des. Codes Cryptogr. 49 (2008), 341–346.
2. C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010. Available at: *www.math.univ-paris13.fr/˜carlet/pubs.html*
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*, J. Des. Codes Crypt., **78** (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* (Ed. 2), Academic Press, San Diego, CA, 2017.
7. S. Hodžić, W. Meidl, E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual and the Gray image*, IEEE Trans. Inf. Theory 64:7 (2018), 5432–5440.
8. P. V. Kumar, R. A. Scholtz, L. R. Welch, *Generalized bent functions and their properties*, J. Combin Theory – Ser. A 40 (1985), 90–107.
9. T. Martinsen, W. Meidl, S. Mesnager, P. Stănică, *Decomposing generalized bent and hyperbent functions*, IEEE Trans. Inf. Theory 63:12 (2017), 7804–7812.

10. T. Martinsen, W. Meidl, A. Pott, P. Stănică, *On symmetry and differential properties of generalized Boolean functions*, Proc. of WAIFI 2018: Arithmetic of Finite Fields, LNCS 11321 (2018), 207–223.
11. T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, Proc. of WAIFI 2016: Arithmetic of Finite Fields, LNCS 10064 (2017), 160–173.
12. T. Martinsen, W. Meidl, P. Stănică, *Partial Spread and Vectorial Generalized Bent Functions*, Designs, Codes & Cryptogr. 85:1 (2017), 1–13.
13. S. Mesnager, Bent functions: fundamentals and results. Springer, Switzerland (2016).
14. S. Mesnager, C. Tang, Y. Qi, *Generalized plateaued functions and admissible (plateaued) functions*, IEEE Trans. Inform. Theory 63 (2017), 6139–6148.
15. S. Mesnager, C. Tang, Y. Qi, L. Wang, B. Wu, and K. Feng, *Further Results on Generalized Bent Functions and Their Complete Characterization*, IEEE Trans. Inform. Theory 64:7 (2018), 5441–5452.
16. A. Pott, *Nonlinear functions in abelian groups and relative difference sets*, Optimal discrete structures and algorithms (ODSA 2000), Discrete Appl. Math. 138 (2004), 177–193.
17. C. Riera, P. Stănică, *Landscape Boolean functions*, to appear in Advances in Math. Communication, 2019. Available at: *https://arxiv.org/abs/1806.05878*.
18. B. Schmidt, *On* (p^a, p^b, p^a, p^{a-b})*-relative difference sets*, J. Algebraic Combin. 6 (1997), 279–297.
19. K. U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA*, IEEE Trans. Inform. Theory 55:4 (2009), 1824–1832.
20. 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).
21. P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes & Cryptogr. 69 (2013), 77–94.
22. C. Tang, C. Xiang, Y. Qi, K. Feng. *Complete characterization of generalized bent and* 2^k*-bent Boolean functions*, IEEE Trans. Inf. Theory 63:7 (2017), 4668–4674.
23. A. M. Youssef, G. Gong, *Hyper-bent functions*, In: Adv. Crypt. – EUROCRYPT 2001, LNCS 2045, Springer, Berlin, 2001, 406–419.
24. F. Zhang, S. Xia, P. Stănică, Y. Zhou, *Further results on constructions of generalized bent Boolean functions*, Inf. Sciences - China. 59 (2016), 1–3.
25. Y. L. Zheng, X. M. Zhang, *On plateaued functions*, IEEE Trans. Inf. Theory 47:9 (2001), 1215–1223.