# On symmetry and differential properties of generalized Boolean functions

Thor Martinsen[1], Wilfried Meidl[2], Alexander Pott[3], Pantelimon Stănică[1]

[1] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA; {tmartins,pstanica}@nps.edu
[2] Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria; meidlwilfried@gmail.com
[3] Institute of Algebra and Geometry, Faculty of Mathematics, Otto von Guericke University Magdeburg, Universitätsplatz 2, 39106, Magdeburg, Germany; alexander.pott@ovgu.de

**Abstract.** In this paper we investigate various differential properties of generalized Boolean functions defined on $\mathbb{F}_2^n$ with values in $\mathbb{Z}_{2^k}$, $k \geq 2$. We characterize linear structures for the generalized Boolean functions in terms of their binary expansion components, and find all symmetric generalized bent functions. Next, we show that there are no symmetric balanced functions defined on $\mathbb{F}_2^n$ with values in a group of order $2^k, k \geq 2$, a contrast to the classical case for $k = 1$, commonly known as the bisection of binomial coefficients. Further, we characterize the avalanche features of a generalized Boolean function in terms of differentials. Lastly, we show that a partially gbent function is plateaued.

**Keywords:** Generalized Boolean functions; linear structures; generalized bent; semibent; partially bent; avalanche features; plateaued.

## 1 Introduction

In [27], Schmidt found a connection between words in multi-carrier code-division multiple access (MC-CDMA) systems and generalized bent functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_4$, as well as functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_q$ were considered from the viewpoint of cyclic codes over rings. Shortly thereafter, generalized Boolean functions became an active area of research [17,21,23,24,27,28,29]. Many authors [8,9,18] have investigated linear structures of Boolean functions. However, thus far, little has been written about linear structures, symmetry, balancedness and avalanche features of generalized Boolean functions.

Let $\mathbb{V}_n$ be an $n$-dimensional vector space over the two-element field $\mathbb{F}_2$ and for an integer $q$, let $\mathbb{Z}_q$ be the ring of integers modulo $q$. By '$+$' and '$-$' we respectively denote addition and subtraction modulo $q$, whereas '$\oplus$' denotes the addition over $\mathbb{V}_n$. 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

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

It has been observed, see [14,22,23,30], that the Boolean functions $a_i$, and furthermore all Boolean functions of the form $a_{k-1} \oplus c_{k-2}a_{k-2} \oplus \cdots \oplus c_0 a_0$, $c_i \in \mathbb{F}_2$, $0 \leq i \leq k-2$, play an important role in the analysis of properties of functions $f \in \mathcal{GB}_n^q$. In accordance with the terminology for vectorial bent functions, we call those Boolean functions *components* of $f$ or *component functions* of $f$.

If $\mathbb{V}_n$ is $\mathbb{F}_2^n$, then 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, 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

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

where $\zeta_q = e^{\frac{2\pi i}{q}}$ and $\mathbf{u} \cdot \mathbf{x}$ denotes a (nondegenerate) inner product on $\mathbb{V}_n$ (for easy writing, we sometimes use $\zeta$, $\mathcal{H}_f$, instead of $\zeta_q$, respectively, $\mathcal{H}_f^{(q)}$, when $q$ is fixed). If $\mathbb{V}_n = \mathbb{F}_2^n$, the vector space of the $n$-tuples over $\mathbb{F}_2$, then for $\mathbf{u} \cdot \mathbf{x}$ we use the conventional dot product. For $q = 2$, we obtain the usual *Walsh-Hadamard transform*

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

The sum

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

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 $\mathcal{C}_f(\mathbf{u})$. Recall [29] that if $f, g \in \mathcal{GB}_n^q$, then

$$\sum_{\mathbf{u} \in \mathbb{V}_n} \mathcal{C}_{f,g}(\mathbf{u})(-1)^{\mathbf{u} \cdot \mathbf{x}} = \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})},$$

$$\mathcal{C}_{f,g}(\mathbf{u}) = 2^{-n} \sum_{\mathbf{x} \in \mathbb{V}_n} \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}(-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

Taking the particular case $f = g$ we obtain

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

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 Boolean function $f$ 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 then also call $f$ *s-plateaued*). If $s = 1$ ($n$ must then be odd), or $s = 2$ ($n$ must then be even), we call $f$ semibent.

Given a Boolean function $f$, the derivative of $f$ with respect to a vector $\mathbf{a}$, denoted by $D_{\mathbf{a}} f$, is the Boolean function defined by

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

For more on Boolean functions, the reader can consult the following excellent references [1,2,3,7,25,31].

## 2 Derivatives and linear structures in the generalized Boolean functions' context

Given a generalized Boolean function $f : \mathbb{V}_n \to \mathbb{Z}_q$, we define the *derivative* $D^{(q)}_{\mathbf{a}} f$ of $f$ with respect to a vector $\mathbf{a} \in \mathbb{V}_n$ to be the generalized Boolean function $D^{(q)}_{\mathbf{a}} f : \mathbb{V}_n \to \mathbb{Z}_q$

$$D^{(q)}_{\mathbf{a}} f(\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{V}_n.$$

When there is no danger of confusion, we write $D_{\mathbf{a}} f$ in lieu of $D^{(q)}_{\mathbf{a}} f$.

We say that $\mathbf{a} \in \mathbb{V}_n$ is a *linear structure* of a generalized Boolean function $f \in \mathcal{GB}^q_n$ if the derivative of $f$ with respect to $\mathbf{a}$ is constant, that is, $f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x}) = c \in \mathbb{Z}_q$ constant, for all $\mathbf{x} \in \mathbb{V}_n$. Observe that if $\mathbf{a}_1, \mathbf{a}_2$ are linear structures for $f$, then there are constants $c_1, c_2$ such that $f(\mathbf{x} \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) - f(\mathbf{x} \oplus \mathbf{a}_2) = c_1$, $f(\mathbf{x} \oplus \mathbf{a}_2) - f(\mathbf{x}) = c_2$, for all $\mathbf{x}$, which by summing renders $f(\mathbf{x} \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) - f(\mathbf{x}) = c_1 + c_2$ for all $\mathbf{x}$. Thus, we see that the set of all linear structures (including $\mathbf{0}$) forms a vector subspace in $\mathbb{V}_n$, which we will denote by $LS_q(f)$ (and when $q$ is fixed, we may write $LS(f)$). From here on, we let $q = 2^k$.

We begin with a characterization for the linear structures of a generalized Boolean function in terms of the generalized Walsh-Hadamard transform. Let $S_f = \{\mathbf{x} \in \mathbb{V}_n \,|\, \mathcal{H}_f(\mathbf{x}) \neq 0\}$ (the generalized Walsh-Hadamard support) and for a vector $\mathbf{a}$, let $\mathbf{a}^{\perp}$ be the orthogonal complement of $\mathbf{a}$, that is, $\mathbf{a}^{\perp} = \{\mathbf{x} \in \mathbb{V}_n \,|\, \mathbf{a} \cdot \mathbf{x} = 0\}$. This is a terminology widely used in linear algebra, although there may be a nontrivial intersection between a subspace and its orthogonal complement. From Parseval's identity, we immediately infer that $S_f \neq \emptyset$.

We might be tempted to conjecture that linear structures for the components transfer to linear structures for the generalized Boolean function, but that is not

true, as we argue next: for example, let $n \geq 3, k \geq 2$, and $f(\mathbf{x}) = a_0(\mathbf{x})$ in $\mathcal{GB}_n^{2^k}$, where $a_0(x_1, \ldots, x_n) = x_1 \cdots x_{n-2}(x_{n-1} \oplus x_n)$ in $\mathcal{B}_n$. We observe that $(0, \ldots, 1, 1) \in LS_2(a_0)$, since $f(x_1, \ldots, x_{n-1} \oplus 1, x_n \oplus 1) = f(x_1, \ldots, x_{n-1}, x_n)$ over $\mathbb{F}_2$. However, $f(x_1, \ldots, x_{n-1} \oplus 1, x_n \oplus 1) = f(x_1, \ldots, x_{n-1}, x_n) + 2x_1 \cdots x_{n-2}$ over $\mathbb{Z}_{2^k}$, thus, $D_{\mathbf{a}} f(\mathbf{x}) = 2x_1 \cdots x_{n-2}$, and therefore $(0, \ldots, 0, 1, 1) \notin LS_{2^k}(f)$.

In reality, the next result settles the "score", by completely characterizing linear structures for the generalized Boolean functions in terms of their components.

**Theorem 1.** *Let $f \in \mathcal{GB}_n^{2^k}$, with $f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i a_i(\mathbf{x})$, $a_i \in \mathcal{B}_n$. The following are equivalent:*

*(i) The vector $\mathbf{a}$ is a linear structure for $f$.*
*(ii) The vector $\mathbf{a}$ satisfies $\zeta^{f(\mathbf{a})-f(\mathbf{0})} = (-1)^{\mathbf{a}\cdot\mathbf{w}}$, for all $\mathbf{w} \in S_f$.*
*(iii) The vector $\mathbf{a}$ is a linear structure for $a_i$, $i \geq 0$, such that $a_i(\mathbf{a}) = a_i(\mathbf{0}), 0 \leq i < k-1$.*

*Proof.* We first show $(i) \Leftrightarrow (ii)$. Let $g(\mathbf{x}) := f(\mathbf{x} \oplus \mathbf{a}) - c$, for some constant $c \in \mathbb{Z}_{2^k}$, $\mathbf{a} \in \mathbb{V}_n$. Then

$$\begin{aligned}
\mathcal{H}_g(\mathbf{w}) &= \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta^{g(\mathbf{x})}(-1)^{\mathbf{x}\cdot\mathbf{w}} \\
&= \sum_{\mathbf{x}\in\mathbb{V}_n} \zeta^{f(\mathbf{x}\oplus\mathbf{a})-c}(-1)^{\mathbf{x}\cdot\mathbf{w}} \\
&\overset{\mathbf{y}:=\mathbf{x}\oplus\mathbf{a}}{=} \zeta^{-c}(-1)^{\mathbf{a}\cdot\mathbf{w}} \sum_{\mathbf{y}\in\mathbb{V}_n} \zeta^{f(\mathbf{y})}(-1)^{\mathbf{y}\cdot\mathbf{w}} \\
&= \zeta^{-c}(-1)^{\mathbf{a}\cdot\mathbf{w}}\mathcal{H}_f(\mathbf{w}).
\end{aligned}$$

Now, if $\mathbf{a}$ is a linear structure, then (with the above notation) $g(\mathbf{x}) = f(\mathbf{x})$ (where $c = f(\mathbf{a}) - f(\mathbf{0})$), hence $\mathcal{H}_g(\mathbf{w}) = \mathcal{H}_f(\mathbf{w})$. Thus, $\zeta^{-c}(-1)^{\mathbf{a}\cdot\mathbf{w}}\mathcal{H}_f(\mathbf{w}) = \mathcal{H}_f(\mathbf{w})$, which renders $\mathcal{H}_f(\mathbf{w})\,(1 - \zeta^{-c}(-1)^{\mathbf{a}\cdot\mathbf{w}}) = 0$. Therefore, taking any $\mathbf{w} \in S_f \neq \emptyset$, we get that $\zeta^c = (-1)^{\mathbf{a}\cdot\mathbf{w}}$, and since $\zeta$ is a primitive $2^k$-root of unity, then necessarily, $c = 0$ or $2^{k-1}$, depending on whether $\mathbf{w} \in \mathbf{a}^{\perp}$, or not. The converse is also true.

Next we show $(i) \Leftrightarrow (iii)$. If $f \in \mathcal{GB}_n^{2^k}$ with $f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i a_i(\mathbf{x})$, $a_0 \in \mathcal{B}_n$, then it is easy to see (by reducing modulo 2) that if $\mathbf{a}$ is a linear structure for $f$, and consequently, $D_{\mathbf{a}}^{(2^k)} f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i \left(a_i(\mathbf{x} \oplus \mathbf{a}) - a_i(\mathbf{x})\right) = c \in \mathbb{Z}_{2^k}$, then $\mathbf{a}$ is a linear structure for $a_0$ whose derivative is $D_{\mathbf{a}}^{(2)} f(\mathbf{x}) = a_0(\mathbf{x} \oplus \mathbf{a}) \oplus a_0(\mathbf{x}) = c \pmod 2$.

Let $f \in \mathcal{GB}_n^{2^k}$ and write $f(\mathbf{x}) = a_0(\mathbf{x}) + 2f_1(\mathbf{x})$, where $a_0 \in \mathcal{B}_n$, $f_1 \in \mathcal{GB}_n^{2^{k-1}}$. Assume that $\mathbf{a}$ is a linear structure for $f$ and so, $D_{\mathbf{a}} f(\mathbf{x}) = c \in \mathbb{Z}_q$ (independent of $\mathbf{x}$). We compute $D_{\mathbf{a}} f$, and obtain (using $(ii)$)

$$D_{\mathbf{a}}(f)(\mathbf{x}) = (a_0(\mathbf{x} \oplus \mathbf{a}) - a_0(\mathbf{x})) + 2\left(f_1(\mathbf{x} \oplus \mathbf{a}) - f_1(\mathbf{x})\right) = c \in \{0, 2^{k-1}\}. \quad (1)$$

Thus, $a_0(\mathbf{x}) = a_0(\mathbf{x}\oplus\mathbf{a})$, and from Equation (1), we infer that $f_1(\mathbf{x}\oplus\mathbf{a}) - f_1(\mathbf{x}) = \dfrac{c}{2} \in \{0, 2^{k-2}\}$ in $\mathbb{Z}_{2^{k-1}}$. Therefore, $\mathbf{a}$ is a linear structure for $f_1$, in addition to

being a linear structure for $a_0$. Inductively, we infer (by the uniqueness of the binary representation) that for all $\mathbf{x}$, $a_i(\mathbf{x} \oplus \mathbf{a}) - a_i(\mathbf{x}) = 0$, for $0 \leq i < k-2$. If $a_{k-1}(\mathbf{x} \oplus \mathbf{a}) - a_{k-1}(\mathbf{x}) = 0$, then $f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x}) = 0$, and if $a_{k-1}(\mathbf{x} \oplus \mathbf{a}) - a_{k-1}(\mathbf{x}) = \pm 1$, then $f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x}) = 2^{k-1}$. Certainly, the reciprocal is true and the claim is shown. □

**Corollary 1.** *Let $f \in \mathcal{GB}_n^{2^k}$. If $\mathbf{a}$ is a linear structure for $f$, then either $S_f \subseteq \mathbf{a}^{\perp}$, or $S_f \subseteq \overline{\mathbf{a}^{\perp}}$ (the set complement of $\mathbf{a}^{\perp}$); also, if $\mathbf{a}$ is a linear structure for $f$, then $f(\mathbf{a}) - f(\mathbf{0}) \in \{0, 2^{k-1}\}$.*

*Remark 1.* It is immediate that if $f$ is a generalized bent Boolean function then $f$ has no linear structure.

Next, we will use the method of Lechner [19] and Lai [18] to simplify the algebraic normal form of a function admitting linear structures. The result is similar and we give here the proof for the reader's convenience. We shall use below the observation that if $\mathbf{a}$ is a linear structure for $f$, then $f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x}) = c$, where $c = f(\mathbf{a}) - f(\mathbf{0})$.

**Proposition 1.** *Let $f \in \mathcal{GB}_n^{2^k}$ and $1 \leq \dim LS_{2^k}(f) = r$. Then, there exists an invertible $n \times n$ matrix $A$ such that*

$$f((x_1, \ldots, x_n) \cdot A) = \sum_{i=1}^{r} \alpha_i x_i + g(x_{r+1}, \ldots, x_n),$$

*where $\alpha_i \in \mathbb{Z}_{2^k}$ and $g \in \mathcal{GB}_{n-r}^{2^k}$ is a generalized Boolean function with no linear structure.*

*Proof.* Since $\dim LS_{2^k}(f) = r$, we let $\{\mathbf{a}_1, \ldots, \mathbf{a}_r\}$ be a basis for $LS_{2^k}(f)$, which can be completed to a basis for $\mathbb{F}_2^n$, say, $\{\mathbf{a}_1, \ldots, \mathbf{a}_r, \mathbf{a}_{r+1}, \ldots, \mathbf{a}_n\}$. We now define the matrix $A$ to be the matrix corresponding to the change of basis from the canonical basis $\{e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)\}$ to the basis $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$, that is, $\mathbf{a}_i = \mathbf{e}_i A$, $1 \leq i \leq n$. Note that if $x \in \mathbb{F}_2$, then $f(x\mathbf{a}) - f(\mathbf{0}) = x\,(f(\mathbf{a}) - f(\mathbf{0}))$. Further, using the fact that $\mathbf{a}_i$ (hence $\mathbf{a}_i x_i$, as well), $1 \leq i \leq r$, are linear structures for $f$, we obtain

$$\begin{aligned}
f((x_1, \ldots, x_n) \cdot A) &= f\left(\left(\sum_{i=1}^{n} \mathbf{e}_i x_i\right) \cdot A\right) \\
&= f\left(\mathbf{a}_1 x_1 \oplus \cdots \oplus \mathbf{a}_r x_r \oplus \cdots \oplus \mathbf{a}_n x_n\right) \\
&= f\left(\mathbf{a}_2 x_2 \oplus \cdots \oplus \mathbf{a}_r x_r \oplus \cdots + \mathbf{a}_n x_n\right) + f(x_1 \mathbf{a}_1) - f(\mathbf{0}) \\
&= f\left(\mathbf{a}_2 x_2 \oplus \cdots \oplus \mathbf{a}_r x_r \oplus \cdots + \mathbf{a}_n x_n\right) + x_1\left(f(\mathbf{a}_1) - f(\mathbf{0})\right) \\
&= f\left(\mathbf{a}_3 x_3 \oplus \cdots + \mathbf{a}_n x_n\right) + x_1\left(f(\mathbf{a}_1) - f(\mathbf{0})\right) + x_2\left(f(\mathbf{a}_2) - f(\mathbf{0})\right) \\
&\cdots\cdots\cdots \\
&= \sum_{i=1}^{r} \alpha_i x_i + f(x_{r+1}\mathbf{a}_{r+1} \oplus \cdots \oplus x_n \mathbf{a}_n),
\end{aligned}$$

where $\alpha_i := f(\mathbf{a}_i) - f(\mathbf{0})$, so $g(x_{r+1}, \ldots, x_n) := f(x_{r+1}\mathbf{a}_{r+1} \oplus \cdots \oplus x_n\mathbf{a}_n)$.

To show the last claim, observe that if $(b_{r+1}, \ldots, b_n)$ is a linear structure for $g$, then $\mathbf{b} = (0, \ldots, 0, b_{r+1}, \ldots, b_n) \cdot A$ is a linear structure for $f$ (and $\mathbf{b}$ is independent of $\mathbf{a}_1, \ldots, \mathbf{a}_r$), since $A$ is invertible and

$$\begin{aligned} f(\mathbf{x} \cdot A \oplus \mathbf{b}) &= \sum_{i=1}^{r} \alpha_i x_i + g((x_{r+1}, \ldots, x_n) \oplus (b_{r+1}, \ldots, b_n)) \\ &= \sum_{i=1}^{r} \alpha_i x_i + g(x_{r+1}, \ldots, x_n) + g(b_{r+1}, \ldots, b_n) - g(\mathbf{0}) \\ &= f(\mathbf{x} \cdot A) + f(\mathbf{b}) - f(\mathbf{0}), \quad \text{for all } \mathbf{x}. \end{aligned}$$

This contradicts the fact that $\dim LS_{2^k}(f) = r$, and the theorem is shown. □

## 3 Symmetric generalized Boolean functions

In this section $\mathbb{V}_n = \mathbb{F}_2^n$, the vector space of $n$-tuples over $\mathbb{F}_2$. Savicky [26] (see also [13]) showed that for each even $n$, the only symmetric bent functions are the quadratic symmetric functions $S_{c,d}(\mathbf{x}) = s_2(\mathbf{x}) \oplus cs_1(\mathbf{x}) \oplus d$, $c, d \in \mathbb{F}_2$, where $s_1, s_2$ are the elementary symmetric polynomials of degree 1, respectively 2. In this section we show that for any (even or odd) $n$, the only symmetric generalized bent Boolean function in $\mathcal{GB}_n^{2^k}$, $k \geq 2$, is essentially the quaternary function $s_1(\mathbf{x}) + 2s_2(\mathbf{x})$. In the second part, we show that there is no balanced symmetric generalized Boolean function in $\mathcal{GB}_n^{2^k}$, $k > 1$.

We shall be using the following result on generalized Boolean bent functions, which for $n$ even first appeared in [23, Theorem 18]. For odd $n$ we may refer to [22,30].

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

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

*$a_i \in \mathcal{B}_n$, $0 \leq i \leq k-1$.*

*(i) If $n$ is even, then all Boolean functions of the form*

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

*$\mathbf{c} = (c_0, c_1, \ldots, c_{k-2}) \in \mathbb{F}_2^{k-1}$, are bent functions. In particular, $a_0(\mathbf{x}) + 2a_1(\mathbf{x})$ is a quaternary gbent function if and only if $a_1$ and $a_1 \oplus a_0$ are bent.*

*(ii) If $n$ is odd, then all Boolean functions of the form*

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

*$\mathbf{c} = (c_0, c_1, \ldots, c_{k-2}) \in \mathbb{F}_2^{k-1}$, are semibent functions. Moreover for every $\mathbf{u} \in \mathbb{V}_n$ we either have $\mathcal{W}_{g_{\mathbf{c}}}(\mathbf{u}) \neq 0$ for all $\mathbf{c} = (c_0, c_1, \ldots, c_{k-2})$ with $c_{k-2} = 0$ or for all $\mathbf{c}$ with $c_{k-2} = 1$ (but not for both). In particular, $a_0(\mathbf{x}) + 2a_1(\mathbf{x})$ is a quaternary gbent function if and only if $a_1$ and $a_1 \oplus a_0$ are semibent such that $\mathcal{W}_{a_1}(\mathbf{u}) = 0$ if and only if $\mathcal{W}_{a_1 \oplus a_0}(\mathbf{u}) \neq 0$.*

By Proposition 2, for a gbent function $f$ in $\mathcal{GB}_n^{2^k}$ given as in (2), $a_{k-1} + \langle a_0, \ldots, a_{k-2} \rangle$ is an affine space of bent, respectively, semibent functions. As pointed out in [14], every gbent function for which the coordinate functions $\{a_0, \ldots, a_{k-2}\}$ are linearly dependent, can be reduced to a gbent function in $\mathcal{GB}_n^{2^{k'}}$, for some $k' < k$ and linearly independent coordinate functions. Conversely we can see $f$ as a naturally lifted version of the gbent function in $\mathcal{GB}_n^{2^{k'}}$ with a very restricted value set in $\mathbb{Z}_{2^k}$. Hence for the classification of (symmetric) generalized bent functions, it is essential to consider only functions for which $\{a_0, \ldots, a_{k-2}\}$ are linearly independent.

A vectorial function $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$ given as $f(\mathbf{x}) = (a_0(\mathbf{x}), a_1(\mathbf{x}), \ldots, a_{k-1}(\mathbf{x}))$ is symmetric if and only if every coordinate function $a_i$, $0 \leq i < k$, is symmetric. A similar statement applies to generalized Boolean functions (we omit the proof).

**Lemma 1.** *Let $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$, $k \geq 2$, and $f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i a_i(\mathbf{x})$, $a_i \in \mathcal{B}_n$. Then $f$ is symmetric if and only if all components $a_i$ are symmetric, $0 \leq i < k$.*

Since for odd $n$ we require symmetric semibent functions, we will use the methods of [26] to also investigate semibent functions. The standard examples of semibent functions are partially bent functions with a one-dimensional linear space. Recall that a partially bent function $f$ is defined as a function for which for all $\mathbf{a} \in \mathbb{F}_2^n$, the derivative $D_{\mathbf{a}}f$ is either balanced or constant. All quadratic functions are partially bent, but by a construction in [32] there exist semibent functions, which are not partially bent.

We start our analysis by observing that $s_2(\mathbf{x}) = \binom{wt(\mathbf{x})}{2} \bmod 2$ and $(s_2 \oplus s_1)(\mathbf{x}) = \binom{wt(\mathbf{x})}{2} + wt(\mathbf{x}) \bmod 2$, hence

$$\begin{aligned} s_2(\mathbf{x}) &= \begin{cases} 0 & : \quad wt(\mathbf{x}) \equiv 0, 1 \bmod 4 \\ 1 & : \quad wt(\mathbf{x}) \equiv 2, 3 \bmod 4 \end{cases} \\ (s_2 \oplus s_1)(\mathbf{x}) &= \begin{cases} 0 & : \quad wt(\mathbf{x}) \equiv 0, 3 \bmod 4 \\ 1 & : \quad wt(\mathbf{x}) \equiv 1, 2 \bmod 4 \end{cases}. \end{aligned} \tag{3}$$

Before we show that $S_{c,d} = s_2 \oplus cs_1 \oplus d$, $c, d \in \mathbb{F}_2$, is semibent, when $n$ is odd, we recall that the Walsh transform of a symmetric function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is (see [26, Equation (1)]),

$$\mathcal{W}_f(\mathbf{u}) = \sum_{k=0}^{n} (-1)^{c_k} \sum_{wt(\mathbf{x})=k} (-1)^{\mathbf{u} \cdot \mathbf{x}} = \sum_{k=0}^{n} (-1)^{c_k} P_k(wt(\mathbf{u}), n), \tag{4}$$

where $c_k = f(\mathbf{x})$ if $\mathrm{wt}(\mathbf{x}) = k$, and $P_k$ is the Krawtchouk polynomial [20]. In particular, if $wt(\mathbf{u}_1) = wt(\mathbf{u}_2)$, then $\mathcal{W}_f(\mathbf{u}_1) = \mathcal{W}_f(\mathbf{u}_2)$. We furthermore will use the generating function of $P_k$, which is given by (see [26, Equation (2)]),

$$(1 - z)^{wt(\mathbf{u})} (1 + z)^{n - wt(\mathbf{u})} = \sum_{k=0}^{n} P_k(wt(\mathbf{u}), n) z^k. \tag{5}$$

**Proposition 3.** *Let $n$ be odd, and $S_{c,d}(\mathbf{x}) = s_2(\mathbf{x}) \oplus cs_1(\mathbf{x}) \oplus d$, $c, d \in \mathbb{F}_2$.*

(*i*) *The symmetric function $S_{c,d}$ is a semibent function with linear space $LS(S_{c,d}) = \{\mathbf{0}, \mathbf{1}\}$.*

(*ii*) *A symmetric semibent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ cannot have the vectors of weight $(n-1)/2$ and the vectors of weight $(n+1)/2$ in the support of its Walsh transform.*

(*iii*) *The functions $S_{c,d}$ are the only symmetric semibent functions, which have a vector of weight $(n-1)/2$ or a vector of weight $(n+1)/2$ in the support of their Walsh transform.*

*Proof.* We first show (*i*). Since $s_2$ is quadratic, it is a partially bent function. We have to show that $LS(s_2)$ has dimension 1. Observe that

$$D_{\mathbf{a}}(s_2) = s_2(\mathbf{x} \oplus \mathbf{a}) \oplus s_2(\mathbf{x}) = \bigoplus_{i=1}^{n} a_i \bigoplus_{\substack{j=1 \\ j \neq i}}^{n} \mathbf{x}_j \oplus C.$$

Inserting the unit vectors $\mathbf{e}_i$, we infer that $D_{\mathbf{a}}(s_2)$ is constant if and only if $\mathbf{a} = \mathbf{0}$ or (since $n$ is odd) $\mathbf{a} = \mathbf{1}$. This shows for all $c, d \in \mathbb{F}_2$ that $S_{c,d}$ is semibent with linear space $\{\mathbf{0}, \mathbf{1}\}$.

We next show both (*ii*) and (*iii*). We determine the Walsh transform of a symmetric function $f$ at a vector $\mathbf{u}_1$ of weight $wt(\mathbf{u}_1) = (n-1)/2$. With (5), we straightforwardly see that for $k = 2l$ and $k = 2l+1$, $0 \leq l \leq (n-1)/2$, we have

$$\sum_{wt(\mathbf{x})=k} (-1)^{\mathbf{u}_1 \cdot \mathbf{x}} = (-1)^l \binom{\frac{n-1}{2}}{l}.$$

Consequently, by (4),

$$\begin{aligned} \mathcal{W}_f(\mathbf{u}_1) &= \sum_{l=0}^{(n-1)/2} (-1)^{c_{2l}} (-1)^l \binom{\frac{n-1}{2}}{l} + \sum_{l=0}^{(n-1)/2} (-1)^{c_{2l+1}} (-1)^l \binom{\frac{n-1}{2}}{l} \\ &= \sum_{l=0}^{(n-1)/2} (-1)^l \binom{\frac{n-1}{2}}{l} \left( (-1)^{c_{2l}} + (-1)^{c_{2l+1}} \right). \end{aligned}$$

Similarly for a vector $\mathbf{u}_2$ of weight $wt(\mathbf{u}_2) = (n+1)/2$ we obtain

$$\mathcal{W}_f(\mathbf{u}_2) = \sum_{l=0}^{(n-1)/2} (-1)^l \binom{\frac{n-1}{2}}{l} \left( (-1)^{c_{2l}} - (-1)^{c_{2l+1}} \right).$$

Suppose that $\mathcal{W}_f(\mathbf{u}_1) = \pm 2^{(n+1)/2}$. Then we must have $(-1)^l((-1)^{c_{2l}} + (-1)^{c_{2l+1}}) = 2$ for all $0 \leq l \leq (n-1)/2$ (then $\mathcal{W}_f(\mathbf{u}_1) = 2^{(n+1)/2}$), or $(-1)^l((-1)^{c_{2l}} + (-1)^{c_{2l+1}}) = -2$ for all $0 \leq l \leq (n-1)/2$ (then $\mathcal{W}_f(\mathbf{u}_1) = -2^{(n+1)/2}$). In the first case, we have $c_{2l} = c_{2l+1} = 0$ if $l$ is even, and $c_{2l} = c_{2l+1} = 1$ if $l$ is odd. (It is the other way around in the second case.) It immediately follows then that

$\mathcal{W}_f(\mathbf{u}_2) = 0$. Moreover, with (3) we see that $\mathcal{W}_f(\mathbf{u}_1) = \pm 2^{(n+1)/2}$ implies that $f = s_2$ or $f = s_2 \oplus 1$.

If on the other hand $\mathcal{W}_f(\mathbf{u}_2) = \pm 2^{(n+1)/2}$, with the same reasoning we see that $\mathcal{W}_f(\mathbf{u}_1) = 0$, and $f = s_2 \oplus s_1$ or $f = s_2 \oplus s_1 \oplus 1$. □

Since for a symmetric function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ we have $\mathcal{W}_f(\mathbf{u}_1) = \mathcal{W}_f(\mathbf{u}_2)$ if $wt(\mathbf{u}_1) = wt(\mathbf{u}_2)$ and the support of the Walsh transform of a semibent function has cardinality $2^{n-1}$, a symmetric semibent function induces a bisection of the binomial coefficients, i.e., a subset $S$ of $\{0, \ldots, n\}$ such that $\sum_{j \in S} \binom{n}{j} = \sum_{j \notin S} \binom{n}{j} = 2^{n-1}$. For odd $n$, the trivial bisections are the sets $S$ that contain exactly one of $\binom{n}{j}$ and $\binom{n}{n-j}$ for all $0 \leq j \leq (n-1)/2$. Bisections of polynomial coefficients is a quite frequently studied problem [6,11,12,16]. It is not known for what values of $n$, a nontrivial bisection exists.

We expect that the functions $S_{c,d}$ are, unconditionally, the only symmetric semibent functions. We have the following partial result.

**Corollary 2.** *Let $n$ be odd. The semibent function $S_{c,d} : \mathbb{F}_2^n \to \mathbb{F}_2$ is the only symmetric partially bent semibent function. If there is no nontrivial bisection of the binomial coefficients $\binom{n}{j}$, then $S_{c,d}$ is the only symmetric semibent function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.*

*Proof.* Suppose that $f$ is a symmetric partially bent semibent function with linear space $\{\mathbf{0}, \mathbf{v}\}$. Then the support of $\mathcal{W}_f$ is $\{\mathbf{0}, \mathbf{v}\}^\perp$ or its coset. Observe that if $\mathbf{v} \neq \mathbf{1}$, then there always exist two vectors $\mathbf{u}_1, \mathbf{u}_2$ of the same weight, only one of which is in $\{\mathbf{0}, \mathbf{v}\}^\perp$. This contradicts the symmetry of $f$. Hence $LS(f) = \{\mathbf{0}, \mathbf{1}\}$, and the support of $\mathcal{W}_f$ consists either of the vectors of even weight or of the vectors of odd weight. With Proposition 3, $f = S_{c,d}$.

If $n$ permits only the trivial bisection of the binomial coefficients, then every symmetric semibent function $f$ has either the vectors of weight $(n-1)/2$ or the vectors of weight $(n+1)/2$ in the support of its Walsh transform. With Proposition 3, $f = S_{c,d}$. □

Since there is only one symmetric bent Boolean function up to addition of an affine function, there is no symmetric vectorial bent function for $k > 1$. As we show next, there is essentially only one example of a symmetric generalized bent Boolean function.

**Theorem 2.** *There are no symmetric vectorial bent functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^k$ for $k > 1$. The only symmetric generalized bent Boolean functions $f \in \mathcal{GB}_n^{2^k}$, $k > 1$, are the quaternary functions $f(\mathbf{x}) = (s_1(\mathbf{x}) \oplus e) + 2S_{c,d}(\mathbf{x})$ for some $c, d, e \in \mathbb{F}_2$ (and their natural lifts to functions in $\mathcal{GB}_n^{2^k}$ with only four values in their value set in $\mathbb{Z}_{2^k}$).*

*Proof.* Let $f(\mathbf{x}) = \sum_{i=0}^{k-1} 2^i a_i(\mathbf{x})$, $a_i \in \mathcal{B}_n$, be a symmetric generalized bent Boolean function. Hence all $a_i \in \mathcal{B}_n$ are symmetric. If $n$ is even, then all components $g_{\mathbf{c}}(\mathbf{x}) = c_0 a_0(\mathbf{x}) \oplus c_1 a_1(\mathbf{x}) \oplus \cdots \oplus c_{k-2} a_{k-2}(\mathbf{x}) \oplus a_{k-1}(\mathbf{x})$ are symmetric bent functions, i.e. $g_{\mathbf{c}}(\mathbf{x}) \in \{S_{c,d}, c, d \in \mathbb{F}_2\}$. Consequently, we are left with the

1-dimensional space of bent functions $S_{c,d}(\mathbf{x}) \oplus \langle s_1(\mathbf{x}) \oplus e \rangle$, $c, d, e \in \mathbb{F}_2$. Note that by Proposition 2(i), all quaternary functions $(s_1(\mathbf{x}) \oplus e) + 2S_{c,d}(\mathbf{x})$, $c, d, e \in \mathbb{F}_2$ are in fact generalized bent.
If $n$ is odd, then for any $\mathbf{c} = (c_0, \ldots, c_{k-3}, 0)$, $\mathbf{d} = (d_0, \ldots, d_{k-3}, 1)$, $c_i, d_i \in \mathbb{F}_2$, the components

$$g_{\mathbf{c}} = a_{k-1} \oplus \bigoplus_{i=0}^{k-3} c_i a_i \quad \text{and} \quad g_{\mathbf{d}} = a_{k-1} \oplus a_{k-2} \oplus \bigoplus_{i=0}^{k-3} d_i a_i$$

are symmetric semibent functions, with the additional property that for any $\mathbf{u} \in \mathbb{F}_2^n$ we have $\mathcal{W}_{g_{\mathbf{c}}}(\mathbf{u}) = 0$ if and only $\mathcal{W}_{g_{\mathbf{d}}}(\mathbf{u}) \neq 0$. By Proposition 3$(ii)$, $\mathcal{W}_{g_{\mathbf{c}}}(\mathbf{u}) \neq 0$ if $wt(\mathbf{u}) = (n-1)/2$ and $\mathcal{W}_{g_{\mathbf{d}}}(\mathbf{u}) \neq 0$ if $wt(\mathbf{u}) = (n+1)/2$, or vice versa. By Proposition 3$(iii)$ then for all such $\mathbf{c}, \mathbf{d} \in \mathbb{F}_2^{k-1}$ we have $g_{\mathbf{c}}(\mathbf{x}) = s_2 \oplus d$, $d \in \mathbb{F}_2$, and $g_{\mathbf{d}} = s_2 \oplus s_1 \oplus e$, $e \in \mathbb{F}_2$, or vice versa. Therefore, the only candidate is $f(\mathbf{x}) = (s_1(\mathbf{x}) \oplus e) + 2S_{c,d}(\mathbf{x})$ for some $c, d, e \in \mathbb{F}_2$. By Proposition 2$(ii)$ it remains to show that the supports of $\mathcal{W}_{s_2}$ and $\mathcal{W}_{s_2 \oplus s_1}$ are disjoint. With Proposition 3, the support of $\mathcal{W}_{s_2}$, respectively, the support of $\mathcal{W}_{s_2 \oplus s_1}$ is $\{\mathbf{0}, \mathbf{1}\}^{\perp}$ or its coset. Furthermore, exactly one of $\mathcal{W}_{s_2}, \mathcal{W}_{s_2 \oplus s_1}$ has the vectors of weight $(n-1)/2$ in its support, which completes the proof. □

*Remark 2.* The possible lifts are described explicitly by $\tilde{f}(\mathbf{x}) = A + Bs_1(\mathbf{x}) + 2^{k-1}s_2(\mathbf{x})$ for constants $0 \leq A, B \leq 2^k - 1$ if $n$ is even, and if $n$ is odd by $\tilde{f}(\mathbf{x}) = C + 2^{k-2}s_1(\mathbf{x}) + 2^{k-1}S_{c,d}(\mathbf{x})$ for some constant $0 \leq C \leq 2^{k-1} - 1$ and $c, d \in \{0, 1\}$. Certainly those functions reduce to and are completely described with the quaternary gbent function $f : \mathbb{F}_2^n \to \mathbb{Z}_4$ given as $f(\mathbf{x}) = s_1(\mathbf{x}) + 2s_2(\mathbf{x})$.

We next impose balancedness to the symmetry of a generalized Boolean function, $f : \mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ (in fact, our result is true for any function from $\mathbb{F}_2^n$ into a group of order $2^k$). We adopt the classical approach by embedding the problem into one of multisection (not necessarily, bisection) of binomial coefficients. The connection is rather simple: since the function is symmetric, its value is independent of the weight of the input. Thus, the symmetric function $f$ has constant value $c_j$ for every weight $j$ vector (of count $\binom{n}{j}$). Imposing balancedness, it means that each such $c_j$ will occur the same number of times, that is, we can split the set of all binomial coefficients into $2^k$ sets, whose sums are equal, namely $2^{n-k}$.

As mentioned above, if $k = 1$, this is an older and quite studied problem [6,11,12,15,16]. While there always exist trivial bisections, it is not known for what values of $n$, a nontrivial bisection exists. Many papers have been written, which employ heavy computations to find values of $n$, for which we can nontrivially bisect the binomial coefficients set $\left\{\binom{n}{j}\right\}_{0 \leq j \leq n}$. Thus, it is a natural question to ask whether a splitting of binomial coefficients of size other than two does exist. It was conjectured in [21] that no such $2^k$-section for $k > 1$ existed. While this question originates from our attempt to investigate balanced and symmetric generalized Boolean functions, it has an interest of its own. As for the bisection, we say that we have a $2^k$-*section* of a set of integers $A$ (whose cardinality is divisible by $2^k$) if there is a partition of cardinality $2^k$ of the set $A$ such that the sum on each partition set is $\frac{1}{2^k} \sum_{x \in A} x$, $1 \leq j \leq 2^k$.

**Theorem 3.** *There is no symmetric balanced function from $\mathbb{F}_2^n$, $n \geq 1$, to any group of order $2^k$, if $k \geq 2$. In particular, for $k \geq 2$, there are no $2^k$-sections of binomial coefficients $\left\{\binom{n}{j}\right\}_{0 \leq j \leq n}$.*

*Proof.* The result is easy to show for $1 \leq n \leq 10$, so we assume that $n \geq 10$. Freiman [10] considered the system of equations

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1m}x_m &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2m}x_m &= b_2, \end{aligned}$$

where $(0,0) \neq (a_{1j}, a_{2,j}) \in \mathbb{Z}^2$, $(b_1, b_2) \in \mathbb{Z}^2$, and he showed that the number of solutions $x_j \in \{0,1\}$ of the above system is exactly

$$J_{b_1,b_2} = 2^m \int_G \int e^{-2\pi i(xb_1+yb_2)} \prod_{j=1}^{m} \frac{1}{2}\left(1 + e^{2\pi i(xa_{1j}+ya_{2j})}\right) d\,x\,d\,y,$$

where $G = \left\{(x,y) \,|\, x,y \in \mathbb{R}, |x| \leq \frac{1}{2}, |y| \leq \frac{1}{2}\right\}$.

Let $n \geq 10$ be fixed, and we assume that there is a $2^k$-section, $k \geq 2$ (we take $k$ largest with this property). We consider such a $2^k$-section and partition the binomial coefficients $\binom{n}{j}$ in $2^k$ (disjoint) sets $A_i, 1 \leq i \leq 2^k$ such that $\sum_{j \in A_i} \binom{n}{j} = 2^{n-k}$, $1 \leq i \leq 2^k$. Since we took $k$ largest with this property (certainly, $k < n$), one of the sets, without loss of generality, say $A_1$, cannot be bisected further. We next consider the system

$$\begin{aligned} \sum_{j \in \cup_{i=2}^{2^k} A_i} x_j \binom{n}{j} + \sum_{j \in A_1} x_j \cdot 0 &= (2^k - 1)2^{n-k} \\ \sum_{j \in \cup_{i=2}^{2^k} A_i} x_j \cdot 0 + \sum_{j \in A_1} x_j \binom{n}{j} &= 2^{n-k}, \end{aligned}$$

and by Freiman's result there are exactly

$$\begin{aligned} J_{(2^k-1)\ 2^{n-k}, 2^{n-k}} &= 2^{n+1} \int_{-1/2}^{1/2} \int_{-1/2}^{1/2} e^{-2\pi 2^{n-k}((2^k-1)x+y)} \\ &\quad \cdot \prod_{j \in \cup_{i=2}^{2^k} A_i} \frac{1}{2}\left(1 + e^{2\pi i x \binom{n}{j}}\right) \prod_{j \in A_1} \frac{1}{2}\left(1 + e^{2\pi i y \binom{n}{j}}\right) d\,x\ d\,y \\ &= 2^{n+1} \int_{-1/2}^{1/2} e^{-(2^k-1)\pi 2^{n-k+1}x} \prod_{j \in \cup_{i=2}^{2^k} A_i} \frac{1}{2}\left(1 + e^{2\pi i x \binom{n}{j}}\right) \\ &\quad \cdot \int_{-1/2}^{1/2} e^{-\pi 2^{n-k+1}y} \prod_{j \in A_1} \frac{1}{2}\left(1 + e^{2\pi i y \binom{n}{j}}\right) \end{aligned}$$

$$= 2^{n+1} \int_{-1/2}^{1/2} \prod_{j \in \cup_{i=2}^{2^k} A_i} \cos\left(\pi x \binom{n}{j}\right) \int_{-1/2}^{1/2} \prod_{j \in A_1} \cos\left(\pi x \binom{n}{j}\right),$$

solutions of that system. By our assumption, $J_{(2^k-1)\ 2^{n-k},2^{n-k}} \geq 1$. We let $\langle , \rangle$ be the regular Euclidean scalar product, and observe that

$$\prod_{j \in A_1} \cos\left(\pi i x \binom{n}{j}\right) = \frac{1}{2^{|A_1|-1}} \sum_{\theta \in \{-1,1\}^{|A_1|-1}} \cos\left(\pi i x \left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle\right).$$

Observe that $\left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle \equiv \sum_{j \in A_1} \binom{n}{j} = 2^{n-k} \equiv 0 \pmod 2$, for all $\theta \in \{-1,1\}^{|A_1|-1}$. Moreover, the scalar product $\left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle \neq 0$, since we assumed that $A_1$ cannot be bisected further. Therefore, the integral

$$\begin{aligned}
&\int_{-1/2}^{1/2} \prod_{j \in A_1} \cos\left(\pi x \binom{n}{j}\right) \\
&= \frac{1}{2^{|A_1|-1}} \int_{-1/2}^{1/2} \sum_{\theta \in \{-1,1\}^{|A_1|-1}} \cos\left(\pi x \left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle\right) \\
&= \frac{1}{2^{|A_1|-1}} \sum_{\theta \in \{-1,1\}^{|A_1|-1}} \int_{-1/2}^{1/2} \cos\left(\pi x \left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle\right) \\
&= \frac{1}{2^{|A_1|-1} \pi \left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle} \sum_{\theta \in \{-1,1\}^{|A_1|-1}} \sin\left(\pi x \left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle\right) |_{-1/2}^{1/2} \\
&= 0,
\end{aligned}$$

since $\left\langle (1,\theta), (\binom{n}{j})_{j \in A_1} \right\rangle \equiv 0 \pmod 2$, which shows that our assumption that, for $k \geq 2$, there are $2^k$-sections of binomial coefficients is false. The theorem is shown. □

## 4 Avalanche features in terms of differentials

Let $f \in \mathcal{GB}_n^{2^k}$ and $\mathbf{a} \in \mathbb{V}_n$, $c \in \mathbb{Z}_{2^k}$. We let

$$\delta(\mathbf{a}, c) := |\{\mathbf{x} \in \mathbb{V}_n \,|\, D_{\mathbf{a}} f(\mathbf{x}) = c\}|,$$

and call the quantity $\Delta_f := \max_{(\mathbf{a},c) \in \mathbb{V}_n^* \times \mathbb{Z}_{2^k}} \delta_f(\mathbf{a}, c)$ the *differential uniformity* of $f$ (and $f$ is a differentially $\Delta_f$-uniform function). The multiset $\{\delta_f(\mathbf{a}, c) \,|\, (\mathbf{a}, c) \in \mathbb{V}_n \times \mathbb{Z}_{2^k}\}$ is called the *differential spectrum* of $f$. It is known that when $f$ has values in $\mathbb{V}_n$, then $\Delta_f \geq 2$ (in odd characteristic, $\Delta_f$ can take the value 1), and

functions achieving this bound are called *almost perfect nonlinear* (APN). Recall that bent functions $f$ from a group $A$ to a group $B$ can be defined as functions for which $f(x+a)-f(x)$ is balanced for every nonzero $a \in A$, i.e. every $b \in B$ is taken on the same number $|A|/|B|$ times. A function $f$ from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ is hence bent if and only if $\Delta_f = 2^{n-k}$. In terms of character sum values a bent function from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ is then a function for which

$$\mathcal{H}_f(\alpha, \mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{\alpha f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} \tag{6}$$

has absolute value $2^{n/2}$ for all nonzero $\alpha \in \mathbb{Z}_{2^k}$ and $\mathbf{u} \in \mathbb{V}_n$. We next investigate differential properties of generalized bent functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$, which satisfy the weaker property that $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$, see Corollary 3 below.

If $\mathbb{V}_n = \mathbb{F}_2^n$, then we say that $f \in \mathcal{GB}_n^{2^k}$ satisfies the (*generalized*) *propagation criterion of order* $\ell$ $(1 \leq \ell \leq n)$, denoted by $gPC(\ell)$, if and only if the autocorrelation $\mathcal{C}_f(\mathbf{v}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x}) - f(\mathbf{x} \oplus \mathbf{v})} = 0$, for all vectors $\mathbf{v} \in \mathbb{F}_2^n$ of weight $0 < wt(\mathbf{v}) \leq \ell$. If $\ell = 1$, we say that $f$ satisfies the (*generalized*) *strict avalanche criterion* ($gSAC$). With the standard calculations we see that $f$ is gbent if and only if $\mathcal{C}_f(\mathbf{v}) = 0$ for all $\mathbf{v}$ (in this case we do not require that $\mathbb{V}_n = \mathbb{F}_2^n$).

**Theorem 4.** *Let $f \in \mathcal{GB}_n^{2^k}$, and $A_j^{(\mathbf{w})} = \{\mathbf{x} | f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) = j\}$. Then $f$ is $gPC(\ell)$ if and only if*

$$|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0, |A_j^{(\mathbf{w})}| = |A_{j+2^{k-1}}^{(\mathbf{w})}|, \text{ for } 0 \leq j \leq 2^{k-1} - 1, 1 \leq wt(\mathbf{w}) \leq \ell.$$

*Proof.* First note that unconditionally we always have $|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0$. For $\mathbf{v} \in \mathbb{V}_n$, $\mathbf{v} \neq \mathbf{0}$, with the notations in the statement of the theorem and $\bar{\zeta} = \zeta^{-1}$ we have

$$\mathcal{C}_f(\mathbf{v}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x}) - f(\mathbf{x} \oplus \mathbf{v})} = \sum_{j=0}^{2^k - 1} |A_j^{(\mathbf{v})}| \bar{\zeta}^j = \sum_{j=0}^{2^{k-1} - 1} (|A_j^{(\mathbf{v})}| - |A_{j+2^{k-1}}^{(\mathbf{v})}|) \bar{\zeta}^j.$$

Since the set $\{\bar{\zeta}^j : 0 \leq j \leq 2^{k-1} - 1\}$ is a basis of $\mathbb{Q}(\zeta)$, hence is linearly independent, we have $\mathcal{C}_f(\mathbf{v}) = 0$ if and only if $|A_j^{(\mathbf{v})}| = |A_{j+2^{k-1}}^{(\mathbf{v})}|$ for $0 \leq j \leq 2^{k-1} - 1$. □

**Corollary 3.** *Let $f \in \mathcal{GB}_n^{2^k}$. Then $f$ is gbent if and only if*

$$|A_0^{(\mathbf{0})}| = 2^n, |A_j^{(\mathbf{0})}| = 0, |A_j^{(\mathbf{w})}| = |A_{j+2^{k-1}}^{(\mathbf{w})}|, \quad \text{for all} \quad 0 \leq j \leq 2^{k-1} - 1, \mathbf{w} \neq 0.$$

Recall that a Boolean function $g : \mathbb{V}_n \to \mathbb{F}_2$ is called *partially bent* if $g(\mathbf{x} \oplus \mathbf{a}) \oplus g(\mathbf{x})$ is either balanced or constant for all $\mathbf{a} \in \mathbb{V}_n$. Partially bent functions from $\mathbb{V}_n$ to $\mathbb{F}_2$ are always $s$-plateaued, where $s$ is the dimension of the linear space of $g$. In an analog way we can define (generalized) *partially bent* functions from $\mathbb{V}_n$ to $\mathbb{Z}_{2^k}$ as functions $f$ for which $f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x})$ is either balanced or

constant for all $\mathbf{a} \in \mathbb{V}_n$. With the standard proof for partially bent functions one can show that generalized partially bent functions $f : \mathbb{V}_n \to \mathbb{Z}_{2^k}$ as defined above, are plateaued with respect to their transform $\mathcal{H}_f(\alpha, u)$ of (6).

In Theorem 4 we characterized gbent functions via their differential properties. With this characterization the following definition of a partially gbent function is natural. As in Theorem 4, let $A_j^{(\mathbf{w})} = \{\mathbf{x} | f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) = j\}$. A function $f \in \mathcal{GB}_n^{2^k}$ is called *partially gbent*, if for all $\mathbf{w} \in \mathbb{V}_n$ we either have $|A_j^{(\mathbf{w})}| = |A_{j+2^{k-1}}^{(\mathbf{w})}|$ for all $0 \leq j \leq 2^{k-1} - 1$, or the derivative $f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x})$ is constant.

**Proposition 4.** *A partially gbent function $f \in \mathcal{GB}_n^{2^k}$ is $s$-plateaued, where $s$ is the dimension of the linear space of $f$.*

*Proof.* Since $\mathcal{H}_{f+c}(\mathbf{u}) = \zeta^c \mathcal{H}_f(\mathbf{u})$, without loss of generality we can suppose that $f(\mathbf{0}) = 0$. For $\mathbf{u} \in \mathbb{V}_n$ we have

$$\begin{aligned}\mathcal{H}_f(\mathbf{u})\overline{\mathcal{H}_f(\mathbf{u})} &= \sum_{\mathbf{z} \in \mathbb{V}_n} \zeta^{f(\mathbf{z})} (-1)^{\mathbf{u} \cdot \mathbf{z}} \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{-f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}} \\ &= \sum_{\mathbf{w} \in \mathbb{V}_n} \zeta^{-f(\mathbf{w})} (-1)^{\mathbf{u} \cdot \mathbf{w}} \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) + f(\mathbf{w})}.\end{aligned}$$

Observe that $f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) + f(\mathbf{w}) = 0$ if $\mathbf{w}$ is a linear structure of $f$ (we use that $f(\mathbf{0}) = 0$). If $\mathbf{w}$ is not a linear structure, then by our assumption $\sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x}) + f(\mathbf{w})} = \zeta^{f(\mathbf{w})} \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x} \oplus \mathbf{w}) - f(\mathbf{x})} = 0$. Hence putting $\Lambda = LS_{2^k}(f)$, $\mathcal{H}_f(\mathbf{u})\overline{\mathcal{H}_f(\mathbf{u})} = 2^n \sum_{\mathbf{w} \in \Lambda} \zeta^{-f(\mathbf{w})} (-1)^{\mathbf{u} \cdot \mathbf{w}}$. Let $\mathbf{z}$ be any element of $S_f = \{\mathbf{x} \in \mathbb{V}_n | \mathcal{H}_f(\mathbf{x}) \neq 0\}$. Then by Theorem 1 we have $\zeta^{f(\mathbf{w})} = (-1)^{\mathbf{z} \cdot \mathbf{w}}$ for every $\mathbf{w} \in \Lambda$. Therefore $\mathcal{H}_f(\mathbf{u})\overline{\mathcal{H}_f(\mathbf{u})} = 2^n \sum_{\mathbf{w} \in \Lambda} (-1)^{(\mathbf{z} \oplus \mathbf{u}) \cdot \mathbf{w}}$, (independently from the choice of $\mathbf{z} \in S_f$). Consequently, if $\mathbf{z} \oplus \mathbf{u} \in \Lambda^\perp$, then $|\mathcal{H}_f(\mathbf{u})|^2 = 2^{n+s}$, where $s = \dim(\Lambda)$, otherwise $\mathcal{H}_f(\mathbf{u}) = 0$. □

*Remark 3.* Observing that $\mathcal{H}_f(\mathbf{u})$ only depends on whether $\mathbf{z} \oplus \mathbf{u} \in \Lambda^\perp$, independent from the choice of $\mathbf{z} \in S_f$, we infer that $S_f$ is a coset of $\Lambda^\perp$ (we also use that by Parseval's identity, $|S_f| = 2^{n-s}$). This coincides with the situation for conventional partially bent functions.

Similar as for conventional partially bent functions, cf. [4,5], we have the following corollary for partially gbent functions.

**Corollary 4.** *Let $\Lambda = LS_{2^k}(f)$ be the linear space of the function $f \in \mathcal{GB}_n^{2^k}$. Then $f$ is partially gbent (partially bent) if and only if for any complement $\Lambda^{comp}$ of $\Lambda$ in $\mathbb{V}_n$, the function $f|\Lambda^{comp}$ is gbent (bent).*

*Proof.* With $D_{\mathbf{a}} f(\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x})$,

$$\mathcal{H}_{D_{\mathbf{a}} f}(\mathbf{0}) = \sum_{\mathbf{x} \in \mathbb{V}_n} \zeta^{f(\mathbf{x} \oplus \mathbf{a}) - f(\mathbf{x})} = \sum_{\mathbf{y} \in \Lambda} \sum_{\mathbf{z} \in \Lambda^{comp}} \zeta^{f(\mathbf{y} \oplus \mathbf{z} \oplus \mathbf{a}) - f(\mathbf{y} \oplus \mathbf{z})}.$$

Using that $f(\mathbf{x}\oplus\mathbf{y})-f(\mathbf{x})+f(\mathbf{y})=0$ if $\mathbf{y}\in\Lambda$, we see that $f(\mathbf{y}\oplus\mathbf{z}\oplus\mathbf{a})-f(\mathbf{y}\oplus\mathbf{z}) = f(\mathbf{z}\oplus\mathbf{a})-f(\mathbf{z})$, hence

$$\mathcal{H}_{D_\mathbf{a}f}(\mathbf{0}) = \sum_{\mathbf{y}\in\Lambda}\sum_{\mathbf{z}\in\Lambda^{comp}} \zeta^{f(\mathbf{z}\oplus\mathbf{a})-f(\mathbf{z})} = |\Lambda| \sum_{\mathbf{z}\in\Lambda^{comp}} \zeta^{f(\mathbf{z}\oplus\mathbf{a})-f(\mathbf{z})}. \tag{7}$$

First suppose that $f$ is partially gbent. Then for $\mathbf{a}\notin\Lambda$ we have $\mathcal{H}_{D_\mathbf{a}f}(\mathbf{0}) = \sum_{\mathbf{x}\in\mathbb{V}_n}\zeta^{f(\mathbf{x}\oplus\mathbf{a})-f(\mathbf{x})}=0$, and hence with (7), $\sum_{\mathbf{z}\in\Lambda^{comp}}\zeta^{f(\mathbf{z}\oplus\mathbf{a})-f(\mathbf{z})}=0$. Consequently, for $\tilde{A}_j^{(\mathbf{a})} = \{\mathbf{z}\in\Lambda^{comp} | f(\mathbf{z}\oplus\mathbf{a})-f(\mathbf{z})=j\}$ we have $|\tilde{A}_j^{(\mathbf{a})}| = |\tilde{A}_{j+2^{k-1}}^{(\mathbf{a})}|$ for all $0\le j\le 2^{k-1}-1$ and all nonzero $\mathbf{a}\in\Lambda^{comp}$. By Theorem 4, $f$ restricted to $\Lambda^{comp}$ is gbent.

Conversely let $f|\Lambda^{comp}$ be gbent for any complement $\Lambda^{comp}$ of $\Lambda$. Let $\mathbf{a}\notin\Lambda$ and let $\Lambda^{comp}$ be a complement of $\Lambda$ containing $\mathbf{a}$. By assumption, with Theorem 4 we have $\sum_{\mathbf{z}\in\Lambda^{comp}}\zeta^{f(\mathbf{z}\oplus\mathbf{a})-f(\mathbf{z})}=0$, hence by Equation (7), $\mathcal{H}_{D_\mathbf{a}f}(\mathbf{0})=0$. Therefore $|A_j^{(\mathbf{a})}| = |A_{j+2^{k-1}}^{(\mathbf{a})}|$ for all $0\le j\le 2^{k-1}-1$, and $f$ is partially gbent by definition. □

**Acknowledgement.** This paper was started while the second and fourth named authors visited the third named author at the Institute of Algebra and Geometry, of Otto von Guericke University Magdeburg. They thank the host and the institute for hospitality and excellent working conditions.

## References

1. L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.
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.
3. C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.
4. C. Carlet, *Partially bent functions*, Des. Codes Cryptogr., vol. 3 (1993), 135–145.
5. A. Çeşmelioğlu, W. Meidl, A. Topuzoğlu, *Partially bent functions and their properties*, Applied algebra and number theory, 22–38, Cambridge Univ. Press, Cambridge, 2014.
6. T. W. Cusick, Y. Li, *k-th order symmetric SAC boolean functions and bisecting binomial coefficients*, Discrete Appl. Math. 149 (2005), 73–86.
7. T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.
8. S. Dubuc, *Characterization of Linear Structures*, Des. Codes Cryptogr. 22 (2001), 33–45.
9. J. H. Evertse, *Linear structures in blockciphers*, in *Advances in Cryptology, EUROCRYPT'87*, ser. Lecture Notes in Computer Science, D. Chaum and W.L. Price, Springer Berlin Heidelberg, 1988, vol. 304, pp. 249–266.
10. G. A. Freiman, *On Solvability of a System of Two Boolean Linear Equations*, Number Theory: New York Seminar 1991–1995, 135–150.

11. J. von zur Gathen, J. Roche, *Polynomials with two values*, Combinatorica 17 (1997), 345–362.
12. K. Gopalakrishnan, D. G. Hoffman, D. R. Stinson, *A note on a conjecture concerning symmetric resilient functions*, Inform. Proc. Lett. 47 (1993), 139–143.
13. A. Gouget, *On the propagation criterion of Boolean functions*, Proc. Workshop on Coding, Cryptogr. and Combin. '03, Birkhäuser Verlag, pp. 153–168, 2004.
14. S. Hodžić, W. Meidl, E. Pasalic, *Full characterization of generalized bent functions as (semi)-bent spaces, their dual and the Gray image*, Preprint 2017.
15. E. J. Ionascu, T. Martinsen, P. Stănică, *Bisecting binomial coefficients*, Discrete Applied Math 227 (2017), 70–83.
16. N. Jefferies, *Sporadic partitions of binomial coefficients*, Elec. Lett. 27:15 (1991), 134–136.
17. P. V. Kumar, R. A. Scholtz, L. R. Welch, *Generalized bent functions and their properties*, J. Combin Theory – Ser. A 40 (1985), 90–107.
18. X. Lai, *Additive and linear structures of cryptographic functions*, in Fast Software Encryption, LNCS 1008, Ed. Springer Berlin Heidelberg, 1995, pp. 75–85.
19. R. L. Lechner, *Harmonic analysis of switching functions*, Recent Developments in Switching Theory (A. Mukhopadhyay, ed.), Academic Press, New York and London (1971).
20. F. J. MacWilliams and N. J. A. Sloane, The theory of error correcting codes, North-Holland, Amsterdam, 1977.
21. T. Martinsen, Correlation Immunity, Avalanche Features, and Other Cryptographic Properties of Generalized Boolean Functions, PhD Dissertation, Naval Postgraduate School, Monterey, CA, 2017.
22. T. Martinsen, W. Meidl, S. Mesnager, P. Stanica, *Decomposing generalized bent and hyperbent functions*, IEEE Trans. Inform. Theory 63:12 (2017), 7804–7812.
23. T. Martinsen, W. Meidl, P. Stănică, *Generalized bent functions and their Gray images*, Proc. of WAIFI 2016 (Gent 2016), LNCS 10064 (2017), 166–173.
24. T. Martinsen, W. Meidl, P. Stănică, *Partial Spread and Vectorial Generalized Bent Functions*, Designs, Codes & Cryptography 85:1 (2017), 1–13.
25. S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.
26. P. Savicky, *On the bent Boolean functions that are symmetric*, European J. Combin. 15 (1994), 407–410.
27. K. U. Schmidt, *Quaternary constant-amplitude codes for multicode CDMA*, IEEE Trans. Inform. Theory 55:4 (2009), 1824–1832.
28. 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).
29. P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, *Bent and generalized bent Boolean functions*, Des. Codes Cryptogr. 69 (2013), 77–94.
30. 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.
31. N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.
32. Y.L. Zheng, X.M. Zhang, *On plateaued functions*, IEEE Trans. Inform. Theory 47:9 (2001), 1215–1223.