2011

Octal Generalized Boolean Functions

Stanica, Pantelimon

http://hdl.handle.net/10945/35441

Octal Generalized Boolean Functions

Pantelimon Stănică, Thor Martinsen,

[1] Department of Applied Mathematics**
Naval Postgraduate School
Monterey, CA 93943–5216, USA
{tmartins,pstanica}@nps.edu

Abstract. In this paper we characterize (octal) bent generalized Boolean functions defined on $\mathbb{Z}_2^n$ with values in $\mathbb{Z}_8$. Moreover, we propose several constructions of such generalized bent functions for both n even and n odd.

Keywords: Generalized Boolean functions; generalized bent functions; cross-corelation.

1 Introduction

Several generalizations of Boolean functions have been proposed in the recent years and the effect of the Walsh–Hadamard transform on them has been studied [8,12,13]. The natural generalizations of bent functions in the Boolean case, namely generalized functions which have flat spectra with respect to the Walsh–Hadamard transform are of special interest.

Let the set of integers, real numbers and complex numbers be denoted by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, respectively. By $\mathbb{Z}_r$ we denote the ring of integers modulo r. A function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ is said to be a Boolean function on n variables and the set of all such functions is denoted by $\mathcal{B}_n$. A function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ (q a positive integer) is said to be a *generalized Boolean function* on n variables [13]. We denote the set of such functions by $\mathcal{GB}_n^q$. We will consider these functions with an emphasis on $q = 8$.

Any element $\mathbf{x} \in \mathbb{Z}_2^n$ can be written as an n-tuple $(x_n, \ldots, x_1)$, where $x_i \in \mathbb{Z}_2$ for all $i = 1, \ldots, n$. The addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ is denoted by '+'. The addition over $\mathbb{Z}_2^n$ for all $n \geq 1$, is denoted by $\oplus$. Addition modulo q is denoted by '+' and is understood from the context. If $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1)$ are two elements of $\mathbb{Z}_2^n$, we define the scalar (or inner) product, by $\mathbf{x} \cdot \mathbf{y} = x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. The cardinality of the set S is denoted by $|S|$. If $z = a + b\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\overline{z} = a - b\imath$ denotes the complex conjugate of z, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. The conjugate of a bit b will also be denoted by $\bar{b}$.

** T.M. is a Ph.D student in Applied Mathematics at the Naval Postgraduate School.

The (normalized) *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is defined by

$$W_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

A function $f \in \mathcal{B}_n$, where n is even, is a *bent function* if $|W_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. In case n is even a function $f \in \mathcal{B}_n$ is said to be a *semibent* function if and only if, $|W_f(\mathbf{u})| \in \{0, \sqrt{2}\}$ for all $\mathbf{u} \in \mathbb{Z}_2^n$.

The sum

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x} \oplus \mathbf{z})}$$

is the *crosscorrelation* of f and g at $\mathbf{z}$. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is $C_{f,f}(\mathbf{u})$ above, which we denote by $C_f(\mathbf{u})$.

Let $\zeta = e^{2\pi\imath/q}$ be the q-primitive root of unity. The (generalized) *Walsh–Hadamard transform* of $f \in \mathcal{GB}_n^q$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is the complex valued function defined by

$$\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

A function $f \in \mathcal{B}_n$ is a *generalized bent function* (*gbent*, for short) if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$.

The sum

$$\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \zeta^{f(\mathbf{x}) - g(\mathbf{x} \oplus \mathbf{z})}$$

is the *crosscorrelation* of f and g at $\mathbf{z}$. The *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{Z}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$.

When $2^{h-1} < q \leq 2^h$, given any $f \in \mathcal{GB}_n^q$ we associate a unique sequence of Boolean functions $a_i \in \mathcal{B}_n$ $(i = 0, 1, \ldots, h-1)$ such that

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{h-1} a_{h-1}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n. \tag{1}$$

2 Properties of Walsh–Hadamard transform on generalized Boolean functions

We gather in the current section several properties of the Walsh–Hadamard transform and its generalized counterpart [6].

Theorem 1 *We have:*

(i) Let $f \in \mathcal{B}_n$. Then, the inverse of the Walsh–Hadamard transform is

$$(-1)^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u} \in \mathbb{Z}_2^n} W_f(\mathbf{u}) (-1)^{\mathbf{u} \cdot \mathbf{y}}.$$

(*ii*) *If* $f, g \in \mathcal{B}_n$, *then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} C_{f,g}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n W_f(\mathbf{x})W_g(\mathbf{x}),$$

$$C_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} W_f(\mathbf{x})W_g(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

(*iii*) *Taking the particular case* $f = g$ *we obtain*

$$C_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} W_f(\mathbf{x})^2(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

(*iv*) *A Boolean function* f *is bent if and only if* $C_f(\mathbf{u}) = 0$ *at all nonzero points* $\mathbf{u} \in \mathbb{Z}_2^n$.

(*v*) *For any* $f \in \mathcal{B}_n$, *the Parseval's identity holds*

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} W_f(\mathbf{x})^2 = 2^n.$$

For more properties of these transforms and Boolean functions, the interested reader can consult [1,2,3].

The properties of the Walsh–Hadamard transform on generalized Boolean functions are similar to the Boolean function case.

Theorem 2 *We have:*

(*i*) *Let* $f \in \mathcal{GB}_n^q$. *The inverse of the Walsh–Hadamard transform is given by*

$$\zeta^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{y}}.$$

Further, $\mathcal{C}_{f,g}(\mathbf{u}) = \overline{\mathcal{C}_{g,f}(\mathbf{u})}$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n$, *which implies that* $\mathcal{C}_f(\mathbf{u})$ *is always real.*

(*ii*) *If* $f, g \in \mathcal{GB}_n^q$, *then*

$$\sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{C}_{f,g}(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{x}} = 2^n \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})},$$

$$\mathcal{C}_{f,g}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}.$$

(*iii*) *Taking the particular case* $f = g$ *we obtain*

$$\mathcal{C}_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2(-1)^{\mathbf{u}\cdot\mathbf{x}}. \tag{2}$$

(*iv*) *If* $f \in \mathcal{GB}_n^q$, *then* f *is gbent if and only if*

$$\mathcal{C}_f(\mathbf{u}) = \begin{cases} 2^n & \text{if } \mathbf{u} = 0, \\ 0 & \text{if } \mathbf{u} \neq 0. \end{cases} \tag{3}$$

(v) Moreover, the (generalized) Parseval's identity holds

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 = 2^n. \tag{4}$$

3 The Walsh–Hadamard Transform on components

Let $\zeta = \mathbf{e}^{2\pi\imath/q}$ be a q-primitive root of unity. Let f be written as $f(\mathbf{x}) = \sum_{i=0}^{h-1} a_i(\mathbf{x})2^i$. For brevity, we use the notations $\zeta_i := \zeta^{2^i}$. It is easy to see that, for $s \in \mathbb{Z}_2$, we have

$$z^s = \frac{1+(-1)^s}{2} + \frac{1-(-1)^s}{2}z, \tag{5}$$

and so, we have the identities $\zeta_i^{a_i(\mathbf{x})} = \frac{1}{2}\left(A_i + A_i'\zeta_i\right)$, where $A_i = 1+(-1)^{a_i(\mathbf{x})}$ and $A_i' = 1-(-1)^{a_i(\mathbf{x})}$, $\bar{I} = \{0, 1, \ldots, h-1\} \setminus I$.

The Walsh–Hadamard coefficients of f are

$$\begin{aligned}
2^{n/2}\mathcal{H}_f(\mathbf{u}) &= \sum_{\mathbf{x}} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}} \zeta^{\sum_{i=0}^{h-1} a_i(\mathbf{x})2^i}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \prod_{i=0}^{h-1} \left(\zeta^{2^i}\right)^{a_i(\mathbf{x})} \\
&= \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \prod_{i=0}^{h-1} \frac{1}{2}\left(1+(-1)^{a_i(\mathbf{x})} + (1-(-1)^{a_i(\mathbf{x})})\zeta_i\right) \\
&= 2^{-h} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{I\subseteq\{0,\ldots,h-1\}} \prod_{i\in I, j\in\bar{I}} \zeta_i A_i' A_j \\
&= 2^{-h} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \prod_{i\in I, j\in\bar{I}} A_i' A_j \\
&= 2^{-h} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \sum_{J\subseteq I, K\subseteq\bar{I}} (-1)^{|J|}(-1)^{\sum_{j\in J} a_j(\mathbf{x})\oplus\sum_{k\in K} a_k(\mathbf{x})} \\
&= 2^{-h} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \sum_{J\subseteq I, K\subseteq\bar{I}} (-1)^{|J|} \sum_{\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}}(-1)^{\sum_{\ell\in J\cup K} a_\ell(\mathbf{x})},
\end{aligned}$$

and so, we obtain the next result.

Theorem 3 *The Walsh–Hadamard transform of $f : \mathbb{Z}_2^n \to \mathbb{Z}_q$, $2^{h-1} < q \leq 2^h$, where $f(\mathbf{x}) = \sum_{i=0}^{h-1} a_i(\mathbf{x})2^i$, $a_i \in \mathcal{B}_n$ is given by*

$$\mathcal{H}_f(\mathbf{u}) = 2^{-h} \sum_{I\subseteq\{0,\ldots,h-1\}} \zeta^{\sum_{i\in I} 2^i} \sum_{J\subseteq I, K\subseteq\bar{I}} (-1)^{|J|} W_{\sum_{\ell\in J\cup K} a_\ell(\mathbf{x})}(\mathbf{u}).$$

In the next section we will redo some of these calculations, for the particular case $q = 8$, which will allow us to completely describe the generalized bent Boolean functions in that case.

4 A Characterization of Generalized Bent Functions in $\mathbb{Z}_8$

In this section we extend the result of Solé and Tokareva [13] to generalized Boolean functions from $\mathbb{Z}_2^n$ into $\mathbb{Z}_8$. Let $\zeta = \mathbf{e}^{2\pi\imath/8} = \frac{\sqrt{2}}{2}(1+\imath)$ be the 8-primitive root of unity. Every function $f : \mathbb{Z}_2^n \to \mathbb{Z}_8$ can be written as

$$f(\mathbf{x}) = a_0(\mathbf{x}) + a_1(\mathbf{x})2 + a_2(\mathbf{x})2^2, \tag{6}$$

where $a_i(\mathbf{x})$ are Boolean functions, and '$+$' is the addition modulo 8. We prove the next lemma, which gives the connection between Walsh–Hadamard transforms of f and it components as in (6).

Lemma 4 *Let $f \in \mathcal{GB}_n^8$ as in* (6). *Then,*

$$4\mathcal{H}_f(\mathbf{u}) = \alpha_0 W_{a_2}(\mathbf{u}) + \alpha_1 W_{a_0 \oplus a_2}(\mathbf{u}) + \alpha_2 W_{a_1 \oplus a_2}(\mathbf{u}) + \alpha_3 W_{a_0 \oplus a_1 \oplus a_2}(\mathbf{u}),$$

where $\alpha_0 = 1 + (1+\sqrt{2})\imath$, $\alpha_1 = 1 + (1-\sqrt{2})\imath$, $\alpha_2 = 1 + \sqrt{2} - \imath$, $\alpha_3 = 1 - \sqrt{2} - \imath$.

Proof. We compute

$$\begin{aligned} 2^{n/2}\mathcal{H}_f(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{a_0(\mathbf{x})+a_a(\mathbf{x})2+a_2(\mathbf{x})2^2}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{a_0(\mathbf{x})}\imath^{a_1(\mathbf{x})}(-1)^{a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}. \end{aligned} \tag{7}$$

Use formula (5) with $z = \imath$ and $z = \zeta$ in equation (7), and obtain

$$\begin{aligned} 2^{n/2}\mathcal{H}_f(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \left(\frac{1+(-1)^{a_0(\mathbf{x})}}{2} + \frac{1-(-1)^{a_0(\mathbf{x})}}{2}\zeta \right) \\ &\qquad \cdot \left(\frac{1+(-1)^{a_1(\mathbf{x})}}{2} + \frac{1-(-1)^{a_1(\mathbf{x})}}{2}\imath \right)(-1)^{a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\ &= \frac{1}{4}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \Big(1 + (1+\sqrt{2})\imath + (1+(1-\sqrt{2})\imath)(-1)^{a_0(\mathbf{x})} \\ &\qquad + (1+\sqrt{2}-\imath)(-1)^{a_1(\mathbf{x})} + (1-\sqrt{2}-\imath)(-1)^{a_0(\mathbf{x})}(-1)^{a_1(\mathbf{x})} \Big) \\ &= \frac{1}{4}\sum_{\mathbf{x}\in\mathbb{Z}_2^n} \Big(\alpha_0(-1)^{a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} + \alpha_1(-1)^{a_0(\mathbf{x})\oplus a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\ &\qquad + \alpha_2(-1)^{a_1(\mathbf{x})\oplus a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} + \alpha_3(-1)^{a_0(\mathbf{x})\oplus a_1(\mathbf{x})\oplus a_2(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \Big), \end{aligned}$$

from which we derive our result. □

Corollary 5 *With the notations of the previous lemma, we have*

$$4\sqrt{2}|\mathcal{H}_f(\mathbf{u})|^2 = W^2-X^2+2XY+Y^2-2WZ-Z^2+\sqrt{2}(W^2+X^2+Y^2+Z^2), \quad (8)$$

where, we use for brevity, $W := W_{a_2}(\mathbf{u})$, $X := W_{a_0\oplus a_2}(\mathbf{u})$, $Y := W_{a_1\oplus a_2}(\mathbf{u})$, $Z := W_{a_0\oplus a_1\oplus a_2}(\mathbf{u})$.

Proof. By replacing α_i, ζ by their complex representations, the corollary follows in a rather straightforward, albeit tedious manner. □

Theorem 6 *Let* $f \in \mathcal{GB}_n^8$ *as in* (6). *Then:*

(i) *If* n *is even, then* f *is generalized bent if and only if* $a_2, a_0 \oplus a_2, a_1 \oplus a_2, a_0 \oplus a_1 \oplus a_2$ *are all bent, and* $(*)$ $W_{a_0\oplus a_2}(\mathbf{u})W_{a_1\oplus a_2}(\mathbf{u}) = W_{a_2}(\mathbf{u})W_{a_0\oplus a_1\oplus a_2}(\mathbf{u})$, *for all* $\mathbf{u} \in \mathbb{Z}_2^n$*;*

(ii) *If* n *is odd, then* f *is generalized bent if and only if* $a_2, a_0 \oplus a_2, a_1 \oplus a_2, a_0 \oplus a_1 \oplus a_2$ *are semi-bent with their values satisfying* $(*)$.

Proof. We use the W, X, Y, Z notations of Corollary 5. First, assume that $a_2, a_0 \oplus a_2, a_1 \oplus a_2, a_0 \oplus a_1 \oplus a_2$ are all bent (respectively, semi-bent). Then, replacing the corresponding values of the Walsh–Hadamard transforms in equation (8) (and using the imposed condition (*) on the Walsh–Hadamard coefficients) we obtain

$$4\sqrt{2}|\mathcal{H}_f(\mathbf{u})|^2 = 4\sqrt{2},$$

and so, $|\mathcal{H}_f(\mathbf{u})| = 1$, that is, f is gbent.

Conversely, we assume that f is gbent, and so,

$$4\sqrt{2} = W^2 - X^2 + 2XY + Y^2 - 2WZ - Z^2 + \sqrt{2}(W^2 + X^2 + Y^2 + Z^2),$$

which prompts the system

$$W^2 - X^2 + 2XY + Y^2 - 2WZ - Z^2 = 0 \quad (9)$$
$$W^2 + X^2 + Y^2 + Z^2 = 4. \quad (10)$$

We are looking for solutions in $2^{-n/2}\,\mathbb{Z}$ (a subset of $\mathbb{Q}$, if n is even or $\sqrt{2}\,\mathbb{Q}$, if n is odd).

We look at equation (10), initially, and apply Jacobi's four squares theorem (see [7], for instance).

Case (i). Let $n = 2k$ be even. Thus, W, X, Y, Z are all rational (certainly, not all 0). Write $W = 2^{-n/2}W', X = 2^{-n/2}X', Y = 2^{-n/2}Y', Z = 2^{-n/2}Z'$, and replace (9) and (10) by the system in integers

$$W'^2 - X'^2 + 2X'Y' + Y'^2 - 2W'Z' - Z'^2 = 0 \quad (11)$$
$$W'^2 + X'^2 + Y'^2 + Z'^2 = 2^{2k+2}. \quad (12)$$

Now, by Jacobi's four-squares theorem, we know there are exactly 24 solutions of (12), which are all variations in ± sign and order of $(\pm 2^k, \pm 2^k, \pm 2^k, \pm 2^k)$ or

$(\pm 2^{k+1}, 0, 0, 0)$. Further, it is straightforward to check that among these 24 solutions, only the eight tuples (X', Y', W', Z') in the list below are also satisfying equation (11),

$$\begin{aligned}&(-2^k, -2^k, -2^k, -2^k), (2^k, 2^k, -2^k, -2^k), (-2^k, -2^k, 2^k, 2^k), (-2^k, 2^k, -2^k, 2^k),\\ &(2^k, -2^k, -2^k, 2^k), (-2^k, 2^k, 2^k, -2^k), (2^k, -2^k, 2^k, -2^k), (2^k, 2^k, 2^k, 2^k).\end{aligned}$$

This implies that $(X, Y, W, Z) \in 2^{-n/2}\mathbb{Z}^4$ are any of the following:

$$\begin{aligned}&(-1, -1, -1, -1), (1, 1, -1, -1), (-1, -1, 1, 1), (-1, 1, -1, 1),\\ &(1, -1, -1, 1), (-1, 1, 1, -1), (1, -1, 1, -1), (1, 1, 1, 1),\end{aligned} \tag{13}$$

and (i) is shown (one can check easily that these solutions also satisfy condition $(*)$).

Case (ii). Let $n = 2k + 1$ be odd. Then, at least one of X, Y, W, Z is nonzero and belongs to $\sqrt{2}\,\mathbb{Q}$). As before, write $W = 2^{-n/2}W', X = 2^{-n/2}X', Y = 2^{-n/2}Y', Z = 2^{-n/2}Z'$, and replace (9) and (10) by the system in integers

$$W'^2 - X'^2 + 2X'Y' + Y'^2 - 2W'Z' - Z'^2 = 0 \tag{14}$$

$$W'^2 + X'^2 + Y'^2 + Z'^2 = 2 \cdot 2^{2k+2}, \tag{15}$$

and so, by Jacobi's four-squares theorem, equation (15) has exactly 24 solutions, which are all variations in ± sign and order of $(\pm 2^{k+1}, \pm 2^{k+1}, 0, 0)$. Further, it is straightforward to check that among these 24 solutions, the eight tuples (X', Y', W', Z') in the list below are also satisfying equation (14),

$$\begin{aligned}&(0, 2^{k+1}, 0, 2^{k+1}), (0, 2^{k+1}, 0, -2^{k+1}), (0, -2^{k+1}, 0, 2^{k+1}), (0, -2^{k+1}, 0, -2^{k+1})\\ &(2^{k+1}, 0, 2^{k+1}, 0), (2^{k+1}, 0, -2^{k+1}, 0, (-2^{k+1}, 0, 2^{k+1}, 0), (-2^{k+1}, 0, -2^{k+1}, 0).\end{aligned}$$

Thus, the solutions (X, Y, W, Z) to (9) and (10) are

$$\begin{aligned}&(0, \sqrt{2}, 0, \sqrt{2}), (0, \sqrt{2}, 0, -\sqrt{2}), (0, -\sqrt{2}, 0, \sqrt{2}), (0, -\sqrt{2}, 0, -\sqrt{2}),\\ &(\sqrt{2}, 0, \sqrt{2}, 0), (\sqrt{2}, 0, -\sqrt{2}, 0), (-\sqrt{2}, 0, \sqrt{2}, 0), (-\sqrt{2}, 0, -\sqrt{2}, 0),\end{aligned}$$

which also satisfy condition (*), and (ii) is shown. □

5 Constructions of generalized bent functions in $\mathbb{Z}_8$

In this section we define several classes of generalized bent Boolean functions.

Theorem 7 *If* $f : \mathbb{Z}_2^{n+2} \to \mathbb{Z}_8$ *(n even) is given by*

$$f(\mathbf{x}, y, z) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 2c(\mathbf{x}) + 1)y + (4b(\mathbf{x}) + 2c(\mathbf{x}) + 1)z - 2yz,$$

where $a, b, c \in \mathcal{B}_n$ *such that all* $a, b, c,$ $a \oplus c$, $b \oplus c$ *and* $a \oplus b$ *are bent satisfying*

$$W_a(\mathbf{x})W_b(\mathbf{x}) + W_{a\oplus c}(\mathbf{x})W_{b\oplus c}(\mathbf{x}) = -2W_{a\oplus b}(\mathbf{x})W_c(\mathbf{x})), \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n, \tag{16}$$

then f *is gbent in* $\mathcal{GB}_{n+2}^8$.

Proof. We compute the Walsh–Hadamard coefficients (using the fact that $\zeta = \frac{1}{\sqrt{2}}(1+\imath)$ and $\zeta^2 = \imath$)

$$\begin{aligned}
2^{(n+2)/2}\mathcal{H}_f(\mathbf{u},v,w) &= \sum_{(\mathbf{x},y,z)\in\mathbb{Z}_2^{n+2}} \zeta^{f(\mathbf{x},y,z)}(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus vy\oplus wz}\\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} \zeta^{4c(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\\
&\quad\cdot \sum_{(y,z)\in\mathbb{Z}_2^2} \zeta^{(4a(\mathbf{x})+2c(\mathbf{x})+1)y+(4b(\mathbf{x})+2c(\mathbf{x})+1)z-2yz}(-1)^{vy\oplus wz} \qquad (17)\\
&= \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{c(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\cdot\Big(1+(-1)^v(-1)^{a(\mathbf{x})}\imath^{c(\mathbf{x})}\zeta\\
&\qquad +(-1)^w(-1)^{b(\mathbf{x})}\imath^{c(\mathbf{x})}\zeta+(-1)^{a(\mathbf{x})\oplus b(\mathbf{x})\oplus c(\mathbf{x})\oplus v\oplus w}\Big).
\end{aligned}$$

Applying equation (5) with $(z,s)=(\imath,c(\mathbf{x}))$, that is,

$$i^{c(\mathbf{x})} = \frac{1+(-1)^{c(\mathbf{x})}}{2}+\frac{1-(-1)^{c(\mathbf{x})}}{2}\imath,$$

we obtain

$$\begin{aligned}
2\mathcal{H}_f(\mathbf{u},v,w) &= W_c(\mathbf{u})+\frac{(-1)^v\zeta}{2}\left(W_{a\oplus c}(\mathbf{u})+W_a(\mathbf{u})+\imath W_{a\oplus c}(\mathbf{u})-\imath W_a(\mathbf{u})\right)\\
&+\frac{(-1)^w\zeta}{2}\left(W_{b\oplus c}(\mathbf{u})+W_b(\mathbf{u})+\imath W_{b\oplus c}(\mathbf{u})-\imath W_b(\mathbf{u})\right)+(-1)^{v\oplus w}W_{a\oplus b}(\mathbf{u})\\
&= W_c(\mathbf{u})+\frac{(-1)^v}{\sqrt{2}}(W_a(\mathbf{u})+\imath W_{a\oplus c}(\mathbf{u}))+\frac{(-1)^w}{\sqrt{2}}(W_b(\mathbf{u})+\imath W_{b\oplus c}(\mathbf{u}))\\
&\qquad +(-1)^{v\oplus w}W_{a\oplus b}(\mathbf{u}).
\end{aligned}$$

Therefore, the real and the imaginary parts of $cH_f(\mathbf{u},v,w)$ are

$$\begin{aligned}
Re(\mathcal{H}_f(\mathbf{u},v,w)) &= W_c(\mathbf{u})+(-1)^{v\oplus w}W_{a\oplus b}(\mathbf{u})+\frac{(-1)^vW_a(\mathbf{u})+(-1)^wW_b(\mathbf{u})}{\sqrt{2}},\\
Im(\mathcal{H}_f(\mathbf{u},v,w)) &= \frac{(-1)^vW_{a\oplus c}(\mathbf{u})+(-1)^wW_{b\oplus c}(\mathbf{u})}{\sqrt{2}}.
\end{aligned}$$

and so,

$$\begin{aligned}
4|\mathcal{H}_f(\mathbf{u},v,w)|^2 &= \frac{1}{2}\left(W_a(\mathbf{u})^2+W_b(\mathbf{u})^2+W_{a\oplus c}(\mathbf{u})^2+W_{b\oplus c}(\mathbf{u})^2\right.\\
&\qquad \left.+2W_c(\mathbf{u})^2+2W_{a\oplus b}(\mathbf{u})^2\right)\\
&+(-1)^{v+w}(W_a(\mathbf{u})W_b(\mathbf{u})+W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u})+2W_c(\mathbf{u})W_{a\oplus b}(\mathbf{u})) \qquad (18)\\
&+\sqrt{2}\,((-1)^v(W_a(\mathbf{u})W_c(\mathbf{u})+W_b(\mathbf{u})W_{a\oplus b}(\mathbf{u}))\\
&+(-1)^w(W_b(\mathbf{u})W_c(\mathbf{u})+W_a(\mathbf{u})W_{a\oplus b}(\mathbf{u})))
\end{aligned}$$

Since $a, b, c, a \oplus c, b \oplus c, a \oplus b$ are all bent then $|W_a(\mathbf{u})| = |W_b(\mathbf{u})| = |W_c(\mathbf{u})| = |W_{a\oplus b}(\mathbf{u})| = |W_{a\oplus c}(\mathbf{u})| = |W_{b\oplus c}(\mathbf{u})| = 1$. Further, from the imposed conditions on these functions' Walsh–Hadamard coefficients, we see that $W_a(\mathbf{u})W_b(\mathbf{u}) + W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + 2W_c(\mathbf{u})W_{a\oplus b}(\mathbf{u}) = 0$, and also $W_a(\mathbf{u})W_c(\mathbf{u}) + W_b(\mathbf{u})W_{a\oplus b}(\mathbf{u}) = 0$, $W_b(\mathbf{u})W_c(\mathbf{u}) + W_a(\mathbf{u})W_{a\oplus b}(\mathbf{u}) = 0$ (that is because if $W_a(\mathbf{u})$ and $W_b(\mathbf{u})$ have the same sign, then $W_c(\mathbf{u}), W_{a\oplus b}$ have opposite signs; further, $W_a(\mathbf{u})$ and $W_b(\mathbf{u})$ have opposite signs, then $W_c(\mathbf{u}), W_{a\oplus b}$ have the same sign). Using these equations, we get that $4|\mathcal{H}_f(\mathbf{u}, v, w)|^2 = 4$, and so, f is gbent.

□

Remark 8 *It is rather straightforward to see that condition* (16) *has* 16 *solutions. More precisely,* $(W_a(\mathbf{x}), W_b(\mathbf{x}), W_{a\oplus c}(\mathbf{x}), W_{b\oplus c}, W_{a\oplus b}(\mathbf{x}), W_c(\mathbf{x}))$ *could be any of the following tuples:*

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

Theorem 9 *If* $f : \mathbb{Z}_2^{n+2} \to \mathbb{Z}_8$ *(n even) is given by*

$$f^\epsilon(\mathbf{x}, y, z) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 1)y + (4b(\mathbf{x}) + 1)z + 2\epsilon yz, \tag{19}$$

where $\epsilon \in \{1, -1\}$, $a, b, c \in \mathcal{B}_n$ *such that all* c, $a \oplus c$, $b \oplus c$ *and* $a \oplus b \oplus c$ *are bent, with*

$$W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + \epsilon W_c(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}) = 0, \text{ for all } \mathbf{u} \in \mathbb{Z}_2^n, \tag{20}$$

then f *is gbent in* $\mathcal{GB}_{n+2}^8$.

Proof. As in the proof of Theorem 7, we compute the Walsh–Hadamard coefficients, obtaining

$$\begin{aligned}
2\mathcal{H}_{f^\epsilon}(\mathbf{u}, v, w) &= W_c(\mathbf{u}) + (-1)^v \zeta W_{a\oplus c}(\mathbf{u}) + (-1)^w \zeta W_{b\oplus c}(\mathbf{u}) \\
&\qquad + (-1)^{v\oplus w} \zeta^{2+2\epsilon} W_{a\oplus b\oplus c}(\mathbf{u}) \\
&= W_c(\mathbf{u}) - \epsilon(-1)^{v\oplus w} W_{a\oplus b\oplus c}(\mathbf{u}) \\
&\quad + \frac{(-1)^v W_{a\oplus c}(\mathbf{u}) + (-1)^w W_{b\oplus c}(\mathbf{u})}{\sqrt{2}} \\
&\quad + \imath \frac{(-1)^v W_{a\oplus c}(\mathbf{u}) + (-1)^w W_{b\oplus c}(\mathbf{u})}{\sqrt{2}},
\end{aligned}$$

using the fact that $\zeta^{2+2\epsilon} = -\epsilon$, for $\epsilon \in \{1, -1\}$. Taking the square of the complex norm, we get

$$\begin{aligned}
4|\mathcal{H}_{f^\epsilon}(\mathbf{u}, v, w)|^2 &= W_{a\oplus c}(\mathbf{u})^2 + W_{b\oplus c}(\mathbf{u})^2 + W_c(\mathbf{u})^2 + W_{a\oplus b\oplus c}(\mathbf{u})^2 \\
&\quad +2(-1)^{v+w}\left(W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + \epsilon W_c(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u})\right) \\
&\quad +\sqrt{2}\left((-1)^v(W_{a\oplus c}(\mathbf{u})W_c(\mathbf{u}) + \epsilon W_{b\oplus c}(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}))\right. \\
&\quad \left.+(-1)^w(W_{b\oplus c}(\mathbf{u})W_c(\mathbf{u}) + \epsilon W_{a\oplus c}(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}))\right) \\
&= 4,
\end{aligned}$$

because c, $a \oplus c$, $b \oplus c$ and $a \oplus b \oplus c$ are all bent, so their Walsh–Hadamard coefficients are 1 in absolute values, and equation (20) implies that the remaining coefficients are all 0 (that can be seen by the following argument: if $A, B, C, D \in \{\pm 1\}$, and $AB + CD = 0$, then by multiplying by BC, we get $AC + BD = 0$, and by multiplying by AC we get $BC + AD = 0$).

Therefore, $|\mathcal{H}_{f^\epsilon}(\mathbf{u}, v, w)|^2 = 1$, so f is gbent, and the theorem is proved. □

Remark 10 *It is rather easy to see that equation* (20) *has* 8 *solutions (as expected, since there are four degrees of freedom and one constraint). Moreover, one can give plenty of concrete examples of functions a, b, c satisfying the conditions of our theorem. For example, if $\epsilon = -1$, one could take in equation* (19), *a bent Boolean c, and $a = b$ such that $c \oplus a$ is bent (for instance, if $a = b$ are affine functions, that condition is immediate). Then, $W_{a\oplus c}(\mathbf{u})W_{b\oplus c}(\mathbf{u}) + \epsilon W_c(\mathbf{u})W_{a\oplus b\oplus c}(\mathbf{u}) = W_{c\oplus a}(\mathbf{u})^2 - W_c(\mathbf{u})^2 = 0$, and so, g as in our theorem is gbent.*

Theorem 11 *Let $f : \mathbb{Z}_2^{n+1} \to \mathbb{Z}_8$ (n is even) be given by*

$$f(\mathbf{x}, y) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 4c(\mathbf{x}) + 2\epsilon)y, \tag{21}$$

where $\epsilon \in \{1, -1\}$. Then f is gbent in $\mathcal{GB}_{n+1}^8$ if and only if a, c are bent in $\mathcal{B}_n$. Moreover, if g is given by

$$g(\mathbf{x}, y) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 2c(\mathbf{x}) + 2\epsilon)y, \tag{22}$$

where $\epsilon \in \{1, -1\}$, $a, c \in \mathcal{B}_n$ such that a, c, $a \oplus c$ are all bent, then g is gbent in $\mathcal{GB}_{n+1}^8$. Further, let h be given by

$$h(\mathbf{x}, y) = 4c(\mathbf{x}) + (4a(\mathbf{x}) + 2\epsilon)y, \tag{23}$$

where $\epsilon \in \{1, -1\}$. Then h is gbent in $\mathcal{GB}_{n+1}^8$ if and only if $c, a \oplus c$ are bent in $\mathcal{B}_n$.

Proof. We will show the first claim, since the proof of the remaining ones are absolutely similar. As in the proof of Theorem 7, the Walsh–Hadamard coefficients at an arbitrary input $(\mathbf{u}, v)$ are

$$\sqrt{2}\mathcal{H}_f(\mathbf{u}, v) = W_c(\mathbf{u}) + \imath^\epsilon(-1)^v W_a(\mathbf{u}) = W_c(\mathbf{u}) + \epsilon\, \imath(-1)^v W_a(\mathbf{u}),$$

and so,

$$2|\mathcal{H}_f(\mathbf{u},v)|^2 = W_c(\mathbf{u})^2 + W_a(\mathbf{u})^2.$$

If a, c are bent, then $|W_c(\mathbf{u})| = |W_a(\mathbf{u})| = 1$, and so $|\mathcal{H}_f(\mathbf{u},v)| = 1$, that is f is gbent. If f is gbent, then the equation $W_c(\mathbf{u})^2 + W_a(\mathbf{u})^2 = 2$ has as rational solutions only $|W_c(\mathbf{u})| = |W_a(\mathbf{u})| = 1$, and so, a, c are bent. □

References

1. C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
2. C. Carlet, *Vectorial Boolean functions for cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge. Available: http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html.
3. T. W. Cusick, P. Stănică, Cryptographic Boolean functions and applications, Elsevier – Academic Press, 2009.
4. J. F. Dillon, *Elementary Hadamard difference sets*, Proc. of Sixth S.E. Conference of Combinatorics, Graph Theory, and Computing, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg 1975, 237–249.
5. S. Gangopadhyay, B. K. Singh and P. Stănică, *On Generalized Bent Functions*, preprint.
6. S. Gangopadhyay, B. K. Singh and P. Stănică, *Generalized Bent Functions in the Framework of Generalized Partial Spreads*, preprint.
7. M. D. Hirschhorn, A simple proof of Jacobis foursquare theorem, Proc. Amer. Math. Soc., 101 (1987), 436–438.
8. P. V. Kumar, R. A. Scholtz, and L. R. Welch, *Generalized bent functions and their properties*, J. Combin. Theory (A) 40 (1985), 90–107.
9. F. J. MacWilliams, N. J. A. Sloane, The theory of error–correcting codes, North-Holland, Amsterdam, 1977.
10. O. S. Rothaus, *On bent functions*, J. Combinatorial Theory Ser. A 20 (1976), 300–305.
11. P. Sarkar, S. Maitra, *Cross–Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes*, Theory Comput. Systems 35 (2002), 39–57.
12. K-U. Schmidt, *Quaternary Constant-Amplitude Codes for Multicode CDMA*, IEEE International Symposium on Information Theory, ISIT'2007 (Nice, France, June 24–29, 2007), 2781–2785; available at http://arxiv.org/abs/cs.IT/0611162.
13. P. Solé, N. Tokareva, *Connections between Quaternary and Binary Bent Functions*, http://eprint.iacr.org/2009/544.pdf.