On constructions and properties of self-dual generalized bent functions

Aleksandr Kutsenko*

Sobolev Institute of Mathematics, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia

alexandrkutsenko@bk.ru

Abstract

Bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$, where $q \geqslant 2$ is a positive integer, are known as generalized bent (gbent) functions (K.-U Schmidt, 2006). There is a class of gbent functions for which it is possible to define a dual gbent function, gbent functions that possess this property are called regular. A regular gbent function is said to be self-dual if it coincides with its dual. In this paper we explore self-dual generalized bent functions. We give necessary and sufficient conditions for the self-duality of Maiorana–McFarland gbent functions, consider self-dual bent functions obtained by the direct sum of generalized Boolean functions. We provide a sufficient condition for a gbent function from Dillon's Partial Spreads to be self-dual. Two iterative constructions based on the generalization of iterative constructions of Boolean self-dual bent functions are presented. We prove that the set of sign functions of self-dual gbent functions in even number n of variables has dimension 2^{n-1}. We find all self-dual gbent functions symmetric with respect to two variables and prove that self-dual gbent function can not be affine. Symmetries that preserve self-duality are also discussed.

1 Introduction

Boolean bent functions were introduced by [20], they have applications in cryptograohy and coding theory. In 2000, Wada [29] established a connection between bent functions and binary constant-amplitude codewords.

Having applications of functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_4$ in code-division multiple access (CDMA) systems, K.-U Schmidt introduced in [21] the bentness of a generalized Boolean function and also studied quaternary generalized bent (gbent) functions (see also paper [22]). Note that generalized Boolean functions were also studied in a perspective of obtaining linear

*The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

codes, see [16]. In recent years generalized bent functions obtained much attention. In papers [13, 24] several constructions and properties of generalized bent functions were obtained. The question of the characterization of generalized bent functions was recently studied in [7, 14, 25].

Self-dual bent functions were explored by C. Carlet et al. in 2010 [3], main constructions and properties were given and the classification for small number of variables was provided. Next steps for the classification were made in [5], quadratic self-dual bent functions were characterized in [9]. Other constructions, metrical properties and groups of automorphisms of self-dual bent functions were studied in [15, 10, 11, 12]. In 2018 L. Sok. et al. in paper [23] studied quaternary self-dual bent functions from the viewpoints of existence, construction, and symmetry. In current work we investigate constructions, symmetries and other properties of self-dual generalized bent functions $\mathbb{F}_2^n \to \mathbb{Z}_q$, when q is even.

A survey on different generalizations of bent functions can be found in [26].

2 Notation

Let $\mathbb{F}_2^n$ be a set of binary vectors of length n. For $x, y \in \mathbb{F}_2^n$ denote $\langle x, y\rangle = \bigoplus_{i=1}^{n} x_i y_i$, where the sign $\oplus$ denotes a sum modulo 2. Denote, following [6], the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in \mathrm{GL}\,(n, \mathbb{F}_2) : LL^T = I_n \right\},$$

where L^{T} denotes the transpose of L and I_n is an identical matrix of order n over the field $\mathbb{F}_2$.

A *generalized Boolean function* f in n variables is any map from $\mathbb{F}_2^n$ to $\mathbb{Z}_q$, the integers modulo q. The set of generalized Boolean functions in n variables is denoted by $\mathcal{GF}_n^q$. Let $\omega = e^{2\pi i/q}$. A *sign* function of $f \in \mathcal{GF}_n^q$ is a complex valued function $F = \omega^f$, we will also refer to it as to a complex vector $\left(\omega^{f_0}, \omega^{f_1}, ..., \omega^{f_{2^n-1}}\right)$ of length 2^n, where $(f_0, f_1, ..., f_{2^n-1})$ is a vector of values of the function f.

The *Hamming weight* $\mathrm{wt}_H(x)$ of the vector $x \in \mathbb{F}_2^n$ is the number of nonzero coordinates of x. The *Hamming distance* $\mathrm{dist}_H(f, g)$ between generalized Boolean functions f, g in n variables is the cardinality of the set $\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}$. The Lee weight of the element $x \in \mathbb{Z}_q$ is $\mathrm{wt}_L(x) = \min\{x, q - x\}$. The Lee distance $\mathrm{dist}_L(f, g)$ between $f, g \in \mathcal{GF}_n^q$ is

$$\mathrm{dist}_L(f, g) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}_L\left(\delta(x)\right),$$

where $\delta \in \mathcal{GF}_n^q$ and $\delta(x) = f(x) + (q-1)g(x)$ for any $x \in \mathbb{F}_2^n$. For Boolean case $q = 2$ the Hamming distance coincides with the Lee distance.

The *(generalized) Walsh–Hadamard transform* of $f \in \mathcal{GF}_n^q$ is the complex valued function:

$$H_f(y) = \sum_{x \in \mathbb{F}_2^n} \omega^{f(x)} (-1)^{\langle x, y\rangle}.$$

A generalized Boolean function f in n variables is said to be *generalized bent* (gbent) if

$$|H_f(y)| = 2^{n/2},$$

for all $y \in \mathbb{F}_2^n$ [21]. If there exists such $\widetilde{f} \in \mathcal{GF}_n^q$ that $H_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$ for any $y \in \mathbb{F}_2^n$, the gbent function f is said to be *regular* and $\widetilde{f}$ is called its *dual*. Note that $\widetilde{f}$ is generalized bent as well. A regular gbent function f is said to be *self-dual* if $f = \widetilde{f}$, and *anti-self-dual* if $f = \widetilde{f} + \frac{q}{2}$. Consequently, it is the case only for even q. So throughout this paper we assume that q is a natural even number.

3 Constructions

3.1 Direct sum

Suppose $n = n_1 + n_2 + \cdots + n_r$ and $p_k \leqslant q$, where n_k, p_k are positive integers for $k = 1, 2, ..., r$. Let $f \in \mathcal{GF}_n^q$, consider gbent functions $f_k \in \mathcal{GF}_{n_k}^{p_k}$, $k = 1, 2, ..., r$. The function

$$f(x) = f_1\left(x^{(1)}\right) + f_2\left(x^{(2)}\right) + \cdots + f_r\left(x^{(r)}\right),$$

where $x^{(k)} \in \mathbb{F}_2^{n_k}$ and $x = \left(x^{(1)}, x^{(2)}, ..., x^{(r)}\right) \in \mathbb{F}_2^n$, is a *direct sum* of generalized Boolean functions f_k. Gbent functions obtained by a direct sum of generalized Boolean functions were studied in paper [8], it was proved that function f is gbent if and only if all f_k are gbent functions. Here we consider self-dual bent functions obtained by this construction.

Proposition 1. *Assume all numbers p_k are even and $f_k \in \mathcal{GF}_{n_k}^{p_k}$ are gbent functions such that $\widetilde{f_k} = f_k + c_k\,(p_k/2)$, where $c_k \in \mathbb{F}_2$, $k = 1, 2, ..., r$. If there is an even number of nonzero coefficients c_k, then the function f is a self-dual gbent function in n variables.*

3.2 Maiorana–McFarland class

Bent functions in $2k$ variables which have a representation

$$f(x, y) = \langle x, \pi(y)\rangle \oplus g(y),$$

where $x, y \in \mathbb{F}_2^k$, $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a Boolean function in k variables, form the well known *Maiorana–McFarland* class of bent functions. It is known [2] that the dual of a Maiorana–McFarland bent function $f(x, y)$ is equal to

$$\widetilde{f}(x, y) = \langle \pi^{-1}(x), y\rangle \oplus g\left(\pi^{-1}(x)\right).$$

A generalization of this construction for the case $q = 4$ was given by Schmidt in [21]. In [24] this construction was given for any even q, thus, forming the following construction

$$f(x, y) = \frac{q}{2}\langle x, \pi(y)\rangle + g(y),$$

where $x, y \in \mathbb{F}_2^k$, $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and g is a generalized Boolean function in k variables. Its dual is

$$\widetilde{f}(x,y) = \frac{q}{2}\langle \pi^{-1}(x), y\rangle + g\left(\pi^{-1}(x)\right).$$

In the article [3] necessary and sufficient conditions of (anti-)self-duality of Maiorana–McFarland bent functions, denoted by $\mathrm{SB}^+_{\mathcal{M}}(n)$ ($\mathrm{SB}^-_{\mathcal{M}}(n)$), were given. In [23] quaternary self-dual Maiorana–McFarland bent functions were studied and necessary and sufficient conditions of self-duality were obtained for them.

In the current work we generalize these results for any even q. Denote the sets of (anti-)self-dual generalized Maiorana–McFarland bent functions by $\mathrm{SB}^+_{\mathcal{M}^q}(n)$ ($\mathrm{SB}^-_{\mathcal{M}^q}(n)$)

Theorem 2. *A generalized Maiorana–McFarland bent function*

$$f(x,y) = \frac{q}{2}\langle x, \pi(y)\rangle + g(y),\ x, y \in \mathbb{F}_2^{n/2},$$

is (anti-)self-dual bent if and only if for any $y \in \mathbb{F}_2^{n/2}$

$$\pi(y) = L(y \oplus b), \quad g(y) = \frac{q}{2}\langle b, y\rangle + d,$$

where $L \in \mathcal{O}_{n/2}, b \in \mathbb{F}_2^{n/2}$, $\mathrm{wt}(b)$ is even (odd), $d \in \mathbb{Z}_q$.

Proof. Let $f(x,y) = \frac{q}{2}\langle x, \pi(y)\rangle \oplus g(y)$, where π is a permutation on $\mathbb{F}_2^{n/2}$, $g \in \mathcal{GF}^q_{n/2}$, $x, y \in \mathbb{F}_2^{n/2}$. By the definition of (anti-)self-duality a generalized bent function is (anti-)self-dual if it coincides with (the complement of) its dual. Then for all $x, y \in \mathbb{F}_2^n$ it must hold

$$\frac{q}{2}\langle x, \pi(y)\rangle + g(y) = \frac{q}{2}\left\langle \pi^{-1}(x), y\right\rangle + g\left(\pi^{-1}(x)\right) + \frac{q}{2}c, \tag{1}$$

where $c \in \mathbb{F}_2$: $c = 0$ if $f = \widetilde{f}$ and $c = 1$ if $f = \widetilde{f} + \frac{q}{2}$.

Put zero vector $x \in \mathbb{F}_2^{n/2}, (x = \mathbf{0})$, in (1), then for any $y \in \mathbb{F}_2^n$ we have

$$g(y) = \frac{q}{2}\left\langle \pi^{-1}(\mathbf{0}), y\right\rangle + g\left(\pi^{-1}(\mathbf{0})\right) + \frac{q}{2}c.$$

The condition (1) can be transformed to

$$\frac{q}{2}\langle x, \pi(y)\rangle + \frac{q}{2}\left\langle \pi^{-1}(\mathbf{0}), y\right\rangle + g\left(\pi^{-1}(\mathbf{0})\right) = \frac{q}{2}\left\langle \pi^{-1}(x), y\right\rangle + \frac{q}{2}\left\langle \pi^{-1}(\mathbf{0}), \pi^{-1}(x)\right\rangle + g\left(\pi^{-1}(\mathbf{0})\right) + \frac{q}{2}c,$$

or, equivalently,

$$\frac{q}{2}\langle x, \pi(y)\rangle + \frac{q}{2}\left\langle \pi^{-1}(\mathbf{0}), y\right\rangle = \frac{q}{2}\left\langle \pi^{-1}(x), y\right\rangle + \frac{q}{2}\left\langle \pi^{-1}(\mathbf{0}), \pi^{-1}(x)\right\rangle + \frac{q}{2}c. \tag{2}$$

In both sides of (2) monomials of algebraic degree more than 2 can not occur, since the left part has algebraic degree at most 1 with respect to x provided that y is fixed

and the right part has algebraic degree at most 1 with respect to y provided that x is fixed. Therefore, the mapping π is an affine permutation, that is $\pi(x) = L(x \oplus b)$ for any $x \in \mathbb{F}_2^n$, where L is a $(n/2) \times (n/2)$ nonsingular binary matrix, $b \in \mathbb{F}_2^{n/2}$.

Since the equality (2) should be considered by modulo q, we only care about the parity of components of both sides, thus, for any $x, y \in \mathbb{F}_2^{n/2}$ having the following equality

$$\langle x, L(y \oplus b)\rangle \oplus \langle b, y\rangle = \left\langle L^{-1}x \oplus b, y\right\rangle \oplus \left\langle b, L^{-1}x \oplus b\right\rangle \oplus c. \tag{3}$$

Put zero vector$x \in \mathbb{F}_2^{n/2}, (x = \mathbf{0})$ in (3), then for any $y \in \mathbb{F}_2^{n/2}$ it must hold $\langle b, b\rangle = c$. Rewrite (3) in the form

$$\left\langle x, Ly \oplus \left(L^{-1}\right)^T y\right\rangle = \left\langle x, Lb \oplus \left(L^{-1}\right)^T b\right\rangle,$$

and consider it for a zero vector $y \in \mathbb{F}_2^{n/2}, (y = \mathbf{0})$:

$$\left\langle x, Lb \oplus \left(L^{-1}\right)^T b\right\rangle = 0,$$

that is $Lb \oplus (L^{-1})^T b = \mathbf{0}$ or, equivalently, $Lb = (L^{-1})^T b$. It means that

$$\left\langle x, \left(L \oplus \left(L^{-1}\right)^T\right) y\right\rangle = 0,$$

for any $x, y \in \mathbb{F}_2^{n/2}$. From this it follows that $L^{-1} = L^T$, that is $L \in \mathcal{O}_{n/2}$. □

It follows that the number of such functions is a function of q and the cardinality of the orthogonal group.

Corollary 3. *It holds*

$$\left|\mathrm{SB}^+_{\mathcal{GM}^q}(n)\right| = \left|\mathrm{SB}^-_{\mathcal{GM}^q}(n)\right| = q \cdot 2^{n/2-1} \left|\mathcal{O}(n/2, \mathbb{F}_2)\right|.$$

3.3 Dillon functions type

In [13] an explicit representation of functions in a generalization of Dillon's $\mathcal{PS}_{ap}$ class to gbent functions with $q = 2^k$ was presented. By comparing the function from $\mathcal{PS}_{ap}$ in a bivariate form with its dual (that was also given in [13]) we obtain the following result.

Theorem 4. *Assume G_j, $j = 0, 1, ..., k-1$, be balanced Boolean functions in m variables with $G_j(0) = 0$ and $\sum_{t \in \mathbb{F}_{2^m}} \omega^{\sum_{j=0}^{k-1} 2^j G_j(t)} = 0$. Then, if $G_j(u) = G_j(1/u)$ for any $u \in \mathbb{F}_{2^m}$ (with the convention $1/0 = 0$), then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{Z}_{2^k}$ given by*

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

is self-dual gbent in $2m$ variables.

3.4 Iterative construction

Let f_0, f_1, f_2, f_3 be Boolean functions in n variables. Consider a Boolean function g in $n+2$ variables which is defined as

$$g(00,x) = f_0(x), \quad g(01,x) = f_1(x), \quad g(10,x) = f_2(x), \quad g(11,x) = f_3(x), \quad x \in \mathbb{F}_2^n.$$

It is known (Preneel et al., 1991; see also [1, 27]) that under condition that all f_0, f_1, f_2, f_3 are Boolean bent functions in n variables, the mentioned function g is a bent function in $n+2$ variables if and only if

$$\widetilde{f_0} \oplus \widetilde{f_1} \oplus \widetilde{f_2} \oplus \widetilde{f_3} = 1,$$

that gives the construction of a bent function in $n+2$ variables through the concatenation of vectors of values of four bent functions in n variables [17].

Following N. Tokareva [27], we will refer to Boolean bent functions obtained by this construction as *bent iterative functions* ($\mathcal{BI}$). The set of such bent functions in n variables is denoted by $\mathcal{BI}_n$. A construction of generalized bent functions in $n+2$ variables obtained by concatenation of four generalized Boolean functions on n variables was studied in [18].

Bent iterative constructions of self-dual Boolean bent functions in $n+2$ variables, based on concatenation of 4 Boolean bent functions in n variables, were presented in [3, 11]. In current work we give two constructions of generalized bent iterative functions that generalize the constructions for Boolean case:

Theorem 5. *1) Let f be a regular gbent function in n variables, then the sign function*

$$\left(F, \widetilde{F}, \widetilde{F}, -F\right),$$

where $F = \omega^f$ and $\widetilde{F} = \omega^{\widetilde{f}}$, is the sign function of a self-dual gbent function in $n+2$ variables;

2) Let f be a self-dual gbent function in n variables with the sign function F, and g be an anti-self-dual gbent function in n variables with the sign function G, then the sign function

$$(F, G, -G, F),$$

where $F = \omega^f$ and $G = \omega^g$, is the sign function of a gbent function in $n+2$ variables.

4 Sign functions of (anti-)self-dual gbent functions

Let I_n be the identity matrix of size n and $H_n = H_1^{\otimes n}$ be the n-fold tensor product of the matrix H_1 with itself, where

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It is known the Hadamard property of this matrix

$$H_n H_n^T = 2^n I_{2^n},$$

where H_n^T is transpose of H_n (it holds $H_n^T = H_n$ by symmetricity of H_n).

Recall an orthogonal decomposition of $\mathbb{R}^{2^n}$ in eigenspaces of H_n from [3] (Lemma 5.2):

$$\mathbb{R}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

where the symbol $\oplus$ denotes a direct sum of subspaces. Consider the same decomposition

$$\mathbb{C}^{2^n} = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right) \oplus \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right),$$

for a complex space $\mathbb{C}^{2^n}$.

As for the Boolean case (see [12]), we note that sign function of any self-dual gbent function is the eigenvector of $\mathcal{H}_n$ attached to the eigenvalue 1, that is an element from the subspace $\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right) = \mathrm{Ker}\left(H_n - 2^{n/2} I_{2^n}\right)$. The same holds for a sign function of any anti-self-dual gbent function, which obviously is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue (-1), that is an element from the subspace $\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right) = \mathrm{Ker}\left(H_n + 2^{n/2} I_{2^n}\right)$.

It is known that

$$\dim\left(\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)\right) = \dim\left(\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)\right) = 2^{n-1},$$

where $\dim(V)$ is the dimension of the subspace $V \subseteq \mathbb{R}^{2^n}$. Moreover, since $\mathcal{H}_n$ is symmetric (Hermitian), the subspaces $\mathrm{Ker}\left(\mathcal{H}_n + I_{2^n}\right)$ and $\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ are mutually orthogonal.

In [11] it was proved that provided $n \geqslant 4$, the linear span of sign functions of self-dual as well as anti-self-dual Boolean bent functions Boolean bent functions in n variables has dimension 2^{n-1}. The same result can be also given for gbent functions:

Theorem 6. *Let $n \geqslant 4$, then the linear span of sign functions of (anti-)self-dual gbent functions in n variables has dimension 2^{n-1}.*

Proof. It is enough to mention that since q is even it holds $(-1) = \omega^{q/2} \in \{\omega, \omega^2, ..., \omega^{q-1}\}$, therefore the set of sign fuctions of (anti-)self-dual Boolean bent functions in n variables is a subset of the set of sign functions of (anti-)self-dual gbent functions in n variables. Then from [11] (Theorem 2) the dimension follows. □

It is worth to note that the example of the basis of the subspace $\mathrm{Ker}\left(\mathcal{H}_n - I_{2^n}\right)$ can be constructed by using the functions obtained in Theorem 5.

When $n = 2$ there are two self-dual Boolean bent functions, namely x_1x_2 and $x_1x_2 \oplus 1$, which have sign functions $(1, 1, 1, -1)$ and $(-1, -1, -1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$. The set $\mathrm{SB}^-(2)$ consists of functions $x_1x_2 \oplus x_1 \oplus x_2$ and $x_1x_2 \oplus x_1 \oplus x_2 \oplus 1$ with sign functions $(1, -1, -1, -1)$ and $(-1, 1, 1, 1)$ respectively. These sign functions are linearly dependent vectors in $\mathbb{R}^4$ as well. Generalization comprises solution of the system

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix} = \begin{pmatrix} \omega^{d_1} \\ \omega^{d_2} \\ \omega^{d_3} \\ \omega^{d_4} \end{pmatrix},$$

where variables are numbers $d_1, d_2, d_3, d_4 \in \mathbb{Z}_q$ in fact. It is clear that the only solution pattern is

$$\left(\omega^d, \omega^d, \omega^d, \omega^{d+q/2}\right) = \omega^d \cdot (1, 1, 1, -1) \in \mathbb{C}^4,$$

where $d \in \mathbb{Z}_q$. It means that any two sign functions of self-dual gbent functions from $\mathrm{SB}_q^+(2)$ are linearly dependent over $\mathbb{C}$.

5 Self-dual gbent functions symmetric with respect to two variables

A generalized Boolean function $h \in \mathcal{GF}_{n+2}^q$ is symmetric with respect to two variables y and z if and only if there exist functions $f, g, s \in \mathcal{GF}_n^q$ such that

$$h(z, y, x) = f(x) + (y \oplus z)g(x) + yzs(x), \quad y, z \in \mathbb{F}_2, x \in \mathbb{F}_2^n. \tag{4}$$

In paper [24] it was proved that a function of such form is gbent if and only if the functions $f, f + g$ are gbent and $s(x) = q/2, x \in \mathbb{F}_2^n$. We study the conditions for self-duality of functions of such form.

Theorem 7. *Let h be a gbent function of the form (4). Then h is self-dual if and only if f is gbent, $g = \widetilde{f} + (q-1)f$, and $s(x) = q/2, x \in \mathbb{F}_2^n$.*

Proof. Let F, FG be sign functions of gbent functions $f, f + g$. It is clear that

$$\omega^h = \begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix}.$$

Then the function h is self-dual gbent if and only if

$$\omega^{\widetilde{h}} = \mathcal{H}_{n+2}\omega^h = \frac{1}{2}\begin{pmatrix} \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n \\ \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n \end{pmatrix}\begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix} = \begin{pmatrix} F \\ FG \\ FG \\ -F \end{pmatrix} = \omega^h.$$

Consider the system

$$\begin{aligned}\omega^{\widetilde{h}} &= \frac{1}{2}\begin{pmatrix}\mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n & \mathcal{H}_n\\ \mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n\\ \mathcal{H}_n & \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n\\ \mathcal{H}_n & -\mathcal{H}_n & -\mathcal{H}_n & \mathcal{H}_n\end{pmatrix}\begin{pmatrix}F\\ FG\\ FG\\ -F\end{pmatrix}\\ &= \frac{1}{2}\begin{pmatrix}\mathcal{H}_nF + \mathcal{H}_n(FG) + \mathcal{H}_n(FG) + \mathcal{H}_nF\\ \mathcal{H}_nF - \mathcal{H}_n(FG) + \mathcal{H}_n(FG) - \mathcal{H}_nF\\ \mathcal{H}_nF + \mathcal{H}_n(FG) - \mathcal{H}_n(FG) - \mathcal{H}_nF\\ \mathcal{H}_nF - \mathcal{H}_n(FG) - \mathcal{H}_n(FG) + \mathcal{H}_nF\end{pmatrix}\\ &= \frac{1}{2}\begin{pmatrix}\widetilde{F} - \widetilde{F} + 2\widetilde{FG}\\ 2\widetilde{F} - \widetilde{FG} + \widetilde{FG}\\ 2\widetilde{F} + \widetilde{FG} - \widetilde{FG}\\ -2\widetilde{FG}\end{pmatrix} = \begin{pmatrix}\widetilde{FG}\\ \widetilde{F}\\ \widetilde{F}\\ -\widetilde{FG}\end{pmatrix}.\end{aligned}$$

Writing

$$\begin{pmatrix}\widetilde{FG}\\ \widetilde{F}\\ \widetilde{F}\\ -\widetilde{FG}\end{pmatrix} = \begin{pmatrix}F\\ FG\\ FG\\ -F\end{pmatrix},$$

we see that $\widetilde{f} = f + g$, or, equivalently, $g = \widetilde{f} + (q-1)f$.

Thus, we have

$$h(z, y, x) = f(x) + (z \oplus y)\left[\widetilde{f}(x) + (q-1)f(x)\right] + \frac{q}{2}zy.$$

□

6 Affinity of self-dual gbent function

In paper [18] for the case when q is divisible by 4, necessary and sufficient conditions for the bentness of generalized Boolean functions of the form

$$f(x) = \sum_{i=1}^{n} \lambda_i x_i + \lambda_0,$$

where $\lambda_0, \lambda_1, ..., \lambda_n \in \mathbb{Z}_q$, were obtained. Functions from this class are referred to as *affine* functions.

It is well known that Boolean bent function and, as a consequence, self-dual Boolean bent function can not be affine. The next result shows non-existence of self-dual gbent functions in the class of affine functions.

Theorem 8. *There are no self-dual generalized bent functions in n variables of the form*

$$f(x)=\sum_{i=1}^{n}\lambda_i x_i+\lambda_0,$$

where $\lambda_0,\lambda_1,...,\lambda_n\in\mathbb{Z}_q$.

Proof. Let f be an affine gbent function in n variables (for the case q not divisible by 4 if such exists, otherwise the result follows), namely

$$f(x)=\sum_{i=1}^{n}\lambda_i x_i+\lambda_0,\quad x\in\mathbb{F}_2^n,$$

where $\lambda_0,\lambda_1,...,\lambda_n\in\mathbb{Z}_q$. It is self-dual if and only if

$$\mathcal{H}_f(y)=\sum_{x\in\mathbb{F}_2^n}\omega^{f(x)}(-1)^{\langle x,y\rangle}=\omega^{\lambda_0}\sum_{x\in\mathbb{F}_2^n}\omega^{\sum\limits_{i=1}^{n}\lambda_i x_i+\frac{q}{2}\langle x,y\rangle}$$
$$=\omega^{\lambda_0}\prod_{i=1}^{n}\sum_{x_i\in\mathbb{F}_2}\omega^{\lambda_i x_i+\frac{q}{2}y_i x_i}=\omega^{\lambda_0}\prod_{i=1}^{n}\left(1+\omega^{\frac{q}{2}y_i+\lambda_i}\right),$$

for any $y\in\mathbb{F}_2^n$.

For every $y\in\mathbb{F}_2^n$ denote

$$\begin{aligned}\widehat{y}&=(y_1,y_2,...,y_{n-1})\in\mathbb{F}_2^{n-1},\\ P_{n-1}(\widehat{y})&=\left(1+\omega^{\frac{q}{2}y_1+\lambda_1}\right)\left(1+\omega^{\frac{q}{2}y_2+\lambda_2}\right)\cdot...\cdot\left(1+\omega^{\frac{q}{2}y_{n-1}+\lambda_{n-1}}\right),\\ a_{n-1}(\widehat{y})&=\lambda_1y_1+\lambda_2y_2+\cdots+\lambda_{n-1}y_{n-1}.\end{aligned}$$

We can note that $P_{n-1}(\widehat{y})\neq 0$ since $\mathcal{H}_f(y)=\omega^{\lambda_0}P_{n-1}(\widehat{y})\left(1+\omega^{\frac{q}{2}y_n+\lambda_n}\right)$ and f is gbent.

Then for any $y\in\mathbb{F}_2^n$ such that $y_n=0$ we have

$$P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right)=2^{n/2}\omega^{a_{n-1}(\widehat{y})},$$

and for any $y\in\mathbb{F}_2^n$ such that $y_n=1$:

$$P_{n-1}(\widehat{y})\left(1+\omega^{\frac{q}{2}+\lambda_n}\right)=2^{n/2}\omega^{a_{n-1}(\widehat{y})+\lambda_n}.$$

So, for any $\widehat{y}\in\mathbb{F}_2^{n-1}$ consider the system

$$\begin{cases}P_{n-1}(\widehat{y})\left(1+\omega^{\lambda_n}\right)=2^{n/2}\omega^{a_{n-1}(\widehat{y})},\\ P_{n-1}(\widehat{y})\left(1-\omega^{\lambda_n}\right)=2^{n/2}\omega^{a_{n-1}(\widehat{y})+\lambda_n}.\end{cases}$$

It is equivalent to

$$\begin{cases} P_{n-1}\left(\widehat{y}\right)\left(1+\omega^{\lambda_n}\right) = 2^{n/2}\omega^{a_{n-1}(\widehat{y})}, \\ P_{n-1}\left(\widehat{y}\right)\left(1-\omega^{\lambda_n}\right) = P_{n-1}\left(\widehat{y}\right)\left(1+\omega^{\lambda_n}\right)\cdot\omega^{\lambda_n}. \end{cases}$$

From that system we obtain the relation

$$P_{n-1}\left(\widehat{y}\right)\left(1-\omega^{\lambda_n}\right) = P_{n-1}\left(\widehat{y}\right)\left(1+\omega^{\lambda_n}\right)\cdot\omega^{\lambda_n},$$

that is $1-\omega^{\lambda_n} = \omega^{\lambda_n} + \left(\omega^{\lambda_n}\right)^2$. The solutions of this equation are $\left(-1\pm\sqrt{2}\right)$. The norm of every of these numbers is not 1 therefore ω^{λ_n} can not be a solution. □

7 Symmetries

Denote, according to [6], the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{L \in GL\left(n, \mathbb{F}_2\right) | LL^T = I_n\right\},$$

where L^T denotes the transpose of L and I_n is an identical matrix of order n over the field $\mathbb{F}_2$.

In paper [5] (see also [3]) it was shown that the mapping

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x\rangle \oplus d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$, preserves self-duality of a bent function. The group which consists of mappings of such form is called an *extended orthogonal group* and denoted by $\overline{\mathcal{O}}_n$ [4, 5]. It is known that this group is a subgroup of $\mathrm{GL}\left(n+2, \mathbb{F}_2\right)$ [5].

In paper [12] known results were generalized within isometric mappings from the set of all mappings of all Boolean functions in $n \geqslant 4$ variables into itself, which preserve the Hamming distance. Namely it was proved the necessity of such a form of mappings for prserving of (anti-)self-duality.

In current work we consider the mappings of the set of all generalized Boolean functions in n variables to itself of the form

$$f(x) \longrightarrow f(\pi(x)) + g(x),$$

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{GF}_n$. It is clear that such mappings preserve both Hamming and Lee distances between generalized Boolean functions.

The following result provides the construction of mappings of such form that preserves (anti-)self-duality of a Boolean function.

Theorem 9. *The mapping of the set of all generalized Boolean functions in n variables to itself of the form*

$$f(x) \longrightarrow f(\pi(x)) + g(x),$$

with

$$\pi(x) = L\left(x \oplus c\right),$$

and

$$g(x) = \frac{q}{2}\langle c, x\rangle + d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ *is even,* $d \in \mathbb{F}_2$, *preserves (anti-)self-duality of a gbent function.*

Proof. Let $f \in \mathrm{SB}_q^+(n) \cup \mathrm{SB}_q^-(n)$ that is $\widetilde{f} = f + \frac{q}{2}\varepsilon$ for some $\varepsilon \in \mathbb{F}_2$. Consider a function $g(x) = f\left(L\left(x \oplus c\right)\right) + \frac{q}{2}\langle c, x\rangle + d$, where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{Z}_q$. Its generalized Walsh–Hadamard transform is

$$\begin{aligned}
\mathcal{H}_g(y) &= \sum_{x\in\mathbb{F}_2^n} \omega^{g(x)}(-1)^{\langle x,y\rangle} = \sum_{x\in\mathbb{F}_2^n} \omega^{f(L(x\oplus c))+\frac{q}{2}\langle c,x\rangle+d+\frac{q}{2}\langle x,y\rangle} \\
&= \omega^d \sum_{x\in\mathbb{F}_2^n} \omega^{\frac{q}{2}\langle x,y\oplus c\rangle+f(L(x\oplus c))} = \omega^d \sum_{z\in\mathbb{F}_2^n} \omega^{\frac{q}{2}\left\langle L^{-1}z\oplus c,y\oplus c\right\rangle+f(z)} \\
&= \omega^{d+\frac{q}{2}\langle c,y\rangle+\frac{q}{2}\langle c,c\rangle} \sum_{z\in\mathbb{F}_2^n} \omega^{\frac{q}{2}\langle z,L(y\oplus c)\rangle+f(z)} \\
&= \omega^{d+\frac{q}{2}\langle c,y\rangle} 2^{n/2} \omega^{\widetilde{f}(L(y\oplus c))} = 2^{n/2}\omega^{f(L(y\oplus c))+\frac{q}{2}\langle c,y\rangle+d+\frac{q}{2}\varepsilon} \\
&= 2^{n/2}\omega^{g(y)+\frac{q}{2}\varepsilon} = 2^{n/2}\omega^{\widetilde{g}(y)},
\end{aligned}$$

hence $\widetilde{g}(y) = g(y) + \frac{q}{2}\varepsilon$ for any $y \in \mathbb{F}_2^n$. □

Theorem 10. *The mapping of the set of all generalized Boolean functions in* n *variables to itself of the form*

$$f(x) \longrightarrow f(\pi(x)) + g(x),$$

with

$$\pi(x) = L\left(x \oplus c\right),$$

and

$$g(x) = \frac{q}{2}\langle c, x\rangle + d,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ *is odd,* $d \in \mathbb{F}_2$, *is a bijection between the sets* $\mathrm{SB}_q^+(n)$ *and* $\mathrm{SB}_q^-(n)$.

Corollary 11. *It holds* $\left|\mathrm{SB}_q^+(n)\right| = \left|\mathrm{SB}_q^-(n)\right|$.

References

[1] Canteaut A., Charpin P. Decomposing bent functions. *IEEE Trans. Inform. Theory*, **49**(8), 2004–2019 (2003).

[2] Carlet C. Boolean functions for cryptography and error correcting code. In: Crama Y., Hammer P.L. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. p. 257–397. Cambridge University Press, Cambridge (2010).

[3] Carlet C., Danielson L.E., Parker M.G., Solé. P. Self-dual bent functions. *Int. J. Inform. Coding Theory*, **1**, 384–399 (2010).

[4] Danielsen L.E., Parker M.G., Solé P. The Rayleigh quotient of bent functions. *Springer Lect. Notes in Comp. Sci.*, 5921, pp. 418–432. Springer, Berlin (2009).

[5] Feulner T., Sok L., Solé P., Wassermann A. Towards the Classification of Self-Dual Bent Functions in Eight Variables. *Des. Codes Cryptogr.*, **68**(1), 395–406 (2013).

[6] Janusz G.J. Parametrization of self-dual codes by orthogonal matrices. *Finite Fields Appl.*, **13**(3), 450–491 (2007).

[7] Hodžić S., Meidl W., Pasalic E. Full Characterization of Generalized Bent Functions as (Semi)-Bent Spaces, Their Dual, and the Gray Image. *IEEE Trans. Inform. Theory*, **64**(7), 5432–5440, 2018.

[8] Hodžić S., Pasalic E. Generalized Bent Functions — Some General Construction Methods and Related Necessary and Sufficient Conditions. *Cryptogr. Commun.*, **7**, 469–483, 2015.

[9] Hou X.-D. Classification of self dual quadratic bent functions. *Des. Codes Cryptogr.*, **63**(2), 183–198 (2012).

[10] Kutsenko A.V., *The Hamming Distance Spectrum Between Self-Dual Maiorana–McFarland Bent Functions*, Journal of Applied and Industrial Mathematics, **12**(1), 112–125 (2018).

[11] Kutsenko A. Metrical properties of self-dual bent functions. *Des. Codes Cryptogr.*, **88**, 201–222 (2020).

[12] Kutsenko A. The group of automorphisms of the set of self-dual bent functions. *Cryptogr. Commun.*, **12**(5), 881–898 (2017).

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

[14] Mesnager S., Tang C., Qi Y., Wang L., Wu B., Feng K. Further Results on Generalized Bent Functions and Their Complete Characterization. *IEEE Trans. Inform. Theory*, 64(7), 4668–4674, 2018.

[15] Mesnager S. Several New Infinite Families of Bent Functions and Their Duals. *IEEE Trans. Inf. Theory*, 60(7), 4397–4407, 2014.

[16] Paterson K.G. Generalized Reed–Muller Codes and Power Control in OFDM Modulation. *IEEE Trans. Inform. Theory*, **46**(1), 104–120, 2000.

[17] Preneel B., Van Leekwijck W., Van Linden L., Govaerts R., Vandewalle J. Propagation characteristics of Boolean functions. In: Advances in Cryptology-EUROCRYPT. Lecture Notes in Computer Science, **473**, pp. 161–173. Springer, Berlin (1990).

[18] Singh B.K. On cross-correlation spectrum of generalized bent functions in generalized Maiorana–McFarland class. *Information Sciences Letters*, **2**(3), 139–145 (2013).

[19] Paterson K.G., Jones A.E. Efficient decoding algorithms for generalized Reed–Muller codes. *IEEE Trans. Commun.*, **48**(8), 1272–1285, 2000.

[20] Rothaus O.S. On bent functions. *J. Combin. Theory. Ser. A*, **20**(3). 300–305 (1976).

[21] Schmidt K.-U. Quaternary constant-amplitude codes for multicode CDMA. *IEEE Trans. Inform. Theory*, **55**, 1824–1832 (2009).

[22] Schmidt K.-U. $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. *IEEE Trans. Inform. Theory*, **55**(10), 5803–5810 (2009).

[23] Sok L., Shi M., Solé P. Classification and Construction of quaternary self-dual bent functions. *Cryptogr. Commun.*, **10**(2), 277–289 (2018).

[24] Stănică P., Martinsen T., Gangopadhyay S., Singh B. K. Bent and generalized bent Boolean functions. *Des. Codes Cryptog.*, **69**, 77–94 (2013).

[25] Tang C., Xiang C., Qi Y., Feng K. Complete Characterization of Generalized Bent and 2^k-Bent Boolean Functions. *IEEE Trans. Inform. Theory*, **63**(7), 4668–4674, 2017.

[26] Tokareva N.N. Generalizations of bent functions — a survey. *J. Appl. Ind. Math.*, **5**(1), 110–129 (2011).

[27] Tokareva N.N. On the number of bent functions from iterative constructions: lower bounds. *Adv. Math. Commun.*, **5**(4), 609–621 (2011).

[28] Tokareva N. Bent Functions, Results and Applications to Cryptography. *Acad. Press. Elsevier*, 2015.

[29] Wada T. Characteristic bit sequences applicable to constant amplitude orthogonal multicode systems. *IEICE Trans. Fundamentals*, **E83-A**(11), 2160–2164, 2000.