On metrical properties of self-dual generalized bent functions

Kutsenko Aleksandr*

Sobolev Institute of Mathematics, Novosibirsk, Russia

Novosibirsk State University, Novosibirsk, Russia

Abstract

Bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$ (K.-U Schmidt, 2006) are known as generalized bent (gbent) functions. In this paper we study self-dual generalized bent functions and some their metrical properties for the Hamming and Lee distance. Necessary and sufficient conditions for self-duality of Maiorana–McFarland gbent functions are given. We find the complete Hamming and Lee distance spectrums between self-dual Maiorana–McFarland gbent functions and, as a corollary, we obtain minimal distances between considered self-dual gbent functions. We prove that the set of quaternary self-dual gbent functions is metrically regular for the Lee distance. The mapping of the set of all generalized Boolean functions in n variables to itself is called isometric if it preserves the distance between any pair of functions. We consider the mappings obtained by a generalization of isometric mappings of the set of all Boolean functions in n variables to itself. Within this generalization we propose an isometric mapping that preserves both Hamming and Lee distances and transforms the set of (anti-)self-dual gbent functions to itself.

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.

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 $\mathcal{GF}_n^q$, for the Boolean case ($q = 2$) we use the notation $\mathcal{F}_n$. Let $\omega = e^{2\pi i/q}$. A *sign* function of $f \in \mathcal{GF}_n^q$ is a complex valued function ω^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

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

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

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

*The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by Russian Foundation for Basic Research (project no. 18-07-01394, 20-31-70043) and Laboratory of Cryptography JetBrains Research.

for all $y \in \mathbb{F}_2^n$ [9]. If there exists such $\widetilde{f} \in \mathcal{GF}_n^q$ that $\mathcal{H}_f(y) = \omega^{\widetilde{f}(y)} 2^{n/2}$ 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 in 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.

A survey on different generalizations of bent functions can be found in [12].

Denote, according to [3], 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 $\mathbb{F}_2$.

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 [1] that a 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 [9]. In [11] 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 [2] necessary and sufficient conditions of (anti-)self-duality of Maiorana–McFarland bent functions, were given. In [10] 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 self-dual and anti-self-dual generalized Maiorana–McFarland bent functions by $\mathrm{SB}^+_{\mathcal{GM}^q}(n)$ ($\mathrm{SB}^-_{\mathcal{GM}^q}(n)$). For the Boolean case ($q = 2$) we will use the notation $\mathrm{SB}^+_{\mathcal{M}}(n)$ ($\mathrm{SB}^-_{\mathcal{M}}(n)$).

Theorem 0.1 *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 $y \in \mathbb{F}_2^{n/2}$

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

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

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

Corollary 0.2 *It holds*

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

In paper [4] the possible Hamming distances between (anti-)self-dual Maiorana–McFarland bent functions for the Boolean case were studied and the complete Hamming distances spectrum was presented, namely it was shown that for $f, g \in \mathrm{SB}^{+}_{\mathcal{M}}(n) \cup \mathrm{SB}^{-}_{\mathcal{M}}(n)$, then

$$\mathrm{dist}(f,g) \in \left\{2^{n-1}, 2^{n-1}\left(1 \pm \frac{1}{2^r}\right), r = 0, 1, ..., n/2-1\right\}.$$

Moreover, it was shown that if either $f, g \in \mathrm{SB}^{+}_{\mathcal{M}}(n)$ or $f, g \in \mathrm{SB}^{-}_{\mathcal{M}}(n)$, then all distances given above are attainable. If f is self-dual bent and g is anti-self-dual bent, then $\mathrm{dist}(f,g) = 2^{n-1}$.

In the current work we generalize this result for any even q in both Hamming and Lee distances. Denote the mentioned spectrum for the Hamming distance by $\mathrm{Sp}_H\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right)$, while for the Lee distance the notation $\mathrm{Sp}_L\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right)$ is used. The Hamming distance spectrum is described by the following

Theorem 0.3 *It holds*

$$\mathrm{Sp}_H\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right) = \left\{2^{n-1}\right\} \cup \bigcup_{r=0}^{n/2-1} \left\{2^{n-1}\left(1 \pm \frac{1}{2^r}\right)\right\}.$$

Moreover, all given distances are attainable.

The Lee distance spectrum is characterized by

Theorem 0.4 *It holds*

$$\mathrm{Sp}_L\left(\mathrm{SB}^{+}_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^{-}_{\mathcal{GM}^q}(n)\right) = \left\{q \cdot 2^{n-2}\right\} \cup \bigcup_{\mathrm{w}=0}^{q/2} \bigcup_{r=0}^{n/2-1} \left\{q \cdot 2^{n-2}\left(1 \pm \frac{1}{2^r}\right) \mp \mathrm{w} \cdot 2^{n-r}\right\}.$$

Moreover, all given distances are attainable.

It is possible to derive the minimal distances from these spectrums.

Proposition 0.5 *The minimal Lee distance between generalized (anti-)self-dual Maiorana–McFarland bent functions in n variables is equal to $2^{n-3}q$, while the minimal Hamming distance is 2^{n-2}.*

Recall that $\mathrm{RM}_q(r, m)$ is the length 2^m linear code over $\mathbb{Z}_q$ that is generated by the monomials of order at most r in variables $x_1, x_2, ..., x_m$, its minimal Lee distance is equal to 2^{m-r} [8]. Hence for $\mathrm{RM}_q(2, m)$ minimal Lee distance is equal to 2^{n-2}. From the obtained results it follows that

Corollary 0.6 *The minimal Lee distance 2^{n-2} between quadratic (generalized) bent functions is attainable on (anti-)self-dual Maiorana–McFarland bent functions from $\mathcal{GM}^q_n$ only for $q = 2$ while the minimal Hamming distance 2^{n-2} is attainable on such functions for any even $q \geqslant 2$.*

Let $X \subseteq \mathbb{Z}_q^n$ be an arbitrary set and let $y \in \mathbb{Z}_q^n$ be an arbitrary vector. Define the *distance* between y and X as $\mathrm{dist}(y, X) = \min\limits_{x \in X} \mathrm{dist}(y, x)$. The *maximal distance* from the set X is

$$\mathrm{d}(X) = \max_{y \in \mathbb{Z}_q^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{Z}_q^n$ is called *maximally distant* from the set X if $\mathrm{dist}(z, X) = \mathrm{d}(X)$. The set of all maximally distant vectors from the set X is called the *metrical complement* of the set X and denoted by $\widehat{X}$. A set X is said to be *metrically regular* if $\widehat{\widehat{X}} = X$. A subset of Boolean functions is said to be *metrically regular* if the set of corresponding vectors of values is metrically regular [13].

In paper [5] it was proved that the set of Boolean self-dual bent functions is metrically regular within the Hamming distance. In current work we prove that within Lee distance this statement holds for the quaternary case $q = 4$ as well.

Theorem 0.7 *The sets of (anti-)self-dual generalized quaternary bent functions are metrically regular for the Lee distance.*

A mapping φ of the set of all (generalized) Boolean functions in n variables to itself is called *isometric* if it preserves the distance between functions, that is,

$$\mathrm{dist}(\varphi(f), \varphi(g)) = \mathrm{dist}(f, g)$$

for any $f, g \in \mathcal{GF}_n$. From Markov's theorem (1956) [7] it follows that the general form of isometric mappings of the set of all Boolean functions in n variables to itself is

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

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$ [7]. In [6] all isometric mappings of the set of all Boolean functions in n variables to itself, that preserve (anti-)self-duality of a bent function were characterized.

In the current work we consider the mappings of the set of all generalized Boolean functions in n variables to itself, which have 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 isometric mappings that preserve both self-duality anti-self-duality of a gbent function.

Theorem 0.8 *The isometric 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

$$\pi(x) = L\left(x \oplus c\right), \quad g(x) = \frac{q}{2}\langle c, x\rangle + d,$$

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

References

[1] 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).

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

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

[4] 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).

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

[6] Kutsenko A., *The group of automorphisms of the set of self-dual bent functions*, Cryptogr. Commun. (2020). DOI: 10.1007/s12095-020-00438-y

[7] Markov A. A., *On transformations without error propagation.* In: Selected Works, Vol. II: Theory of Algorithms and Constructive Mathematics. Mathematical Logic. Informatics and Related Topics, p. 70–93, MTsNMO, Moscow (2003) [Russian].

[8] Paterson K.G., Jones A.E., *Efficient decoding algorithms for generalized Reed–Muller codes.* IEEE Trans. Commun., vol. 48, no. 8, pp. 1272–1285, 2000.

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

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

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

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

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