The Duality Mapping and Unitary Operators Acting on the Set of All Generalized Boolean Functions

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

CTCrypt 2021

Moscow region
June 1-4, 2021

Outline

Generalized Boolean functions

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 $\mathcal{F}_n$.
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 $x \in \mathbb{F}_2^n$.

Generalized Boolean functions

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 $\mathcal{F}_n$.
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 $x \in \mathbb{F}_2^n$.

Generalized bent functions

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

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

where $\omega = e^{2\pi i/q}$.

According to Schmidt (2009), a generalized Boolean function f in n variables is said to be *generalized bent* (gbent) if

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

for all $y \in \mathbb{F}_2^n$ [4].

Applications of generalized Boolean functions

- Generalized Reed–Muller codes has been suggested by Paterson (2000) for use in orthogonal frequency-division multiplexing (OFDM). These codes offer error correcting capability combined with substantially reduced peak-to-mean power ratios;
- Gangopadhyay S., Poonia V.S., Aggarwal D., Parekh R. Generalized Boolean Functions and Quantum Circuits on IBM-Q // Proceedings of 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (2019).

Generalizations of bent functions

Bent functions were generalized by P. V. Kumar et al. in 1985 by considering functions of the form $\mathbb{Z}_q^n \to \mathbb{Z}_q$ with corresponding definition of bentness. A.S. Ambrosimov in 1994 generalized the concept of a bent function for the case of an arbirary funite field. Bent functions from a finite Abelian group into a finite Abelian group were studied by V. I. Solodovnikov (2002) and by O.A. Logachev, A.A. Sal'nikov, V.V. Yashchenko (1997).

Generalizations of bent functions

Having applications of functions from $\mathbb{F}_2^n$ to $\mathbb{Z}_4$ in code-division multiple access (CDMA) systems, K.-U Schmidt in 2006–2009 generalized the notion of bentness for functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_q$, where $q \geqslant 2$ is a positive integer and studied these functions for the case $q = 4$.

A survey on different generalizations of bent functions can be found in «Tokareva N.N., Generalizations of bent functions – a survey // J. Appl. Ind. Math. **5**(1), 110–129 (2011)».

Generalized bent functions

In recent years generalized bent functions obtained much attention. Stănică et al. (2013) and Martinsen et al. (2017) obtained several constructions and properties of generalized bent functions. The question of the characterization of generalized bent functions was recently studied by Tang et al. (2017). Hodžić et al. (2018), Mesnager et al. (2018).

Duality mapping

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.

The *duality mapping* is a mapping that transforms every regular gbent function to its dual one. Thus, it is essentially defined only on regular gbent functions.

Duality mapping

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.

The *duality mapping* is a mapping that transforms every regular gbent function to its dual one. Thus, it is essentially defined only on regular gbent functions.

Martinsen, Meidl and Stănică in 2017 shown that every gbent function $\mathbb{F}_2^n \to \mathbb{Z}_{2^k}$ variables is regular, except the case $q = 4$ and n odd.

Self-dual gbent functions

A regular gbent function f in said to be *self-dual* if $f = \widetilde{f}$, and *anti-self-dual* if $f = \widetilde{f} + \frac{q}{2}$.

Further we will assume that q is even.

Known results

The extension of the concept of self-duality for different generalizations of bent functions was made in several papers.

- The classification of quadratic self-dual bent functions of the form $\mathbb{F}_p^n \to \mathbb{F}_p$, p odd prime, was made by X.-D. Hou (2013);
- The self-duality for bent functions within the same generalization type was studied by A. Çeşmelioğlu et al. (2013);
- L. Sok. et al. (2018) studied quaternary self-dual bent functions of the form $\mathbb{F}_2^n \to \mathbb{Z}_4$ from the viewpoints of existence, construction, and symmetry.

Direct sum

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

The function

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

where $x^{(k)} \in \mathbb{F}_2^{n_k}$ and $x = \left(x^{(1)}, x^{(2)}, \ldots, x^{(r)}\right) \in \mathbb{F}_2^n$, is a *direct sum* of generalized Boolean functions f_k.
Gbent functions obtained by a direct sum of generalized Boolean functions were studied by Hodžić et al. (2015), it was proved that function f is gbent if and only if all f_k are gbent functions.

Direct sum: self-dual case

Here we consider self-dual bent functions obtained by this construction.

Proposition

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

Maiorana–McFarland bent functions

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 that a dual of a Maiorana–McFarland bent function $f(x, y)$ is equal to

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

Maiorana–McFarland gbent functions

A generalization of this construction for the case $q = 4$ was given by Schmidt in 2009.

Stănică et al. (2013) generalized this construction for any even q:

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

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

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

Maiorana–McFarland gbent functions: notation

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 $\mathrm{SB}^{+}_{\mathcal{M}}(n)$ ($\mathrm{SB}^{-}_{\mathcal{M}}(n)$).

Maiorana–McFarland self-dual gbent functions: $q = 2$

In 2010 Carlet et al. found necessary and sufficient conditions of (anti-)self-duality of Maiorana–McFarland bent functions.

Denote, following Janusz (2009), the orthogonal group of index n over the field $\mathbb{F}_2$ as

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

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

Maiorana–McFarland self-dual gbent functions: $q = 2$

In 2010 Carlet et al. found necessary and sufficient conditions of (anti-)self-duality of Maiorana–McFarland bent functions.

It was proved that the function

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

is (anti-)self-dual gbent function if and only if

$$\pi(y) = L(y \oplus c), \quad g(y) = \langle c, y \rangle \oplus d,$$

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

Maiorana–McFarland self-dual gbent functions: $q = 4$

Sok et al. (2018) studied quaternary self-dual Maiorana–McFarland bent functions, necessary and sufficient conditions of self-duality were obtained for them. It was proved that the function

$$f(x, y) = 2\langle x, \pi(y)\rangle + g(y),$$

is quaternary (anti-)self-dual gbent function if and only if

$$\pi(y) = L(y \oplus c), \quad g(y) = 2\langle c, y\rangle + d,$$

where $L \in \mathcal{O}_{n/2}$, $c \in \mathbb{F}_2^{n/2}$, $\mathrm{wt}(c)$ is even (odd), $d \in \mathbb{Z}_4$.

Maiorana–McFarland self-dual gbent functions: even q

Theorem

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

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

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

Maiorana–McFarland self-dual gbent functions: even q

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

Corollary

It holds

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

where (MacWilliams, 1969)

$$|\mathcal{O}_k| = \begin{cases} 2^{\frac{k^2}{4}} \prod_{i=1}^{\frac{k}{2}-1} \left(2^{2i}-1\right), & k \text{ is even}, \\ 2^{\frac{(k-1)^2}{4}} \prod_{i=1}^{\frac{k-1}{2}} \left(2^{2i}-1\right), & k \text{ is odd}. \end{cases}$$

Iterative constructions: Boolean case

Let $f_0, f_1, f_2, f_3 \in \mathcal{F}_n$. Consider a Boolean function g in $n+2$ variables which is defined as

$$g(00, x) = f_0(x), \;\; g(01, x) = f_1(x), \;\; g(10, x) = f_2(x), \;\; g(11, x) = f_3(x),$$

It is known (Preneel et al., 1991; (see also A. Canteaut, P. Charpin, (2003); Tokareva, (2011)) 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

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

Iterative constructions of self-dual gbent functions

Further we obtain two iterative constructions of self-dual gbent functions that immediately come from their counterparts within the Boolean case.

Proposition

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;

Iterative constructions of self-dual gbent functions

Proposition (continuation)

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.

It follows that the number of iterative self-dual gbent functions is at least

$$|\mathcal{GB}_n^{q,\mathrm{reg}}| + \left|\mathrm{SB}_q^+(n)\right| \cdot \left|\mathrm{SB}_q^-(n)\right|,$$

where $\mathcal{GB}_n^{q,\mathrm{reg}}$ — the set of regular gbent functions in n variables.

Maiorana–McFarland self-dual gbent functions: spectrum of distances

Maiorana–McFarland self-dual gbent functions: spectrum of distances

Denote the spectrum for the attainable Hamming distances by

$$\mathrm{Sp}_H\left(\mathrm{SB}^+_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^-_{\mathcal{GM}^q}(n)\right),$$

while for the attainable Lee distances the notation

$$\mathrm{Sp}_L\left(\mathrm{SB}^+_{\mathcal{GM}^q}(n) \cup \mathrm{SB}^-_{\mathcal{GM}^q}(n)\right),$$

is used.

Maiorana–McFarland self-dual gbent functions: spectrum of Hamming distances

The Hamming distance spectrum is described by the following

Theorem

It holds

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

Moreover, all given distances are attainable.

Maiorana–McFarland self-dual gbent functions: spectrum of Lee distances

The Lee distance spectrum is characterized by

Theorem

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.

Maiorana–McFarland self-dual gbent functions: spectrum of Lee distances

Recall that $\mathrm{RM}_q(r, n)$ is the length 2^n linear code over $\mathbb{Z}_q$ that is generated by the monomials of order at most r in variables $x_1, x_2, \ldots, x_n$, its minimal Lee distance is equal to 2^{n-r} (Paterson et al., 2000). Hence for $\mathrm{RM}_q(2, n)$ minimal Lee distance is equal to 2^{n-2}.

From the obtained results it follows that

Corollary

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

Metrical regularity

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 $\mathrm{dist}(z, X) = \mathrm{d}(X)$.

Metrical regularity

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.

Metrical regularity

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.

It is known (AVK, 2020) that the set of Boolean self-dual bent functions is metrically regular within the Hamming distance.

Self-dual gbent functions: metrical regularity for $q = 4$

Proposition

The Lee distance between quaternary self-dual and anti-self-dual gbent functions is equal to 2^n.

Self-dual gbent functions: metrical regularity for $q = 4$

Proposition

The Lee distance between quaternary self-dual and anti-self-dual gbent functions is equal to 2^n.

Theorem

For the Lee distance the sets of (anti-)self-dual generalized quaternary bent functions are metrically regular sets with covering radius 2^n.

Self-dual gbent functions: metrical regularity for $q = 4$

The problem of determing the minimal Hamming or Lee distance can be studied within iterative scope.

Proposition

The minimal Hamming and Lee distances between quaternary self-dual and anti-self-dual gbent functions is equal to 2^n. For even q it holds

$$\min_{f,g \in \mathrm{SB}_q^+(n)} \mathrm{dist}(f,g) \leqslant 2 \cdot \left(\min_{f,g \in \mathrm{SB}_q^+(n-2)} \mathrm{dist}(f,g) \right).$$

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). Denote $\mathcal{H}_n = 2^{-n/2} H_n$.

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

A 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 $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$. A sign function of any anti-self-dual gbent function is an eigenvector of $\mathcal{H}_n$ attached to the eigenvalue (-1), that is an element from the subspace $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$.
It is known that

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

The subspaces $\mathrm{Ker}\,(\mathcal{H}_n + I_{2^n})$ and $\mathrm{Ker}\,(\mathcal{H}_n - I_{2^n})$ are mutually orthogonal.

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

For gbent functions we obtain the following

Proposition

Let $n \geqslant 4$ be an even number, then the linear span of sign functions of (anti-)self-dual gbent functions in n variables has dimension 2^{n-1} over $\mathbb{C}$.

Sign functions of (anti-)self-dual gbent functions: case $n = 2$

For $n = 2, q = 2$ we have sign functions $(1, 1, 1, -1)$ and $(-1, -1, -1, 1)$. These sign functions are linearly dependent vectors in $\mathbb{R}^4$. Sign functions for anti-self-dual case are linearly dependent vectors in $\mathbb{R}^4$ as well.

Generalization comprises a solution of the system

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

The form of the solution is

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

Subfunctions of self-dual gbent function

In 2018 Sok et al. suggested an algorithm for the generation of all self-dual gbent functions for the case $q = 4$. It is based on the

Theorem

Let $n \geqslant 4$ be an even number and $f \in \mathrm{SB}_q^+(n)$. For sign function $\omega^f = \left(F^{00}, F^{01}, F^{10}, F^{11}\right)$, where
$F^{00}, F^{01}, F^{10}, F^{11} \in \left\{1, \omega, \omega^2, \ldots, \omega^{q-1}\right\}^{2^{n-2}}$, *it holds*

$$\left\langle F^{00}, F^{01} \right\rangle + \left\langle F^{10}, F^{11} \right\rangle = 0,$$
$$\left\langle F^{00}, F^{10} \right\rangle + \left\langle F^{01}, F^{11} \right\rangle = 0.$$

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

$$h(z, y, x) = f(x) + (y \oplus z)g(x) + y \cdot z \cdot s(x), \quad y, z \in \mathbb{F}_2, x \in \mathbb{F}_2^n. \quad (1)$$

Stănică et al. (2013) proved that a function of such form is gbent if and only if the functions $f, f + g$ are gbent and $s(x) = q/2, x \in \mathbb{F}_2^n$.

In current work we study the conditions for self-duality of functions of such form.

Self-dual gbent functions symmetric with respect to two variables

In current work we study the conditions for self-duality of functions of such form.

Theorem

Let h be a gbent function of the form

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

Then h is self-dual if and only if f is gbent in n variables, $g = \widetilde{f} + (q-1)f$, and $s(x) = q/2$, $x \in \mathbb{F}_2^n$.

Affinity of gbent function

For the case when q is divisible by 4 it is known that there exist generalized Boolean functions of the form

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

where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$ (Singh, 2013). Functions from this class are referred to as *affine* functions.

Affinity of self-dual gbent function

In current work we study the question of the existence for self-dual case.

Theorem

There are no self-dual gbent functions in n variables of the form

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

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

Operator acting on the sign function

Let $\varphi : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ be linear operator with matrix A in standard basis of the space $\mathbb{C}^{2^n}$. We shall say that φ *transforms* the generalized Boolean function $f \in \mathcal{GF}_n^q$ with sign function F to the generalized Boolean function $f' \in \mathcal{GF}_n^q$ if the sign function F' of f' is equal to AF, that is $F' = AF = \varphi(F)$.

Unitary operators

Denote by $\mathcal{U}_n^q$ the set of unitary operators $\mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ which transform the set of generalized Boolean functions in n variables $\mathcal{GF}_n^q$ into itself.

Theorem

Operators from $\mathcal{U}_n^q$ are completely characterized by monomial matrices with nonzero elements from the set $\{1, \omega, \omega^2, \ldots, \omega^{q-1}\}$ and only them.

Relation to Boolean case

From Markov's theorem (1956) it follows that the general form of isometric mappings 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 $g \in \mathcal{F}_n$.
Then we can reformulate the previous result in terms of mappings of (generalized) Boolean functions:

Theorem

The action of any operator from $\mathcal{U}_n^q$ on the set $\mathcal{GF}_n^q$ is uniquely represented in the form

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

where π is a permutation on $\mathbb{F}_q^n$ and $g \in \mathcal{GF}_n^q$

Relation to Boolean case

So, for binary case we immediately obtain correspondence between $\mathcal{U}_n^2$ and $\mathcal{I}_n$:

Corollary

For $q = 2$ there is an one-to-one correspondence between the set $\mathcal{U}_n^q$ and the set of isometric mappings of all Boolean functions in n variables into itself ($\mathcal{I}_n$), defined by Markov's theorem.

Duality mapping

By using Sylvester Hadamard matrix it is possible to define the duality mapping as follows

$$\omega^f \longrightarrow \mathcal{H}_n \omega^f = \omega^{\widetilde{f}},$$

where f is a regular gbent function in n variables.

Unitary operators preserving eigenspaces of the duality mapping

Proposition

For an operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$ with a matrix U the following conditions are equivalent:

1) *$\varphi_{\pi,g}$ preserves self-duality;*
2) *$\varphi_{\pi,g}$ preserves anti-self-duality;*
3) *$U\mathcal{H}_n = \mathcal{H}_n U$.*

Unitary operators preserving eigenspaces of the duality mapping

Theorem

Operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$ preserves (anti-)self-duality of generalized bent function if and only if

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2}\langle c, x\rangle + d, \ x \in \mathbb{F}_2^n, \quad x \in \mathbb{F}_2^n,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}_H(c)$ is even, $d \in \mathbb{Z}_q$.

Known symmetries

Sok et al. (2018) proved that

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

with

$$\pi(x) = Lx, \quad g(x) = d,$$

where $L \in \mathcal{O}_n$, $d \in \mathbb{Z}_q$, preserves (anti-)self-duality of a quaternary gbent function.

Classification of quaternary self-dual bent functions in 4 variables

Representative from equivalence class	Size
0220202022000000	24
2022220222020200	64
0330313133110110	48
0330302132010110	120
1321213122010100	96
0220213023100000	48
Number of quaternary self-dual bent functions in four variables	400

Unitary operators which define bijections between the eigenspaces of the duality mapping

Proposition

An operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$ with matrix U defines a bijection between $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$ if and only if $U\mathcal{H}_n = -\mathcal{H}_n U$.

Unitary operators which define bijections between the eigenspaces of the duality mapping

Proposition

An operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$ with matrix U defines a bijection between $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$ if and only if $U\mathcal{H}_n = -\mathcal{H}_n U$.

Theorem

Operator $\varphi_{\pi,g} \in \mathcal{U}_n^q$ defines a bijections between $\mathrm{SB}_q^+(n)$ and $\mathrm{SB}_q^-(n)$ if and only if

$$\pi(x) = L(x \oplus c), \quad g(x) = \frac{q}{2}\langle c, x\rangle + d, \quad x \in \mathbb{F}_2^n,$$

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}_H(c)$ is odd, $d \in \mathbb{Z}_q$.

From the existence of such correspondence it follows that

Corollary

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

For Boolean case the mentioned fact was proved by Carlet et al. (2010).

The duality mapping and unitary operators

Theorem

If n is an even number, then in $\mathcal{U}_n^q$ there is no such operator whose fixed points include all self-dual gbent functions.

The duality mapping and unitary operators

Theorem

If n is an even number, then in $\mathcal{U}_n^q$ there is no such operator whose fixed points include all self-dual gbent functions.

Theorem

If n is an even number, then in $\mathcal{U}_n^q$ there is no such operator which assigns the dual bent function to every regular bent function from the set $\mathcal{GB}_n^q$.

Thanks for attention!