Metrical properties of the set of bent functions in view of duality

Aleksandr Kutsenko, Natalia Tokareva

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

CTCrypt 2020

Moscow region
September 15-17, 2020

Bent functions

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function in n variables.
The set of Boolean functions in n variables is denoted as $\mathcal{F}_n$.
A *Hamming distance* $\mathrm{dist}(f, g)$ between Boolean functions f, g in n variables is a cardinality of the set $\{x \in \mathbb{F}_2^n : f(x) \oplus g(x) = 1\}$.
The Walsh-Hadamard transform (WHT) of the Boolean function f in n variables is an integer function $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, defined as

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

A Boolean function f in n variables (n is even) is said to be bent if $|W_f(y)| = 2^{n/2}$ for any $y \in \mathbb{F}_2^n$ (Rothaus, 1976).

Applications of bent functions

Bent functions form a remarkable class of Boolean functions related to such combinatorial objects as Hadamard matrices (Rothaus, 1976), difference sets (Hou, 1998; Dillon, 1974), strongly regular graphs (Bernasconi et al., 2001), spreading sequences for CDMA and error correcting codes.

In symmetric cryptography, due to maximal nonlinearity, these functions can be used as building blocks of stream ciphers (Grain, 2004) and block ciphers (CAST, 1997) in order to make them more resilent to linear cryptanalysis (Matsui, 1994) and differential cryptanalysis (Biham, Shamir, 1991) .

Open problems

Some of open problems concerning bent functions are listed below:

- Number of bent functions (in $n \geqslant 10$ variables)?

Example of lower bound: $2^{(n/2)+\log(n-2)-1}$ (Maiorana–McFarland class);

Example of upper bound: $2^{2^{n-1}+\frac{1}{2}\binom{n}{n/2}}$ (Boolean functions in n variables with degree at most $n/2$);

- Affine classification of bent functions (in 10, 12, etc. variables)?

- New constructions of bent functions?

- Correlation between maximal nonlinearity and other important cryptoghraphic properties (s.t. the algebraic immunity, etc) of a Boolean function?

History of bent functions

The famous paper «On bent functions» was writen by O. S. Rothaus in 1966. It was declassified in 1976 (J. Combin. Theory. Ser. A, 1976, vol. 20, no. 3, pp. 300–305.).

History of bent functions

The famous paper «On bent functions» was writen by O. S. Rothaus in 1966. It was declassified in 1976 (J. Combin. Theory. Ser. A, 1976, vol. 20, no. 3, pp. 300–305.).

It is known that Yu. A. Vasiliev, B.M. Kloss, V.A. Eliseev, and O.P. Stepchenkov studied properties of the Walsh–Hadamard transform of a Boolean function in 1960s. V.A. Eliseev and O.P. Stepchenkov introduced the notation of *minimal function*, which is in fact a counterpart of a bent function.

An counterpart of the McFarland construction of bent functions was proposed by V.A. Eliseev in 1962.

History of bent functions

The famous paper «On bent functions» was writen by O. S. Rothaus in 1966. It was declassified in 1976 (J. Combin. Theory. Ser. A, 1976, vol. 20, no. 3, pp. 300–305.).

It is known that Yu. A. Vasiliev, B.M. Kloss, V.A. Eliseev, and O.P. Stepchenkov studied properties of the Walsh–Hadamard transform of a Boolean function in 1960s. V.A. Eliseev and O.P. Stepchenkov introduced the notation of *minimal function*, which is in fact a counterpart of a bent function.

An counterpart of the McFarland construction of bent functions was proposed by V.A. Eliseev in 1962.

In 1962, V.A. Eliseev and O.P. Stepchenkov proved that provided $n \geqslant 4$, the degree of a bent function is at most $n/2$.

History of bent functions

- Glukhov M.M. Planar mappings of finite fields and their generalizations. In: Presentation for the conference “Algebra and logic: theory and applications”, (Krasnoyarsk, Russia, July 21-27); 2013 [in Russian].
- Kuz'min A.S., Markov V.T., Nechaev A.A., Shishkin V.A., Shishkov A.B. Bent functions and hyper-bent functions over field with 2^l elements. Probl Inf Transm 2008; 44(1):12–33.
- Chapter 3 of the book «Bent Functions: Results and Applications to Cryptography» by Natalia Tokareva (Acad. Press, Elsevier, 2015. 230 p.).

Books and reviews

- **Tokareva N.** «Bent Functions, Results and Applications to Cryptography» 2015.
- **Mesnager S.** «Bent functions: Fundamentals and results» 2016.

Reviews:

- **Dillon J. F.** «A survey of bent functions» 1972 (The NSA Technical Journal).
- **Kuz'min A. S., Nechaev A. A., Shishkin V. A.** «Bent and hyper-bent functions over the finite field» 2007.
- **Carlet C., Mesnager S.** «Four decades of research on bent functions» 2016.
- **Çeşmelioğlu A., Meidl W., Pott A.** «A survey on bent functions and their duals» 2019.
- **Glukhov M. M.**, «On the approximation of discrete functions by linear functions» 2016.
- **Carlet C.** «Open Questions on Nonlinearity and on APN Functions» 2015.

Duality of a bent function

For every bent function its dual Boolean function is uniquely defined.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function in n variables.
A Boolean function $\widetilde{f}$ is said to be dual of f, if $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$ for any $y \in \mathbb{F}_2^n$.

Some properties of dual functions (see, Carlet, 2010):

- Every dual function is a bent function, moreover it holds $\widetilde{\widetilde{f}} = f$;
- The mapping $f \longrightarrow \widetilde{f}$ which acts on the set of bent functions, preserves the Hamming distance.

Self-dual bent functions

A bent function is said to be (anti-) self-dual bent, if $f = \widetilde{f}$ $\left(f = \widetilde{f} \oplus 1\right)$.

The set of (anti-)self-dual bent functions in n variables is denoted by $\mathrm{SB}^+(n)$ $\left(\mathrm{SB}^-(n)\right)$.

Self-dual bent functions

A bent function is said to be (anti-) self-dual bent, if $f = \widetilde{f}$ $\left(f = \widetilde{f} \oplus 1\right)$.

The set of (anti-)self-dual bent functions in n variables is denoted by $\mathrm{SB}^+(n)$ $\left(\mathrm{SB}^-(n)\right)$.

- Carlet C., Danielson L.E., Parker M.G., Solé P., Self-dual bent functions, Int. J. Inform. Coding Theory, **1**, 384–399 (2010);
- Hou X.-D., Classification of self dual quadratic bent functions, Des. Codes Cryptogr. **63**(2), 183–198 (2012);
- Hyun J.Y., Lee H., Lee Y., MacWilliams duality and Gleason-type theorem on self-dual bent functions, Des. Codes Cryptogr., **63**(3), 295–304 (2012);
- 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);
- Luo G., Cao X., Mesnager S. Several new classes of self-dual bent functions derived from involutions. Cryptogr. Commun. (2019).
- Logachev O. A., Sal'nikov A. A., Yashchenko V. V. Bent functions on a finite abelian group. Diskr. Mat. **9**(4), 3–20 (1997).

Open problems

- The number of self-dual bent functions;
- New constructions of self-dual bent functions;
- Metrical properties (e.g. spectrum of Hamming distances).

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

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

It is known (Preneel et al., 1991; see also Canteaut, Charpin (2003), Tokareva (2011)) that under condition $f_0, f_1, f_2, f_3 \in \mathcal{B}_n$ 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.

Iterative construction

We will refer to bent functions obtained by this construction as *bent iterative functions* ($\mathcal{BI}$) and denote the set of such bent functions in n variables by $\mathcal{BI}_n$.

Theorem (ref 2)

For any even $n \geqslant 2$

$$\frac{|\mathcal{B}_n|^4}{|X_n|} \leqslant |\mathcal{BI}_{n+2}| \leqslant |\mathcal{B}_{n+2}|,$$

where $X_n = \{f \oplus h : f, h \in \mathcal{B}_n\}$.

Iterative construction

Thus, for calculating the exact number of bent iterative functions, one has to study the structure of the set X_n. So, we come to a new problem statement.

Open problem: bent sum decomposition (Tokareva, 2011). What Boolean functions can be represented as the sum of two bent functions in n variables? How many such representations does a Boolean function admit?

Iterative construction: connection with dual function

Hypothesis (Tokareva, 2011). Any Boolean function in n variables of degree not more than $n/2$ can be represented as the sum of two bent functions in n variables, where $n \geqslant 2$ is an even number.

Theorem (ref 3)

A bent function in $n \geqslant 4$ variables can be represented as the sum of two bent functions in n variables if and only if its dual bent function does.

So, it follows that the mentioned Hypothesis with the decomposition problem can not be considered separately for a bent function and its dual.

Iterative construction

Thus, for calculating the exact number of bent iterative functions, one has to study the structure of the set X_n. So, we come to a new problem statement.

Open problem: bent sum decomposition (Tokareva, 2011). What Boolean functions can be represented as the sum of two bent functions in n variables? How many such representations does a Boolean function admit?

Iterative construction: self-duality

Theorem (ref 6)

Let $g \in \mathcal{BI}_{n+2}$. Then g is self-dual bent if and only if there exists such pair of functions $g_1, g_2 \in \mathcal{B}_n$:

$$f_0 = (g_1 \oplus g_2)\, h \oplus g_1 = \widetilde{g}_2,$$
$$f_1 = (g_1 \oplus g_2)\, h \oplus g_2 = \widetilde{g_1 \oplus h},$$
$$f_2 = (g_1 \oplus g_2)\, h \oplus g_2 \oplus h = \widetilde{g}_1,$$
$$f_3 = (g_1 \oplus g_2)\, h \oplus g_1 \oplus h \oplus 1 = \widetilde{g_2 \oplus h \oplus 1},$$

where

$$h = g_1 \oplus \widetilde{g}_1 \oplus g_2 \oplus \widetilde{g}_2.$$

Iterative construction: self-duality

Corollary

For any $f \in \mathcal{B}_n$ *and* $\varphi \in \mathrm{SB}^+(n)$, $\psi \in \mathrm{SB}^-(n)$, $\alpha \in \mathbb{F}_2$

$$f'(y_1, y_2, x) = (y_1 \oplus y_2)\left(f(x) \oplus \widetilde{f}(x)\right) \oplus f(x) \oplus y_1 y_2,$$

$$f''(y_1, y_2, x) = (y_1 \oplus y_2)(\varphi(x) \oplus \omega(x)) \oplus \varphi(x) \oplus (\alpha \oplus 1) y_1 \oplus \alpha y_2 \oplus y_1 y_2,$$

where

$$y_1, y_2, x \in \mathbb{F}_2^n,$$

are self-dual bent functions in $n + 2$ *variables.*

The first construction (for f') was earlier presented by Carlet et al. (2010) as an example of the construction which uses the indirect sum of bent functions.

Metrical regulaity: definitions

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and let $y \in \mathbb{F}_2^n$ 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

$$\mathrm{d}(X) = \max_{y \in \mathbb{F}_2^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{F}_2^n$ is called *maximally distant* from a 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 $\widehat{X}$ (Oblaukhov, 2016).

Metrical regulaity: definitions

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and let $y \in \mathbb{F}_2^n$ 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

$$\mathrm{d}(X) = \max_{y \in \mathbb{F}_2^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{F}_2^n$ is called *maximally distant* from a 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 $\widehat{X}$ (Oblaukhov, 2016).

A set X is said to be *metrically regular* if $\widehat{\widehat{X}} = X$ (N. T., 2012). A subset of Boolean functions to be *metrically regular* if the set of corresponding vectors of values is metrically regular.

Metrical regulaity: bent functions

Let $\mathrm{GA}(n)$ stands for the affine group. It is well-known that any mapping of the form

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

where $A \in \mathrm{GL}(n)$, $b, c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$, preserves bentness.

Metrical regulaity: bent functions

Let $\mathrm{GA}(n)$ stands for the affine group. It is well-known that any mapping of the form

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

where $A \in \mathrm{GL}(n)$, $b, c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$, preserves bentness.

Theorem (ref 1)

For each non-affine Boolean function $h \in \mathcal{F}_n$ there exists a bent function $f \in \mathcal{B}_n$ such that $f \oplus h$ is not bent.

Metrical regulaity: bent functions

Theorem (ref 3)

A Boolean function in n variables is

- *a bent function if and only if it has the maximal possible distance $2^{n-1} - 2^{n/2-1}$ to the set of all affine functions, that is it is an element of $\widehat{\mathcal{A}_n}$;*
- *an affine function if and only if it has the maximal possible distance $2^{n-1} - 2^{n/2-1}$ to the set of all bent functions, that is it is an element of $\widehat{\mathcal{B}_n}$.*

Metrical regulaity: bent functions

Thus, it follows that there exists a «*duality*», in some sense, between the definitions of bent functions and affine functions.

Corollary

1) *The set $\mathcal{A}_n$ of all affine Boolean functions in n variables is metrically regular.*
2) *The set $\mathcal{B}_n$ of all bent functions in n variables is metrically regular.*

Metrical regulaity: self-dual bent functions

From the results of (Carlet et al., 2010) it folows that

$$\mathrm{d}\left(\mathrm{SB}^{+}(n)\right) = 2^{n-1},$$

since

$$\mathrm{SB}^{-}(n) \subseteq \widehat{\mathrm{SB}^{+}(n)}.$$

Metrical regulaity: self-dual bent functions

From the results of (Carlet et al., 2010) it folows that

$$\mathrm{d}\left(\mathrm{SB}^{+}(n)\right) = 2^{n-1},$$

since

$$\mathrm{SB}^{-}(n) \subseteq \widehat{\mathrm{SB}^{+}(n)}.$$

In [] we have proved that

$$\widehat{\mathrm{SB}^{+}(n)} \subseteq \mathrm{SB}^{-}(n).$$

Metrical regulaity: self-dual bent functions

Theorem (ref 6)

Let $n \geqslant 4$, then a Boolean function in n variables is:

- *self-dual bent if and only if it has the maximal possible distance 2^{n-1} to the set of all anti-self-dual bent functions, that is, it is an element of $\widehat{\mathrm{SB}^-(n)}$;*
- *anti-self-dual bent if and only if it has the maximal possible distance 2^{n-1} to the set of all self-dual bent functions, that is, it is an element of $\widehat{\mathrm{SB}^+(n)}$.*

Again, we can say that there exists a metrical «*duality*», in some sense, between the self-dual and anti-self-dual bent functions.

The group of automorphisms: definitions

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and let $y \in \mathbb{F}_2^n$ 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

$$\mathrm{d}(X) = \max_{y \in \mathbb{F}_2^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{F}_2^n$ is called *maximally distant* from a 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 $\widehat{X}$ (Oblaukhov, 2016).

The group of automorphisms: definitions

Let $X \subseteq \mathbb{F}_2^n$ be an arbitrary set and let $y \in \mathbb{F}_2^n$ 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

$$\mathrm{d}(X) = \max_{y \in \mathbb{F}_2^n} \mathrm{dist}(y, X).$$

In coding theory this number is also known as the *covering radius* of the set X. A vector $z \in \mathbb{F}_2^n$ is called *maximally distant* from a 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 $\widehat{X}$ (Oblaukhov, 2016).

A set X is said to be *metrically regular* if $\widehat{\widehat{X}} = X$ (N. T., 2012). A subset of Boolean functions to be *metrically regular* if the set of corresponding vectors of values is metrically regular.

The group of automorphisms: definitions

A mapping φ of the set of all Boolean functions in n variables to itself is called *isometric* if it preserves the Hamming distance between functions. Denote the set of all isometric mappings of the set of all Boolean functions in n variables to itself by $\mathcal{I}_n$.

The group of automorphisms: definitions

A mapping φ of the set of all Boolean functions in n variables to itself is called *isometric* if it preserves the Hamming distance between functions. Denote the set of all isometric mappings of the set of all Boolean functions in n variables to itself by $\mathcal{I}_n$.

It is known (A. A. Markov, 1956) that every isometric mapping of all Boolean functions in n variables to itself has the unique representation of the form

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

where π is a permutation on the set $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$. The mapping of this form is denoted by $\varphi_{\pi,g} \in \mathcal{I}_n$.

The group of automorphisms: definitions

A mapping φ of the set of all Boolean functions in n variables to itself is called *isometric* if it preserves the Hamming distance between functions. Denote the set of all isometric mappings of the set of all Boolean functions in n variables to itself by $\mathcal{I}_n$.

The *group of automorphisms* of a fixed subset $M \subseteq \mathcal{F}_n$ is the group of isometric mappings of the set of all Boolean functions in n variables to itself preserving the set M. It is denoted by $\mathrm{Aut}\,(M)$.

The group of automorphisms: the set of bent functions

Some attempts to determine the automorphism group of a given bent function were undertaken by U. Dempwolff in 2006. Results were presented in terms of elementary Abelian Hadamard difference sets (equivalently, bent functions).

It is clear that the mapping of the form

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

where $A \in \mathrm{GL}(n)$, $b, c \in \mathbb{F}_2^n$, $d \in \mathbb{F}_2$, is isometric.

The group of automorphisms: the set of bent functions

«Duality» between bent functions and affine functions implies

Proposition (ref 1)

$\mathrm{Aut}\,(\mathcal{B}_n) = \mathrm{Aut}\,(\mathcal{A}_n)$.

The group of automorphisms of the set of all affine functions in n variables consists, of mappings $\varphi_{\pi,g}$ with affine permutation π and affine shift g.

The group of automorphisms: the set of bent functions

Note that the set of all affine functions in n variables forms a group isomorphic to $\mathbb{F}_2^{n+1}$. Let the symbol $\ltimes$ stands for the semidirect product, then the result is formulated as follows.

Theorem (ref 1)

$$\mathrm{Aut}\,(\mathcal{B}_n) = \mathrm{GA}(n) \ltimes \mathbb{F}_2^{n+1}.$$

It follows the non-existence of a more general approach to equivalence of bent functions, than based on affine transform of coorddinates and an affine shift.

The group of automorphisms: the set of self-dual bent functions

Denote, following (Janusz, 2007), the orthogonal group of index n over the field $\mathbb{F}_2$ as

$$\mathcal{O}_n = \left\{ L \in GL(n,2) | LL^T = I_n \right\},$$

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

The group of automorphisms: the set of self-dual bent functions

It was shown by Carlet et al. (2010) that the mapping

$$f(x) \longrightarrow f\left(Lx\right) \oplus d,$$

where $L \in \mathcal{O}_n$, $d \in \mathbb{F}_2$, preserves self-duality of a bent function.

Feulner et al. (2013) generalized the previous result: it was proved 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.

It is obvious that this mapping is an element from $\mathcal{I}_n$.

The group of automorphisms: the set of self-dual bent functions

Consider mappings of the form

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

where $L \in \mathcal{O}_n$, $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is even, $d \in \mathbb{F}_2$. The group which consists of mappings of such form is called an *extended orthogonal group*

The group of automorphisms: the set of self-dual bent functions

Theorem (ref 7)

If $n \geqslant 4$, then isometric mapping $\varphi_{\pi,g}$ belongs to $\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right)$ if and only if, for any $x, y \in \mathbb{F}_2^n$, it holds

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

Theorem (7)

For $n \geqslant 4$ it holds

$$\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right) = \mathrm{Aut}\left(\mathrm{SB}^{-}(n)\right) = \overline{\mathcal{O}}_n.$$

Bijections between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$

Carlet et al. (2010) described a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$, based on the decomposition of sign functions of (anti-)self-dual bent function. In terms of isometric mappings this transform can be represented as

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

where $c = (1, 0, 0, ..., 0) \in \mathbb{F}_2^n$.
In the paper of Hou (2012) it was mentioned that the more general form of this mapping

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

where $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ is odd, is a bijection between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$.
It is obvious that this mapping is an element from $\mathcal{I}_n$.

Isometric bijections between self-dual and anti-self-dual bent functions

Theorem (ref 6)

An isometric mapping $f(x) \longrightarrow f(\pi(x)) \oplus g(x)$ *of the set of all Boolean functions in* $n \geqslant 4$ *variables into itself is a bijection between* $\mathrm{SB}^+(n)$ *and* $\mathrm{SB}^-(n)$ *if and only if*

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

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

Isometric mappings and duality mapping

Theorem (ref 4)

The mapping that assigns to every bent function in n variables its dual function cannot be extended to the isometric mapping of all Boolean functions in n variables into itself.

Isometric mappings and duality mapping

According to Carlet et al., (2010) the *Rayleigh quotient* S_f of a Boolean function $f \in \mathcal{F}_n$ is the number

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

The Rayleigh quotient characterizes the Hamming distance between a bent function and its dual. Let $f \in \mathcal{B}_n$, then

$$\mathrm{dist}(f, \widetilde{f}) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f.$$

Danielson et al. (2009) studied the operations on Boolean functions that preserve bentness and the Rayleigh quotient.

Isometric mappings and duality mapping

$$\mathrm{dist}(f, \widetilde{f}) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f.$$

Thus, the general form of isometric mappings, which preserve the Hamming distance between every bent function and its dual, is described by $\mathrm{Aut}\left(\mathrm{SB}^+(n)\right)$ that is by the extended orthogonal group $\overline{\mathcal{O}}_n$.

Isometric mappings and duality mapping

Assume $f, g \in \mathcal{B}_n$ and $\varphi(f) = g$

$$\begin{array}{ccc} f & \xrightarrow{\text{dual}} & \widetilde{f} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle ?} \\ g & \xrightarrow{\text{dual}} & \widetilde{g} \end{array}$$

Isometric mappings and duality mapping

Assume $f, g \in \mathcal{B}_n$ and $\varphi(f) = g$

$$\begin{array}{ccc} f & \xrightarrow{\text{dual}} & \widetilde{f} \\ \varphi \downarrow & & \downarrow \varphi \\ g & \xrightarrow{\text{dual}} & \widetilde{g} \end{array}$$

Isometric mappings and duality mapping

Assume $f, g \in \mathcal{B}_n$ and $\varphi(f) = g$

$$\begin{array}{ccc} f & \xrightarrow{\text{dual}} & \widetilde{f} \\ \varphi \downarrow & & \downarrow \varphi \\ g & \xrightarrow{\text{dual}} & \widetilde{g} \end{array}$$

The general form of isometric mappings, which possess the property

$$(\varphi(f) = g) \Longrightarrow (\widetilde{\varphi(f)} = \widetilde{g})$$

is again described by $\mathrm{Aut}\left(\mathrm{SB}^{+}(n)\right)$ that is by the extended orthogonal group $\overline{\mathcal{O}}_n$.

[1] Tokareva N. N., The group of automorphisms of the set of bent functions. Discrete Mathematics and Applications, 2010, vol. 20, no. 5, pp. 655–664.

[2] Tokareva N. N. On the number of bent functions from iterative constructions: lower bounds. Adv. Math. Commun., 2011, vol. 5, no. 4, pp. 609–621.

[3] Tokareva N. Duality between bent functions and affine functions. Discrete Mathematics, 2012, vol. 312, no. 3, pp. 666–670.

[4] Tokareva N. N. On decomposition of a dual bent function into sum of two bent functions. Prikladnaya Diskretnaya Matematika, 2014, no. 4(26), pp. 59–61. (in Russian)

[5] Kutsenko A. V. On some properties of known isometric mappings of the set of bent functions. Prikladnaya Diskretnaya Matematika. Supplementary, 2017, no. 10, pp. 43–44. (in Russian)

[6] Kutsenko A. Metrical properties of self-dual bent functions. Designs, Codes and Cryptography, 2020, vol. 88, no. 1, pp. 201–222.

[7] Kutsenko A. The group of automorphisms of the set of self-dual bent functions. Cryptography and Communications, 2020, vol. 12, no. 5, pp. 881–898.

Thanks for attention!