Isometric mappings of the set of all Boolean functions into itself which preserve self-duality and the Rayleigh quotient

Kutsenko Aleksandr

Novosibirsk State University
Novosibirsk, Russia

Florence, Italy
June 16-21, 2019

Bent functions

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

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

A Boolean function f in n variables (n is even) is said to be bent [1] if $|W_f(y)| = 2^{n/2}$ for any $y \in \mathbb{F}_2^n$.

[1] Rothaus O. // J. Combin. Theory. Ser. A. 1976.

Applications of bent functions

Bent functions form a remarkable class of Boolean functions with applications in many domains, such as difference sets, spreading sequences for CDMA, error correcting codes and cryptology.

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 [2] and differential [3] cryptanalysis.

[2] Matsui M. // Advances in Cryptology - EUROCRYPT'93. Proc. Berlin: Springer, 1994.

[3] Biham E., Shamir A. // J. Cryptology. 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 cryptographic properties (s.t. the algebraic immunity, etc) of a Boolean function?

Dual 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 $\tilde{f}$ is said to be dual of f, if $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ for any $x \in \mathbb{F}_2^n$.

Some properties of dual functions:

• Every dual function is a bent function, moreover it holds $\tilde{\tilde{f}} = f$ [4];

• The mapping $f \longrightarrow \tilde{f}$ which acts on the set of bent functions, preserves Hamming distance [5].

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

[5] Carlet C. Boolean functions for cryptography and error-correcting codes // Boolean models and methods in mathematics, computer science, and engineering. New York: Cambridge Univ. Press, 2010. P. 257-397.

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

- 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);
- Sok L., Shi M., Solé. P., Classification and Construction of quaternary self-dual bent functions, Cryptogr. Commun., **10**(2), 277–289 (2017);
- Luo G., Cao X., Mesnager S. Several new classes of self-dual bent functions derived from involutions. Cryptogr. Commun. (2019).

Open problems

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

Known metrical properties of self-dual bent functions

- For any pair of functions $f \in \mathrm{SB}^+(n)$ and $g \in \mathrm{SB}^-(n)$ it holds (Carlet et al., 2010)

$$\mathrm{dist}(f, g) = 2^{n-1};$$

- The complete Hamming distance spectrum between self-dual Maiorana–McFarland bent functions (A. V. K., 2018);
- For $n \geqslant 4$ it holds (A. V. K., 2018)

$$\min_{f,g \in \mathrm{SB}^+(n), f \neq g} \mathrm{dist}(f, g) = 2^{n/2};$$

Known metrical properties of self-dual bent functions

- Let $n \geqslant 4$, then the following statements hold:
  - The metrical complement of the set $\mathrm{SB}^{+}(n)$ coincides with $\mathrm{SB}^{-}(n)$;
  - The metrical complement of the set $\mathrm{SB}^{-}(n)$ coincides with $\mathrm{SB}^{+}(n)$ (A. V. K., 2018);
- The the sets $\mathrm{SB}^{+}(n)$ and $\mathrm{SB}^{-}(n)$ are metrically regular sets both with covering radius 2^{n-1} (A. V. K., 2018).

Isometry of the set of all Boolean functions

A mapping φ of the set of all Boolean functions in n variables into itself is *isometric* if it preserves Hamming distances between functions, i.e.

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

It is known (A. A. Markov, 1956) that every such mapping has an unique representation of the form

$$f(x) \longrightarrow f(s(x)) \oplus h(x),$$

where $s : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ is a permutation and h is a Boolean function in n variables.

The set of all isometric mappings of the set of all Boolean functions in n variables into itself is denoted by $\mathcal{I}_n$.

Isometries of bent functions

Every isometric mapping of the set of all Boolean functions in n variables into itself that transforms bent functions into bent functions is a combination of an affine transform of coordinates and an affine shift — i.e, it has the form

$$f(x) \longrightarrow f(Ax \oplus b) \oplus a(x),$$

where A — a nondegenerate $n \times n$ matrix over the field $\mathbb{F}_2$, b — a binary vector of length n, $a(x)$ — an affine function in n variables.

[6] Tokareva N. N. The group of automorphisms of the set of bent functions // Discrete Mathematics and Applications. 2010. V. 20. Nv5-6. P. 655-664.

Isometries of bent functions

Every isometric mapping of the set of all Boolean functions in n variables into itself that transforms bent functions into bent functions is a combination of an affine transform of coordinates and an affine shift — i.e, it has the form

$$f(x) \longrightarrow f(Ax \oplus b) \oplus a(x),$$

where A — a nondegenerate $n \times n$ matrix over the field $\mathbb{F}_2$, b — a binary vector of length n, $a(x)$ — an affine function in n variables.

It is known (A. V. K., 2017) that there is no such isometric mapping of all Boolean functions in n variables into itself which assigns to every bent function its dual function.

Known symmetries which preserve self-duality

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 $\mathbb{F}_2$.

Known symmetries which preserve self-duality

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 $\mathcal{I}_n$.

Characterization of isometric mappings from $\mathcal{I}_n$ which preserve self-duality

Proposition

Let $n \geqslant 4$. Isometric mapping $\varphi \in \mathcal{I}_n$ preserves self-duality if and only if it preserves anti-self-duality.

Characterization of isometric mappings from $\mathcal{I}_n$ which preserve self-duality

Theorem

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 preserves (anti-)self-duality if and only if*

$$\pi(x) = L(x \oplus c)$$

and

$$g(x) = \langle c, x \rangle \oplus d,$$

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

Known symmetries which are 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

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

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

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

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 $\mathcal{I}_n$.

Characterization of isometric mappings from $\mathcal{I}_n$ which are bijections between $\mathrm{SB}^+(n)$ and $\mathrm{SB}^-(n)$

Theorem

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

$$\pi(x) = L(x \oplus c)$$

and

$$g(x) = \langle c, x\rangle \oplus d,$$

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

The Rayleigh quotient

For a complex Hermitian $n \times n$ matrix M and nonzero vector $x \in \mathbb{C}^n$ the Rayleigh quotient (Rayleigh ratio) is a number

$$R(M, x) = \frac{x^\dagger M x}{x^\dagger x}.$$

It is known that

$$\min_{x \in \mathbb{C}^n, x \neq \mathbf{0}} R(M, x) = \lambda_{\min}(M),$$

$$\max_{x \in \mathbb{C}^n, x \neq \mathbf{0}} R(M, x) = \lambda_{\max}(M).$$

The maximization of the Rayleigh quotient appears in many problems in engineering and pattern recognition.

The Rayleigh quotient of a Boolean function

In [4] the Rayleigh quotient S_f of a Boolean function $f \in \mathcal{F}_n$ was defined as

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

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

The Rayleigh quotient of a Boolean function

In [4] the Rayleigh quotient S_f of a Boolean function $f \in \mathcal{F}_n$ was defined as

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

For any $f \in \mathcal{B}_n$ the normalized Rayleigh quotient N_f is a number

$$N_f = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \widetilde{f}(x)} = 2^{-n/2} S_f .$$

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

The Rayleigh quotient of a Boolean function

In [4] the Rayleigh quotient S_f of a Boolean function $f \in \mathcal{F}_n$ was defined as

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

It is known [4] (Theorem 3.1) that for any $f \in \mathcal{F}_n$ the absolute value of S_f is at most $2^{3n/2}$ with equality if and only if f is self-dual $\left(+2^{3n/2}\right)$ or anti-self-dual $\left(-2^{3n/2}\right)$ bent function.

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

Known symmetries which preserve the Rayleigh quotient of a Boolean function

In the article [7] examples of operations on Boolean functions that preserve bentness and the Rayleigh quotient were given.

Namely, it was proven that for any $f \in \mathcal{B}_n, L \in \mathcal{O}_n, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$ the functions $g, h \in \mathcal{B}_n$ defined as

$$g(x) = f(Lx) \oplus d, \qquad h(x) = f(x \oplus c) \oplus \langle c, x \rangle,$$

provide $S_g = S_f$ and $S_h = (-1)^{\langle c,c \rangle} S_f$.

The mentioned operations are isometric mappings from $\mathcal{I}_n$.

[7] Danielsen L. E., Parker M. G., Solé P. (2009) The Rayleigh Quotient of Bent Functions. In: Parker M. G. (eds) Cryptography and Coding. IMACC 2009. Lecture Notes in Computer Science, vol 5921. Springer, Berlin, Heidelberg.

Isometric mappings

Theorem

An isometric mapping of the set of all Boolean functions in $n \geqslant 4$ variables into itself preserves the Rayleigh quotient if and only if it preserves self-duality.

Theorem

An isometric mapping of the set of all Boolean functions in $n \geqslant 4$ variables into itself changes the sign of the Rayleigh quotient if and only if it is a bijection between $\mathrm{SB}^{+}(n)$ and $\mathrm{SB}^{-}(n)$.

Preserving the Hamming distance between every bent function and its dual

Corollary

Any isometric mapping of the set of all Boolean functions in $n \geqslant 4$ variables into itself which preserves the Rayleigh quotient or changes the sign of the Rayleigh quotient also preserves bentness.

Preserving the Hamming distance between every bent function and its dual

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

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

Thus, from previous results it follows that the isometric mapping preserves bentness and the Hamming distance between every bent function in $n \geqslant 4$ variables and its dual if and only if it preserves self-duality.

Summary of results

Let φ be an isometric mapping of the set of all Boolean functions in $n \geqslant 4$ variables into itself with matrix A, namely

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

where π is a permutation in $\mathbb{F}_2^n$ and $g \in \mathcal{F}_n$.

Summary of results

Theorem

The following conditions are equivalent:

- φ *preserves self-duality;*
- φ *preserves anti-self-duality;*
- φ *preserves the Rayleigh quotient;*
- φ *preserves bentness and the Hamming distance between any bent function and its dual;*
- $\pi(x) = L\,(x \oplus c)$ *and* $g(x) = \langle c, x\rangle \oplus d$*, where* $L \in \mathcal{O}_n$*,* $c \in \mathbb{F}_2^n$*,* $\mathrm{wt}(c)$ *is even,* $d \in \mathbb{F}_2$*.*

Summary of results

Theorem

The following conditions are equivalent:

- φ *is a bijection between* $\mathrm{SB}^+(n)$ *and* $\mathrm{SB}^-(n)$*;*
- φ *changes sign of the Rayleigh quotient;*
- $\pi(x) = L(x \oplus c)$ *and* $g(x) = \langle c, x \rangle \oplus d$*, where* $L \in \mathcal{O}_n$*,* $c \in \mathbb{F}_2^n$*,* $\mathrm{wt}(c)$ *is odd,* $d \in \mathbb{F}_2$*.*

It follows that the way of classifying self-dual bent functions proposed by Carlet et al. (2010) and Feulner et al. (2013) is the most general within isometric mappings.

International Students' Olympiad in Cryptography NSUCRYPTO

NSUCRYPTO-2019 will be held from October 13 to October 21, 2019.

Thanks for attention!