Properties of generalized bent functions and Gram matrices of Boolean bent functions

Aleksandr Kutsenko

Sobolev Institute of Mathematics SB RAS,
Novosibirsk State University

The 12th Workshop on
Current Trends in Cryptology (CTCrypt 2023)
Volgograd, June 6–9, 2023

Bent functions

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).

Bent functions

- maximal distance to affine functions — maximal nonlinearity (cryptography, coding theory);
- Walsh spectrum is flat (signal processing theory, spreading sequences for CDMA).

Tokareva N. Bent Functions: Results and Applications to Cryptography, 2015, 220 p.

Dual bent function

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

The condition $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ for any $x \in \mathbb{F}_2^n$ gives the Boolean function $\tilde{f}$ that is said to be dual of f
(O.S. Rothaus, J.F. Dillon, 70s).

Some properties of dual functions:

- Every dual function is a bent function, moreover it holds $\tilde{\tilde{f}} = f$;
- The mapping $f \to \tilde{f}$ which acts on the set of bent functions, preserves Hamming distance (Carlet, 1994).

Sylvester–Hadamard matrix

$$H_0 = (1), \quad H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}, \ n \geqslant 2.$$

This matrix is known as Sylvester–Hadamard matrix. It is known the Hadamard property of this matrix $H_n H_n^{\mathrm{T}} = 2^n I_{2^n}$.

It defines the duality mapping in matrix form:

$$(-1)^f \longrightarrow (-1)^{\widetilde{f}} = \frac{1}{2^{n/2}} H_n (-1)^f.$$

Self-dual bent functions

A bent function is said to be self-dual, if $f = \widetilde{f}$.

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

Self-dual bent functions are fixed points of the duality mapping.

Their characteristic (sign) vectors are eigenvectors of the Sylvester–Hadamard matrix.

(Yarlagadda, Hershey, A note on the eigenvectors of Hadamard matrices of order 2^n // Linear Algebra & Appl., 1982)

Self-dual bent functions: history

- B. Preneel et al. (Propagation characteristics of Boolean functions // EUROCRYPT'90) introduced **dual** and **anti-dual** bent functions;

Self-dual bent functions: history

- B. Preneel et al. (Propagation characteristics of Boolean functions // EUROCRYPT'90) introduced **dual** and **anti-dual** bent functions;
- Logachev, Sal'nikov, Yashchenko considered more general definition of **self-dual bent functions on a finite group** (Bent functions on a finite abelian group // Discrete Math. Appl., 1997);

Self-dual bent functions: current state

- Carlet, Solé, Parker, Danielsen, «Self-dual bent functions» (2010);

Self-dual bent functions: current state

- Carlet, Solé, Parker, Danielsen, «Self-dual bent functions» (2010);
- Hou «Classification of self dual quadratic bent functions» (2012);
- Hyun, Lee, Lee «MacWilliams duality and Gleason-type theorem on self-dual bent functions» (2012);
- Feulner, Solé, Sok, Wassermann «Towards the classification of self-dual bent functions in eight variables» (2013);
- Mesnager «Several new infinite families of bent functions and their duals» (2014);
- Luo, Cao, Mesnager «Several new classes of self-dual bent functions derived from involutions» (2019);
- Li, Kan, Mesnager, Peng, Tan, Zheng «Generic constructions of (Boolean and vectorial) bent functions and their consequence» (2022);
- Su, Guo «A further study on the construction methods of bent functions and self-dual bent functions based on Rothaus's bent function» (2023).

Outline

Let f be a vector of values of a Boolean function f in n variables

$$\mathrm{f} = \left(f_0, f_1, \ldots, f_{2^k-1}\right)$$

where f_i are vectors of values of Boolean functions in $n-k$ variables. In fact, f_i are subfunctions. We consider the case $k=2$.

Motivation (for self-dual):

- best known lower and upper bounds were obtained upon characteristic vectors analysis;
- known metrical properties are based on the characteristic vectors properties.

Start point

Let f be a vector of values of a self-dual bent function f in n variables

$$\mathrm{f} = (f_0, f_1, f_2, f_3)\,,$$

where f_i are vectors of values of Boolean functions in $n-2$ variables.

Such subfunctions of a bent function in n variables have the same extended Fourier spectrum (Canteaut et al., 2003):

- all of them are bent;
- near-bent functions with the spectrum having three values 0, $\pm 2^{n/2}$;
- they have the same extended Fourier spectrum with five values 0, $\pm 2^{(n-2)/2}$, $\pm 2^{n/2}$.

Concatenation of four bent functions

Preneel et al. in 1990 proved that given four bent functions f_i in n variables, the concatenation of vectors of values of f_i yields a bent function in $n+2$ variables if and only if

$$W_{f_0}(y)W_{f_1}(y)W_{f_2}(y)W_{f_3}(y) = -2^{2n} \text{ for any } y \in \mathbb{F}_2^n.$$

In terms of duals this condition is equivalent to the following

$$\widetilde{f_0}(y) \oplus \widetilde{f_1}(y) \oplus \widetilde{f_2}(y) \oplus \widetilde{f_3}(y) = 1 \text{ for any } y \in \mathbb{F}_2^n.$$

The class is known as *bent iterative* ($\mathcal{BI}$) functions (Tokareva, 2011). The self-duality of functions from this construction was studied in (A.K., 2020).

Concatenation of four bent functions

The idea of concatenation also appeares in a scope of so called **bent based** bent sequences (Adams, Tavares, 1992).

The construction of a bent sequence of length $4l$ through the concatenation of four bent sequences of length l.

Concatenation of four bent functions: known constructions of self-dual functions

- the construction **C1**:

$$\left(h, \widetilde{h}, \widetilde{h}, h \oplus 1\right),$$

  where h is bent function in n variables (Carlet et al., 2010);

- the construction **C2**:

$$(f, g \oplus 1, g, f),$$

  where f is a self-dual bent function, g is an anti-self-dual bent function both in n variables (A.K., 2020).

Gram matrices

Gram matrices for self-dual case

Consider inner products $g_{ij} = \langle F_i, F_j \rangle$, where $F_k = (-1)^{f_k}$.

Gram matrices for self-dual case

Consider inner products $g_{ij} = \langle F_i, F_j \rangle$, where $F_k = (-1)^{f_k}$.

The form of the Gram matrix of self-dual bent functions is characterized by

Theorem (CTCrypt 2022)

The Gram matrix of any bent function in n variables has form

$$\begin{pmatrix} 2^{n-2} & b & b & -a \\ b & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -b \\ -a & -b & -b & 2^{n-2} \end{pmatrix},$$

for some even integers a, b such that

$$-2^{n-2} + 2|b| \leqslant a \leqslant 2^{n-2}.$$

Gram matrices for the known constructions

The constructions **C1** and **C2** provide the following matrices:

$$\mathrm{Gram}(\mathbf{C1}) = \begin{pmatrix} 2^{n-2} & \mathcal{S}_h & \mathcal{S}_h & -2^{n-2} \\ \mathcal{S}_h & 2^{n-2} & 2^{n-2} & -\mathcal{S}_h \\ \mathcal{S}_h & 2^{n-2} & 2^{n-2} & -\mathcal{S}_h \\ -2^{n-2} & -\mathcal{S}_h & -\mathcal{S}_h & 2^{n-2} \end{pmatrix},$$

which has rank 1 when $\mathcal{S}_h = 2^{n-2}$ (f is self-dual bent), and 2 otherwise, and

$$\mathrm{Gram}(\mathbf{C2}) = \begin{pmatrix} 2^{n-2} & 0 & 0 & 2^{n-2} \\ 0 & 2^{n-2} & -2^{n-2} & 0 \\ 0 & -2^{n-2} & 2^{n-2} & 0 \\ 2^{n-2} & 0 & 0 & 2^{n-2} \end{pmatrix}$$

with rank equal to 2. It is obvious that for both constructions the sets $\{F_i\}$ are linearly dependent.

Sufficient condition for bentness of subfunctions

For a bent function f with the Gram matrix $\mathrm{Gram}(f)$ the Gramian has the following expression

$$\mathrm{Gramian}(f) = \left(2^{n-2} - a\right)^2 \left(2^{n-2} + a - 2b\right) \left(2^{n-2} + a + 2b\right).$$

All combinations for which the Gramian is zero were covered in

Theorem (CTCrypt 2022)

If the Gram matrix of a self-dual bent function f is singular then all subfunctions $\{f_i\}_{i=0}^{3}$ are bent.

Sufficient condition for bentness of subfunctions

Theorem (CTCrypt 2022)

If the Gram matrix of a self-dual bent function f is singular then all subfunctions $\{f_i\}_{i=0}^{3}$ are bent.

In particular, the experiments show that

Remark

For $n = 4$ all self-dual bent functions with bent subfunctions have singular Gram matrices.

Question on necessity for self-dual case

Theorem (CTCrypt 2022)

If the Gram matrix of a self-dual bent function f is singular then all subfunctions $\{f_i\}_{i=0}^{3}$ are bent.

Theorem (CTCrypt 2022)

For every even $n \geqslant 6$ there exist self-dual bent functions in n variables with invertible Gram matrices, such that all their subfunctions $\{f_i\}_{i=0}^{3}$ are bent.

Thus, the converse does not hold for $n \geqslant 6$, that is the linear dependence of sign functions provides only **sufficient** condition for subfunctions in $n-2$ variables to be bent.

Question on necessity for self-dual case: $\deg = 2$

Question on necessity for self-dual case: $\deg = 2$

$$f(y_1, y_2, x) = \lambda_1 y_1 \oplus \lambda_2 y_2 \oplus \lambda_{12} y_1 y_2 \oplus y_1 \langle u, x\rangle \oplus y_2 \langle v, x\rangle \oplus g(x),$$
$$y_1, y_2 \in \mathbb{F}_2, x \in \mathbb{F}_2^{n-2}, (\text{assume } f(0) = 0).$$

$$\begin{aligned}
f(00, x) &= f_0(x) = g(x),\\
f(01, x) &= f_1(x) = g(x) \oplus \langle v, x\rangle \oplus \lambda_2,\\
f(10, x) &= f_2(x) = g(x) \oplus \langle u, x\rangle \oplus \lambda_1,\\
f(11, x) &= f_3(x) = g(x) \oplus \langle u \oplus v, x\rangle \oplus \lambda_1 \oplus \lambda_2 \oplus \lambda_{12}, \quad x \in \mathbb{F}_2^{n-2}.
\end{aligned}$$

Question on necessity for self-dual case: $\deg = 2$

$$f(y_1, y_2, x) = \lambda_1 y_1 \oplus \lambda_2 y_2 \oplus \lambda_{12} y_1 y_2 \oplus y_1 \langle u, x\rangle \oplus y_2 \langle v, x\rangle \oplus g(x),$$
$$y_1, y_2 \in \mathbb{F}_2, x \in \mathbb{F}_2^{n-2}, (\text{assume } f(0) = 0).$$

$$\begin{aligned}
f(00, x) &= f_0(x) = g(x),\\
f(01, x) &= f_1(x) = g(x) \oplus \langle v, x\rangle \oplus \lambda_2,\\
f(10, x) &= f_2(x) = g(x) \oplus \langle u, x\rangle \oplus \lambda_1,\\
f(11, x) &= f_3(x) = g(x) \oplus \langle u \oplus v, x\rangle \oplus \lambda_1 \oplus \lambda_2 \oplus \lambda_{12}, \quad x \in \mathbb{F}_2^{n-2}.
\end{aligned}$$

It is clear that f_i are bent and Gram matrix is non-singular if and only if u, v are linearly independent.

Question on necessity for self-dual case: $\deg = 2$

$$
\begin{cases}
\langle u, u\rangle = \langle u, v\rangle = \langle v, v\rangle = 0,\\
\left(B \oplus B^{\mathrm{T}}\right) u = v,\\
\left(B \oplus B^{\mathrm{T}}\right) v = u,\\
u_i u_j \oplus v_i v_j \oplus \left\langle \left(B \oplus B^{\mathrm{T}}\right)^{(i)}, \left(B \oplus B^{\mathrm{T}}\right)^{(j)} \right\rangle = \delta_{ij},\\
\langle u, Bu\rangle = \lambda_1 \oplus \lambda_2,\\
\langle v, Bv\rangle = \lambda_1 \oplus \lambda_2,\\
\lambda_1 u_i \oplus u_i v_i \oplus \lambda_2 v_i \oplus \left(B \oplus B^{\mathrm{T}}\right)_i B \left(B \oplus B^{\mathrm{T}}\right)^{(i)} \oplus b_{ii} = 0,\\
i, j = 1, 2, \ldots, n-2.
\end{cases}
$$

Question on necessity for self-dual case: $\deg = 2$

Theorem

*For every even $n \geqslant 6$ there exists a (**quadratic**) self-dual bent function f in n variables with invertible Gram matrix, such that subfunctions $\{f_i\}_{i=0}^{3}$ are bent.*

Gram matrices for self-dual case vs general case

$$\begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}F_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}F_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}F_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}F_3. \end{cases}$$

Gram matrices for self-dual case vs general case

$$\begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}F_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}F_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}F_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}F_3. \end{cases} \qquad \begin{cases} F_0 + F_1 + F_2 + F_3 = 2\mathcal{H}R_0, \\ F_0 - F_1 + F_2 - F_3 = 2\mathcal{H}R_1, \\ F_0 + F_1 - F_2 - F_3 = 2\mathcal{H}R_2, \\ F_0 - F_1 - F_2 + F_3 = 2\mathcal{H}R_3 \end{cases}$$

(R_0, R_1, R_2, R_3) — sign vector of the dual bent function.

Gram matrix of a bent function

Theorem

The Gram matrices of a bent function f in n variables and its dual $\tilde{f}$ have form

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix},$$

$$\mathrm{Gram}(\tilde{f}) = \begin{pmatrix} 2^{n-2} & c & b & -a \\ c & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -c \\ -a & -b & -c & 2^{n-2} \end{pmatrix}$$

for some even integers a, b, c such that

$$-2^{n-2} + |b+c| \leqslant a \leqslant 2^{n-2} - |b-c|.$$

Sufficient condition for bentness of subfunctions

For a bent function f with the Gram matrix $\mathrm{Gram}(f)$ the Gramian has the following expression

$$\begin{aligned}\mathrm{Gramian}(f) = & \left(2^{n-2} - a + b - c\right)\left(2^{n-2} - a - b + c\right) \\ & \times \left(2^{n-2} + a - b - c\right)\left(2^{n-2} + a + b + c\right).\end{aligned}$$

Sufficient condition for bentness of subfunctions

The next results covers all combinations for which the Gramian is zero.

Theorem

If the Gram matrix of a bent function f is singular then all subfunctions $\{f_i\}_{i=0}^{3}$ are bent. Moreover, all such subfunctions of its dual are also bent.

Sufficient condition for bentness of subfunctions

The next results covers all combinations for which the Gramian is zero.

Theorem

If the Gram matrix of a bent function f is singular then all subfunctions $\{f_i\}_{i=0}^{3}$ are bent. Moreover, all such subfunctions of its dual are also bent.

Corollary

If sign vectors of subfunctions $\{f_i\}_{i=0}^{3}$ of a bent function are linearly dependent then all these subfunctions are bent.

$f = (f_0, f_1, f_2, f_3)$ — decomposition of the vector of values of a (self-dual) bent function f in n variables

$$g_{ij} = \sum_{x \in \mathbb{F}_2^{n-2}} (-1)^{f_i(x) \oplus f_j(x)}$$

$\mathrm{Gram}(f) = (g_{ij})$ — the Gram matrix of the function f

General form of the Gram matrix of bent function and its dual one:

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix}$$

$$\mathrm{Gram}(\widetilde{f}) = \begin{pmatrix} 2^{n-2} & c & b & -a \\ c & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -c \\ -a & -b & -c & 2^{n-2} \end{pmatrix}$$

The determinant of the Gram matrix:

$$\mathrm{Gramian}(f) = \left(2^{n-2} - a + b - c\right)\left(2^{n-2} - a - b + c\right) \times \left(2^{n-2} + a - b - c\right)\left(2^{n-2} + a + b + c\right).$$

If the Gramian is equal to zero, all subfunctions $\{f_i\}_{i=0}^{3}$ are bent. The converse holds for $n = 4$ for self-dual case and does not hold for $n \geqslant 6$.

Generalizations of bent functions: history

- Kumar, Scholtz, Welch «Generalized bent functions and their properties» (1985);
- Matsufuji, Imamura «Real-valued bent function and its application to the design of balanced quadriphase sequences with optimal correlation properties» (1991);
- Logachev, Salnikov, Yashchenko «Bent functions on a finite Abelian group» (1997);
- Solodovnikov «Bent functions from a finite Abelian group into a finite Abelian group» (2002);
- Schmidt «Quaternary constant-amplitude codes for multicode CDMA» (published in 2009, preprint appeared in 2007).

A survey on different generalizations of bent functions can be found in «Tokareva N.N., Generalizations of bent functions — a survey (2011)».

Generalized bent functions

The generalized Walsh-Hadamard transform (WHT) of the generalized Boolean function $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ in n variables is a function $H_f : \mathbb{F}_2^n \to \mathbb{C}$, defined as

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

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

A generalized Boolean function f in n variables is said to be generalized bent (gbent) if $|H_f(y)| = 2^{n/2}$ for any $y \in \mathbb{F}_2^n$ (Schmidt, 2009).

Generalizied bent functions

- Solé, Tokareva «Connections between quaternary and binary bent functions» (2009);
- Stănică, Martinsen, Gangopadhyay, Singh «Bent and generalized bent functions» (2013);
- Martinsen, Meidl, Stănică «Generalized bent functions and their Gray images» (2017);
- Tang, Xiang, Qi, Feng «Complete characterization of generalized bent and 2^k-bent Boolean functions» (2017);
- Hodžić, Meidl, Pasalic «Full characterization of generalized bent functions as (semi)-bent spaces, their dual, and the Gray image» (2018);
- Mesnager, Tang, Qi, Wang, Wu, Feng «Further results on generalized bent functions and their complete characterization» (2018);
- Meidl, «A survey on p-ary and generalized bent functions» (2022).

Applications of generalized Boolean functions

Applications of generalized Boolean functions

- Generalized Reed–Muller codes were suggested by Paterson (2000) to use in orthogonal frequency-division multiplexing (OFDM). These codes offer error correcting capability combined with substantially reduced peak-to-mean power ratios;

Applications of generalized Boolean functions

- Generalized Reed–Muller codes were suggested by Paterson (2000) to use in orthogonal frequency-division multiplexing (OFDM). These codes offer error correcting capability combined with substantially reduced peak-to-mean power ratios;
- Gangopadhyay, Poonia, Aggarwal, Parekh, «Generalized Boolean Functions and Quantum Circuits on IBM-Q» (2019);

Applications of generalized Boolean functions

- Generalized Reed–Muller codes were suggested by Paterson (2000) to use in orthogonal frequency-division multiplexing (OFDM). These codes offer error correcting capability combined with substantially reduced peak-to-mean power ratios;
- Gangopadhyay, Poonia, Aggarwal, Parekh, «Generalized Boolean Functions and Quantum Circuits on IBM-Q» (2019);
- Generalized bent functions have strong relation with vectorial bent functions, they also generate sets of component Boolean bent functions.

Dual to generalized bent function

For a subset of so called regular gbent function the dual generalized Boolean function is uniquely defined.

The condition $H_f(x) = \omega^{\tilde{f}(x)} 2^{n/2}$ for any $x \in \mathbb{F}_2^n$ gives the generalized Boolean function $\tilde{f}$ that is said to be dual of f. Every dual function is a gbent function, moreover it holds $\tilde{\tilde{f}} = f$.
If for any $y \in \mathbb{F}_2^n$ it holds $H_f(y) = \zeta \omega^{\widetilde{f}(y)} 2^{n/2}$, where $\zeta \in \mathbb{C}$ and $|\zeta| = 1$, the gbent function f is said to be weakly regular.

A regular gbent function f is said to be self-dual if $f = \widetilde{f}$, and anti-self-dual if $f = \widetilde{f} + q/2$. Consequently, it is the case only for even q.

Gbent functions of algebraic degree 1

Generalized Boolean functions of the form

$$f(x) = \sum_{j=1}^{n} \lambda_j x_j + \lambda_0, \quad x \in \mathbb{F}_2^n,$$

where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$, in the literature often are referred to as «affine» functions. In fact, their vectors of values are codewords of the generalized Reed–Muller code $\mathrm{RM}_q(1, n)$ (Davis, Jedwab, 1999; Paterson, 2000).

Gbent functions of algebraic degree 1

Generalized Boolean functions of the form

$$f(x) = \sum_{j=1}^{n} \lambda_j x_j + \lambda_0, \quad x \in \mathbb{F}_2^n,$$

where $\lambda_0, \lambda_1, \ldots, \lambda_n \in \mathbb{Z}_q$, in the literature often are referred to as «affine» functions. In fact, their vectors of values are codewords of the generalized Reed–Muller code $\mathrm{RM}_q(1,n)$ (Davis, Jedwab, 1999; Paterson, 2000).

Gbentness of these functions was studied by Singh in 2013 for the case when q is divisible by 4 and it was shown that if $\lambda_j \in \{\frac{q}{4}, \frac{3q}{4}\}$ for any $j = 1, 2 \ldots, n$, then these functions are gbent. It was proved that affine generalized Boolean function is gbent if and only if

$$\prod_{j=1}^{n} \left(1 + (-1)^{y_j} \cos \frac{2\pi\lambda_j}{q}\right) = 1 \text{ for any } y \in \mathbb{F}_2^n.$$

Affine gbent functions

In (Schmidt, 2009) the quaternary function

$$f(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \ldots + x_n$$

and its shifts were considered for obtaining a constant-amplitude code. For quaternary case it is gbent, moreover, it is regular but only for even n. A very similar construction of real-valued bent functions was proposed in (Matsufuji, Imamura, 1993).

Affine gbent functions

In (Schmidt, 2009) the quaternary function

$$f(x_1, x_2, \ldots, x_n) = x_1 + x_2 + \ldots + x_n$$

and its shifts were considered for obtaining a constant-amplitude code. For quaternary case it is gbent, moreover, it is regular but only for even n. A very similar construction of real-valued bent functions was proposed in (Matsufuji, Imamura, 1993).

The next result shows the non-existence of self-dual gbent functions within the class of affine functions.

Proposition (CTCrypt 2021)

There are no affine self-dual gbent functions.

Characterization of affine gbent functions

In the next result we prove that the values of coefficients, proposed in (Singh, 2013), are also necessary for affine generalized Boolean function to be gbent.

Theorem

Affine generalized Boolean function is gbent if and only if $q \equiv 0 \pmod 4$ *and* $\lambda_j \in \left\{\frac{q}{4}, \frac{3q}{4}\right\}$ *for any* $j = 1, 2, \dots, n$.

Characterization of affine gbent functions

In the next result we prove that the values of coefficients, proposed in (Singh, 2013), are also necessary for affine generalized Boolean function to be gbent.

Theorem

Affine generalized Boolean function is gbent if and only if $q \equiv 0 \pmod 4$ *and* $\lambda_j \in \{\frac{q}{4}, \frac{3q}{4}\}$ *for any* $j = 1, 2, \ldots, n$.

Corollary

The number of affine gbent functions is equal to $q \cdot 2^n$.

Theorem

Affine gbent function is regular if and only if at least one of conditions is satisfied:

1) *n is even;*
2) $q \equiv 0 \pmod 8$,

and its dual gbent is equal to

$$\widetilde{f}(x) = \sum_{j=1}^{n} (q - \lambda_j)\, x_j + \left(\lambda_0 + \frac{3q}{4} n + \frac{3}{2} \sum_{k=1}^{n} \lambda_k\right).$$

If n is odd and $q \equiv 4 \pmod 8$, *gbent function is weakly regular with* $\zeta = \exp\left(\frac{3\pi i}{q} \sum_{k=1}^{n} \lambda_k\right)$, *its dual is equal to*

$$\widetilde{f}(x) = \sum_{j=1}^{n} (q - \lambda_j)\, x_j + \left(\lambda_0 + \frac{3q}{4} n\right).$$

It follows that the dual of affine gbent function, if exists, is also **affine**.

Its coefficients are the ones of f that are reflected with a respect to q.

$$\lambda_j \longrightarrow q - \lambda_j, \quad j = 1, 2, \ldots, n.$$

At the same time the coefficient λ_0 is changed in another way.

$$\lambda_0 \longrightarrow \lambda_0 + \frac{3q}{4}n + \frac{3}{2}\sum_{k=1}^{n} \lambda_k$$

A polyphase vector (sequence) of $f \in \mathcal{GF}_n^q$ is a complex-valued vector

$$F = \omega^f = \left(\omega^{f_0}, \omega^{f_1}, \dots, \omega^{f_{2^n-1}}\right)$$

of length 2^n, where $(f_0, f_1, \dots, f_{2^n-1})$ is a vector of values of the function f.

We can also note an interesting fact

Corollary

The polyphase vector $\omega^{\widetilde{f}}$ of the dual gbent function $\widetilde{f}$ of affine gbent function f is equal to the complex conjugation of ω^f up to the global phase $\exp\left(\frac{3\pi i}{2} + \frac{3\pi i}{q}\sum_{k=1}^{n}\lambda_k\right)$.

It means the duality mapping, acting on polyphase vectors of gbent functions, coincides with the conjugation up to the global phase, that depends on coefficients of affine gbent function.

Component Boolean functions

Let $2^{k-1} < q \leqslant 2^k$. For any generalized Boolean function in n variables it is possible to associate a unique sequence of so called component Boolean functions $a_0, a_1, \ldots, a_{k-1} \in \mathcal{F}_n$ such that (Stănică, Martinsen, Gangopadhyay, Singh, 2013):

$$f(x) = a_0(x) + 2a_1(x) + \ldots + 2^{k-1}a_{k-1}(x), \quad x \in \mathbb{F}_2^n.$$

Component Boolean functions

Let $2^{k-1} < q \leqslant 2^k$. For any generalized Boolean function in n variables it is possible to associate a unique sequence of so called component Boolean functions $a_0, a_1, \ldots, a_{k-1} \in \mathcal{F}_n$ such that (Stănică, Martinsen, Gangopadhyay, Singh, 2013):

$$f(x) = a_0(x) + 2a_1(x) + \ldots + 2^{k-1}a_{k-1}(x), \quad x \in \mathbb{F}_2^n.$$

Hodžić, Meidl, Pasalic in 2018 proved that for the case $q = 2^k$ and even n, provided that f is gbent its dual gbent $\widetilde{f}$ has the following form

$$\widetilde{f}(x) = b_0(x) + 2b_1(x) + \ldots + 2^{k-1}b_{k-1}(x), \quad x \in \mathbb{F}_2^n,$$

where $b_{k-1} = \widetilde{a}_{k-1}$ and $b_j = \widetilde{a}_{k-1} \oplus \left(\widetilde{a_{k-1} \oplus a_j}\right)$.

Further we will consider the case $q = 2^k$, where $k \geqslant 3$.

Theorem

The component Boolean functions $a_0, a_1, \ldots, a_{n-1} \in \mathcal{F}_n$ of affine gbent function are equal to

$$\begin{aligned}
a_0(x) &= c_0, \\
a_1(x) &= c_1, \\
&\vdots \\
a_{k-3}(x) &= c_{k-3}, \\
a_{k-2}(x) &= c_{k-2} \oplus \bigoplus_{j=1}^{n} x_j, \\
a_{k-1}(x) &= c_{k-1} \oplus \bigoplus_{h=1}^{n} b_h x_h \oplus \bigoplus_{1 \leqslant r < s \leqslant n} x_r x_s,
\end{aligned}$$

where $x \in \mathbb{F}_2^n$ and vector c is the binary representation of the element λ.

Theorem

The component Boolean functions $b_0, b_1, \ldots, b_{n-1} \in \mathcal{F}_n$ of the dual to affine gbent function are equal to

$$\begin{aligned} b_0(x) &= \widetilde{c}_0 \\ b_1(x) &= \widetilde{c}_1 \\ &\vdots \\ b_{k-3}(x) &= \widetilde{c}_{k-3} \\ b_{k-2}(x) &= \widetilde{c}_{k-2} \oplus \bigoplus_{j=1}^{n} x_j \\ b_{k-1}(x) &= \widetilde{c}_{k-1} \oplus \bigoplus_{l=1}^{n} x_l \oplus \bigoplus_{h=1}^{n} b_h x_h \oplus \bigoplus_{1 \leqslant r < s \leqslant n} x_r x_s, \end{aligned}$$

where $x \in \mathbb{F}_2^n$ and vector $\widetilde{c}$ is the binary representation of the element $\widetilde{\lambda}_0 = \lambda_0 + \frac{3q}{4} n + \frac{3}{2} \sum_{k=1}^{n} \lambda_k$.

Lee distance

The Lee weight of the element $x \in \mathbb{Z}_q$ is $\mathrm{wt}_L(x) = \min\{x, q - x\}$.

The Lee weight of generalized Boolean function is the sum of Lee weights of all its values:

$$\mathrm{wt}_L(f) = \sum_{x \in \mathbb{F}_2^n} \mathrm{wt}_L(f(x)).$$

The Lee distance $\mathrm{dist}_L(f, g)$ between generalized Boolean functions f, g is equal to $\mathrm{wt}_L(f - g)$, where the operation " $-$ " is considered over the ring $\mathbb{Z}_q$.

The duality mapping is isometric on the set of affine gbent functions

It is well-known that the duality mapping, being defined on Boolean bent functions, is isometry, that is it preserves the Hamming distance between any pair of bent functions (Carlet, 1994). It has a great interest in a scope of bent functions since it is the only known isometric mapping of the set of bent functions that is not an element of its group of automorphisms.

We prove that

Theorem

Within the Lee distance the duality mapping is an isometry of the set of regular affine gbent functions.

Thanks for attention!