

On metric complements of some subclasses of bent functions

Nikolay Kolomeec, Natalia Tokareva

Novosibirsk State University
Novosibirsk, Russia

June 4, 2026

The 15th Workshop on Current Trends in Cryptology
CTCrypt 2026
Minsk, Belarus

$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is a **Boolean function** in n variables

$\mathcal{F}_n$ is the set of all Boolean functions in n variables

$d(f, g)$ is the **Hamming distance** between $f, g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$

$\langle a, b \rangle = a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_n b_n$, where $a, b \in \mathbb{F}_2^n$

$x \mapsto \langle a, x \rangle \oplus c$ is an **affine function**, $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$

$\mathcal{A}_n$ is the set of all **affine functions** in n variables

$a \oplus D = \{a \oplus x : x \in D\}$, $A \oplus B = \{a \oplus b : a \in A, b \in B\}$, etc.

An **affine subspace** of $\mathbb{F}_2^n$ is $a \oplus L$, L is a linear subspace of $\mathbb{F}_2^n$

The **Walsh–Hadamard transform** of a function $g \in \mathcal{F}_n$:

$$W_g : x \in \mathbb{F}_2^n \mapsto \sum_{y \in \mathbb{F}_2^n} (-1)^{g(y) \oplus \langle x, y \rangle}$$

As a rule, we will consider functions in $2n$ variables

A function $f : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2$ is a **bent function** if $W_f(x) = \pm 2^n$ for all $x \in \mathbb{F}_2^{2n}$

The **dual** function $\tilde{f}$ of f is defined as

$$(-1)^{\tilde{f}(x)} = 2^{-n} W_f(x) \text{ for all } x \in \mathbb{F}_2^{2n}$$

$\tilde{f}$ is a bent function too and $\tilde{\tilde{f}} = f$

$\mathcal{B}_{2n}$ is the set of all **bent** functions in $2n$ variables



Bent functions were introduced in 1960th

- by **O. Rothaus** in the USA,
- by **V. A. Eliseev** and **O. P. Stepchenkov** in the USSR.

They have the following applications:

- Boolean functions with high nonlinearity (cryptography),
- Hadamard matrices (combinatorics),
- Kerdock codes and codes for CDMA (coding theory).

A bent function is **not balanced**.

Bent functions are used in S-boxes of block cipher **CAST**, in hash function **HAVAL**.

Metric complements and metric regularity

Definition 1

- The **distance** from $f \in \mathcal{F}_n$ to $S \subseteq \mathcal{F}_n (\mathbb{F}_2^m)$:

$$d(f, S) = \min_{g \in S} d(f, g).$$

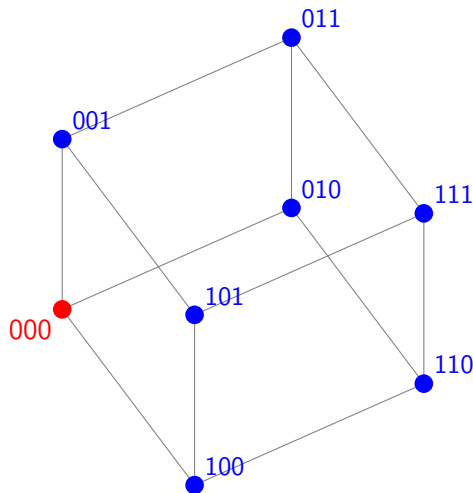
- The **covering radius** of S :

$$r(S) = \max_{g \in \mathcal{F}_n (\mathbb{F}_2^m)} d(g, S).$$

- The **metric complement** of S :

$$\text{Comp}(S) = \{g \in \mathcal{F}_n (\mathbb{F}_2^m) : d(f, S) = r(S)\}.$$

For instance, $\text{Comp}(\mathbb{F}_2^3 \setminus \{000\}) = \{000\}$.



Definition 2 (N. Tokareva, 2010)

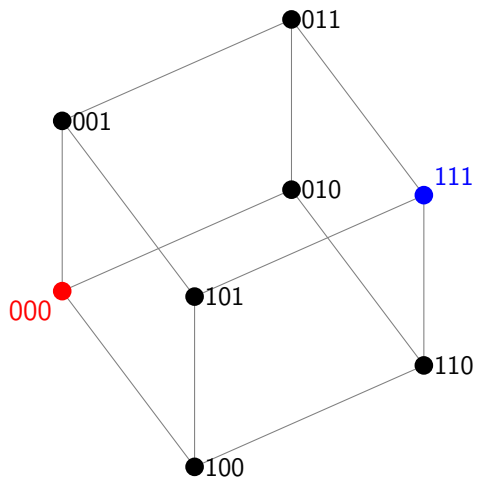
The set $S \subseteq \mathcal{F}_n(\mathbb{F}_2^m)$ is **metrically regular** if

$$\text{Comp}(\text{Comp}(S)) = S.$$

For instance, $\text{Comp}(\{111\}) = \{000\}$ and $\text{Comp}(\{000\}) = \{111\}$.

Investigations of metrically regular sets:

- N. Tokareva (2010, 2012);
- A. Oblaukhov (2016, 2018, 2019, 2020, 2021);
- A. Kutsenko (2020).



We recall that all **isometries** of $\mathcal{F}_n$ are exactly the following mappings:

$$f \in \mathcal{F}_n \mapsto f \circ \pi \oplus h,$$

where $\pi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is invertible and $h \in \mathcal{F}_n$; $f \circ \pi$ is the function $x \in \mathbb{F}_2^n \mapsto f(\pi(x))$.

$\text{Comp}(S \circ \pi \oplus h) = \text{Comp}(S) \circ \pi \oplus h$ for such π and h .

The group of automorphisms $\text{Aut}(S)$ of $S \subseteq \mathcal{F}_n$ is the set of all isometries ξ of $\mathcal{F}_n$ such that

$$\xi(S) = \{\xi(f) : f \in S\} = S.$$

The following properties are satisfied:

- $\text{Aut}(S) \subseteq \text{Aut}(\text{Comp}(S))$,
- $\text{Aut}(S) = \text{Aut}(\text{Comp}(S))$ for metrically regular S .

By definition,

- $r(\mathcal{A}_{2n}) = 2^{2n-1} - 2^{n-1}$ is the **maximum nonlinearity** of a function in $2n$ variables
- $\mathcal{B}_{2n} = \text{Comp}(\mathcal{A}_{2n})$,
- $r(\mathcal{A}_{2n+1})$ is unknown.

$\mathcal{A}_{2n} = \text{Comp}(\mathcal{B}_{2n})$, i.e. $\mathcal{B}_{2n}$ and $\mathcal{A}_{2n}$ are metrically regular (N. Tokareva, 2010).

An additional metric characterization of $S \subseteq \mathcal{B}_{2n}$: if S is metrically regular, then this is the metric complement of $\text{Comp}(S)$.

The group of automorphisms of $S \subseteq \mathcal{B}_{2n}$.

We will consider only «bent» distance $2^{2n-1} - 2^{n-1}$.

$\mathcal{Q}_{2n}$ — the set of all **quadratic** bent functions in $2n$ variables.

Theorem 3

It holds that $\text{Comp}(\mathcal{Q}_{2n}) = \mathcal{A}_{2n}$ and $r(\mathcal{Q}_{2n}) = 2^{2n-1} - 2^{n-1}$.

The following classes are not metrically regular as well.

Corollary 4

Let $\mathcal{Q}_{2n} \subseteq S \subseteq \mathcal{B}_{2n}$. Then $\text{Comp}(S) = \mathcal{A}_{2n}$ and $r(S) = 2^{2n-1} - 2^{n-1}$. Moreover, any such $S \neq \mathcal{B}_{2n}$ is not metrically regular.

This also imply that

- $\text{Comp}(\mathcal{B}_{2n}) = \mathcal{A}_{2n}$,
- $\text{Aut}(\mathcal{Q}_{2n}) = \text{Aut}(\mathcal{B}_{2n})$.

Eliseev–Maiorana–McFarland bent functions

The **Eliseev–Maiorana–McFarland class** $\mathcal{M}_{2n}$ consists of all functions of the form

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y), \quad x, y \in \mathbb{F}_2^n, \text{ where}$$

- π is any permutation on $\mathbb{F}_2^n$,
- $\varphi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is any Boolean function.

It was introduced independently by **V. A. Eliseev**, **J. A. Maiorana** and **R. L. McFarland** (1960th – 1970th).

The dual bent function to f is $\tilde{f}(x, y) = \langle y, \pi^{-1}(x) \rangle \oplus \varphi(\pi^{-1}(x))$, i.e.

$$\widetilde{\mathcal{M}}_{2n} = \{(x, y) \mapsto f(y, x) : f \in \mathcal{M}_{2n}\}.$$

The elements of $\text{Aut}(\mathcal{B}_{2n})$ maps $\mathcal{M}_{2n}$ to $\mathcal{M}_L$ for some n -dimensional $L \subseteq \mathbb{F}_2^{2n}$:

$$\mathcal{M}_L = \{f \in \mathcal{B}_{2n} : f \text{ is affine on } a \oplus L \text{ for all } a \in \mathbb{F}_2^{2n}\}.$$

We also need to «extend» the set $\mathcal{A}_m$ of affine Boolean functions:

$$\mathcal{A}_L = \{f \in \mathcal{F}_m : f(x) \oplus f(x \oplus a) \text{ is constant for each } a \in L\}.$$

The most useful sets for us are

$$\mathcal{A}_{m,k} = \mathcal{A}_{\mathbb{F}_2^{m-k} \times \{0\}^k} \text{ and } \mathcal{A}'_{m,k} = \mathcal{A}_{\{0\}^k \times \mathbb{F}_2^{m-k}}.$$

In other words, we can define them as

$$\begin{aligned} \mathcal{A}_{m,k} &= \{(x, y) \mapsto \langle a, x \rangle \oplus g(y) : g \in \mathcal{F}_k, a, x \in \mathbb{F}_2^{m-k}\}, \\ \mathcal{A}'_{m,k} &= \{(x, y) \mapsto g(x) \oplus \langle a, y \rangle : g \in \mathcal{F}_k, a, y \in \mathbb{F}_2^{m-k}\}. \end{aligned}$$

The following holds:

$$\mathcal{A}_m = \mathcal{A}_{m,0} = \mathcal{A}_{m,1} \subset \mathcal{A}_{m,2} \subset \dots \subset \mathcal{A}_{m,m} = \mathcal{F}_m.$$

Theorem 5

The following holds:

- ① $\text{Comp}(\mathcal{M}_{2n}) = \mathcal{A}_{2n,n}$ and $\text{Comp}(\mathcal{A}_{2n,n}) = \mathcal{M}_{2n}$,
- ② $\text{Comp}(\widetilde{\mathcal{M}}_{2n}) = \mathcal{A}'_{2n,n}$ and $\text{Comp}(\mathcal{A}'_{2n,n}) = \widetilde{\mathcal{M}}_{2n}$,

i.e. both $\mathcal{M}_{2n}$ and $\widetilde{\mathcal{M}}_{2n}$ are metrically regular. Also,

$$r(\mathcal{M}_{2n}) = r(\widetilde{\mathcal{M}}_{2n}) = 2^{2n-1} - 2^{n-1}.$$

Similar to $\mathcal{Q}_{2n}$, we can easily construct sets whose metric complement is $\mathcal{A}_{2n}$.

Corollary 6

Let $\mathcal{M}_{2n} \cup \widetilde{\mathcal{M}}_{2n} \subseteq S \subseteq \mathcal{B}_{2n}$. Then $\text{Comp}(S) = \mathcal{A}_{2n}$ and $r(S) = 2^{2n-1} - 2^{n-1}$. Moreover, any such $S \neq \mathcal{B}_{2n}$ is not metrically regular.

It is not difficult to describe metric complements of all classes affine equivalent to $\mathcal{M}_{2n}$.

Corollary 7

Let L be a linear subspace of $\mathbb{F}_2^{2n}$ of dimension n . Then

- ① $\text{Comp}(\mathcal{M}_L) = \mathcal{A}_L$ and $\text{Comp}(\mathcal{A}_L) = \mathcal{M}_L$,
- ② $\text{Comp}(\widetilde{\mathcal{M}}_L) = \mathcal{A}_{L^\perp}$ and $\text{Comp}(\mathcal{A}_{L^\perp}) = \widetilde{\mathcal{M}}_L$,
- ③ $\mathcal{M}_L$ and $\widetilde{\mathcal{M}}_L$ are metrically regular, $r(\mathcal{M}_L) = r(\widetilde{\mathcal{M}}_L) = 2^{2n-1} - 2^{n-1}$,
- ④ $\text{Comp}(\mathcal{M}_{L_1} \cup \dots \cup \mathcal{M}_{L_s}) = \mathcal{A}_{L_1 \oplus \dots \oplus L_s}$, где $L_1, \dots, L_s$ — линейные подпространства $\mathbb{F}_2^{2n}$ размерности n и $s \geq 2$,
- ⑤ $\text{Comp}(\mathcal{M}_{L_1} \cup \dots \cup \mathcal{M}_{L_s}) = \mathcal{A}_{2n} \iff$ the dimension of $L_s \oplus \dots \oplus L_s$ is at least $2n - 1$.

The generalized Eliseev–Maiorana–McFarland bent
functions and their duals

The **generalized Eliseev–Maiorana–McFarland class** $\mathcal{M}_{2n,k}$ (V.V. Yaschenko, 1997) consisting of all **bent functions** of the form

$$f(x, y) = \langle x, \Phi(y) \rangle \oplus \varphi(y), \quad x \in \mathbb{F}_2^k, \quad y \in \mathbb{F}_2^{2n-k}, \quad \text{where}$$

- $\Phi : \mathbb{F}_2^{2n-k} \rightarrow \mathbb{F}_2^k$ is some **balanced mapping** (it takes each value of $\mathbb{F}_2^k$ on the same number of arguments), $k \leq n$,
- $\varphi : \mathbb{F}_2^{2n-k} \rightarrow \mathbb{F}_2$ is some Boolean function.

These classes are **not** constructive. They satisfy

$$\mathcal{M}_{2n} = \mathcal{M}_{2n,n} \subseteq \mathcal{M}_{2n,n-1} \subseteq \dots \subseteq \mathcal{M}_{2n,2} \subseteq \mathcal{M}_{2n,1} = \mathcal{B}_{2n}.$$

We will use $\mathcal{M}_L$ for $\dim L < n$ as well.

It is «hard» to simplify the expression for a dual bent function.

There are other «generalizations of $\mathcal{M}_{2n}$ ».

Theorem 8

Let $k < n$. Then

- ① $\text{Comp}(\mathcal{M}_{2n,k}) = \mathcal{A}_{2n}$ and $r(\mathcal{M}_{2n,k}) = 2^{2n-1} - 2^{n-1}$,
- ② $\mathcal{M}_{2n,k}$ is not metrically regular if $2 \leq k < n$.

The same obviously holds for $\mathcal{M}_L$.

Corollary 9

Let L be a linear subspace of $\mathbb{F}_2^{2n}$. Then

- ① $\text{Comp}(\mathcal{M}_L) = \mathcal{A}_{2n}$ and $r(\mathcal{M}_L) = 2^{2n-1} - 2^{n-1}$ if $1 \leq \dim L < n$,
- ② $\mathcal{M}_L$ is not metrically regular if $2 \leq \dim L < n$,
- ③ any $S \subset \mathcal{B}_{2n}$ containing $\mathcal{M}_L$, where $2 \leq \dim L < n$, is not metrically regular.

At the same time, the metric properties of $\widetilde{\mathcal{M}}_{2n,k}$ are different.

Theorem 10

Let $k \leq n$. Then $\text{Comp}(\widetilde{\mathcal{M}}_{2n,k}) = \mathcal{A}'_{2n,k}$ and $\text{Comp}(\mathcal{A}'_{2n,k}) = \widetilde{\mathcal{M}}_{2n,k}$, i.e. $\widetilde{\mathcal{M}}_{2n,k}$ is metrically regular, and $r(\widetilde{\mathcal{M}}_{2n,k}) = 2^{2n-1} - 2^{n-1}$.

The same obviously holds for $\mathcal{M}_L$.

Corollary 11

Let L be at most n -dimensional linear subspace of $\mathbb{F}_2^{2n}$. Then $\text{Comp}(\widetilde{\mathcal{M}}_L) = \mathcal{A}_{L^\perp}$ and $\text{Comp}(\mathcal{A}_{L^\perp}) = \widetilde{\mathcal{M}}_L$, i.e. $\widetilde{\mathcal{M}}_L$ is metrically regular. Also, $r(\widetilde{\mathcal{M}}_L) = 2^{2n-1} - 2^{n-1}$.

The mapping $\widetilde{\mathcal{D}} : f \in \mathcal{B}_{2n} \mapsto \widetilde{f}$ is an **isometry on the set** $\mathcal{B}_{2n}$:

$$d(f, g) = d(\widetilde{f}, \widetilde{g}) \text{ for all } f, g \in \mathcal{B}_{2n}.$$

However, this mapping **cannot** be extended to an isometry of $\mathcal{F}_{2n}$ (A. Kutsenko, 2020).

The difference in metric regularity of $\mathcal{M}_{2n,k}$ and $\widetilde{\mathcal{M}}_{2n,k}$ also imply this fact.

We note that

- $\mathcal{M}_{2n,k}$ and $\widetilde{\mathcal{M}}_{2n,k}$ are subsets of $\mathcal{B}_{2n}$,
- $\widetilde{\mathcal{D}}$ is an isometry on the set $\mathcal{B}_{2n}$.

This is not enough for $\mathcal{M}_{2n,k}$ and $\widetilde{\mathcal{M}}_{2n,k}$ to have the same metric properties.

The characterization of dual bent functions of generalized
Eliseev–Maiorana–McFarland bent functions

Since the class $\widetilde{\mathcal{M}}_{2n,k}$ is metric regular, we can characterize it as the metric complement of $\text{Comp}(\widetilde{\mathcal{M}}_{2n,k})$.

This characterization can be easily transformed to the following theorem.

Theorem 12

Let $f : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2$ and $1 \leq k \leq n$. Then $f \in \widetilde{\mathcal{M}}_{2n,k} \iff f(x, y) \oplus g(x)$ is a bent function for any $g : \mathbb{F}_2^k \rightarrow \mathbb{F}_2$, where $x \in \mathbb{F}_2^k$ and $y \in \mathbb{F}_2^{2n-k}$.

In the case of $\widetilde{\mathcal{M}}_{2n,k}$ we have the following.

Corollary 13

Let $f \in \mathcal{B}_{2n}$. Then $f \in \widetilde{\mathcal{M}}_{2n,2} \iff f(x, y) \oplus x_1 x_2$ is a bent function, where $x_1, x_2 \in \mathbb{F}_2$ and $y \in \mathbb{F}_2^{2n-2}$.

Let the function $f = (f_a)_{a \in \mathbb{F}_2^{n_1}}$ of $n_1 + n_2$ is defined as

$$f(x, y) = \bigoplus_{a \in \mathbb{F}_2^{n_1}} f_a(y) \prod_{i=1}^{n_1} (x_i \oplus a_i \oplus 1), \quad (1)$$

where each $f_a : \mathbb{F}_2^{n_2} \rightarrow \mathbb{F}_2$.

This is the representation of f using **its subfunctions**:

$$f_a(y) = f(a, y) \text{ for all } a \in \mathbb{F}_2^{n_1} \text{ and } y \in \mathbb{F}_2^{n_2}.$$

This is the easiest case for Theorem 12.

Corollary 14

Let $f = (f_a)_{a \in \mathbb{F}_2^{n_1}}$ for $f_a : \mathbb{F}_2^{n_2} \rightarrow \mathbb{F}_2$. Then $f \in \widetilde{\mathcal{M}}_{n_1+n_2, n_1} \iff (f_a \oplus g(a))_{a \in \mathbb{F}_2^{n_1}}$ is a bent function for any $g : \mathbb{F}_2^{n_1} \rightarrow \mathbb{F}_2$.

The following construction was proposed by I.P. Baksova and Yu.V. Tarannikov (2020).

Let $n_2 \geq n_1$, $n_1 + n_2$ be even and $(C_a)_{a \in \mathbb{F}_2^{n_1}}$ be an ordered partition of $\mathbb{F}_2^{n_2}$ into 2^{n_1} its affine $(n_2 - n_1)$ -dimensional subspaces.

Then the function $f = (f_a)_{a \in \mathbb{F}_2^{n_1}}$ in $n_1 + n_2$ is a bent function if the Walsh–Hadamard coefficients of each $f_a : \mathbb{F}_2^{n_2} \rightarrow \mathbb{F}_2$ satisfy the following condition:

$$W_{f_a}(y) = \begin{cases} \pm 2^{\frac{n_1+n_2}{2}} & \text{if } y \in C_a \\ 0 & \text{otherwise} \end{cases}.$$

All such bent functions form the class K_{n_1, n_2} of cardinality

$$|K_{n_1, n_2}| = |\mathcal{B}_{n_2 - n_1}|^{2^{n_1}} N_{n_2, n_2 - n_1},$$

where $N_{n_2, n_2 - n_1}$ is the number of all distinct $(C_a)_{a \in \mathbb{F}_2^{n_1}}$.

Corollary 15

The following class inclusion is correct: $K_{n_1, n_2} \subseteq \widetilde{\mathcal{M}}_{n_1+n_2, n_1}$.

In the recent work (S. Kudin, E. Pasalic, A. Polujan et al., 2025), the class $\mathcal{M}_{2n, n-1}$ was investigated. For instance, the following was proved:

$$|\mathcal{M}_{2n, n-1}| = 2^{3 \cdot 2^{n-1}} N_{n+1, 2},$$

where $N_{n+1, 2}$ is the number of all ordered partitions of $\mathbb{F}_2^{n+1}$ into its 2-dimensional affine subspaces.

Corollary 16

It holds that $K_{n-1, n+1} = \widetilde{\mathcal{M}}_{2n, n-1}$.

We note that the set $\mathcal{B}_{2n}$ can be described in terms of **bent rectangles** (S.V. Agievich, 2002, 2008), which is also a representation using subfunctions.

V.N. Potapov, A.A. Taranenko and Yu.V. Tarannikov (2023) proved that

$$\log_2 |K_{n-1,n+1}| = \frac{3n}{2} \cdot 2^n(1 + o(1)).$$

Until recently, this was the **best lower bound** of the cardinality of $\mathcal{B}_{2n}$: for $m = 2n$,

$$\log_2 |\mathcal{B}_m| \geq \frac{3m}{4} \cdot 2^{m/2}(1 + o(1)),$$

whereas

$$\log_2 |\mathcal{M}_m^\#| = \frac{m}{2} \cdot 2^{m/2}(1 + o(1)).$$

Corollary 17

*The mentioned lower bound of $|\mathcal{B}_{2n}|$ takes into account only **normal** bent functions: each of them is constant on some n -dimensional affine subspace of $\mathbb{F}_2^{2n}$.*

Example 2: 4-decompositions of bent functions

The representation $f = (f)_{a \in \mathbb{F}_2^2}$ can be written as $f = (f_{00}, f_{01}, f_{10}, f_{11})$.

This is known as bent 4-decompositions $f_0 || f_1 || f_2 || f_3$.

Corollary 18

Let $f = (f_{00}, f_{01}, f_{10}, f_{11}) \in \mathcal{B}_{2n}$, where $n \geq 2$. Then

- $f \notin \widetilde{\mathcal{M}}_{2n,2} \iff$ either all $f_{00}, f_{01}, f_{10}, f_{11}$ are bent functions or their Walsh–Hadamard spectrum is **five-valued**;
- $f \in \widetilde{\mathcal{M}}_{2n,2} \iff$ all $f_{00}, f_{01}, f_{10}, f_{11}$ have **three-valued** Walsh–Hadamard spectrum.

The corollary describes all possible cases of representing $f = (f_{00}, f_{01}, f_{10}, f_{11}) \in \mathcal{B}_{2n}$.

We recall that one of this case is called the **iterative construction** (A. Canteaut, P. Charpin, 2002; N. Tokareva, 2011): for bent functions f_{00}, f_{01}, f_{10} ,

$$f = (f_{00}, f_{01}, f_{10}, f_{11}) \in \mathcal{B}_{2n+2} \iff f_{11} \text{ is a bent function and } \widetilde{f_{00}} \oplus \widetilde{f_{01}} \oplus \widetilde{f_{10}} \oplus \widetilde{f_{11}} = 1.$$

Thank you for your attention!