

On the cardinality of some classes generated by Maiorana–McFarland bent functions

N. A. Kolomeec, D. A. Bykov

Novosibirsk State University
Novosibirsk, Russia

June 3, 2025

The 14th Workshop on Current Trends in Cryptology
CTCrypt 2025
Veliky Novgorod 2025

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

$\text{dist}(f, g)$ — 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**, $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$

$\text{Ind}_D : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is the **characteristic function** of $D \subseteq \mathbb{F}_2^n$

$a \oplus D = \{a \oplus x : x \in D\}$

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

Coordinates $I = \{i_1, \dots, i_k\}$, where $1 \leq i_1 < i_2 < \dots < i_k \leq n$; also, $\bar{I} = \{1, \dots, n\} \setminus I$

$x \in \mathbb{F}_2^n$ to $\mathbb{F}_2^k$: $x_I = (x_{i_1}, \dots, x_{i_k})$

$y \in \mathbb{F}_2^k$ to $\mathbb{F}_2^n$: $y^I = x$, where $x_I = y$ and $x_j = 0$ for $j \notin I$



Nonlinearity of $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is the Hamming distance between it and the closest affine function in n variables

Bent functions are maximal nonlinear Boolean functions in even number of 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**

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

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

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

This is of the «primary» constructions of bent functions

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

$$|\mathcal{M}_{2n}| = 2^n! 2^{2^n} = \sqrt{2\pi} 2^{n2^n - (\log_2 e - 1)2^n + n/2} (1 + o(1))$$

A secondary construction that uses affine subspaces

Let us define **the set** $\mathcal{N}(f)$ consisting of all

$f \oplus \text{Ind}_U$, where

- f is a bent function in $2n$ variables
- U is a n -dimensional affine subspace of $\mathbb{F}_2^{2n}$ such that f is affine on U

f is **affine on** U if $f|_U = \ell|_U$ for some affine $\ell : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2$

This construction was proposed by **J. F. Dillon** (1974)

$\mathcal{N}(f)$ are all bent functions at the minimum distance 2^n from f (2009)

The classes $\widehat{\mathcal{M}}_{2n}$ and $\mathcal{N}(\mathcal{M}_{2n})$ are determined by

$$\widehat{\mathcal{M}}_{2n} = \bigcup_{f \in \mathcal{M}_{2n}} \mathcal{N}(f) \text{ and } \mathcal{N}(\mathcal{M}_{2n}) = \widehat{\mathcal{M}}_{2n} \setminus \mathcal{M}_{2n}$$

These classes can be determined not only for $\mathcal{M}_{2n}$

The extended-affine equivalence generates $\mathcal{M}_{2n}^\#$ containing all

$$f(xA \oplus a) \oplus \ell(x), \text{ where}$$

- $f \in \mathcal{M}_{2n}^\#$
- A is an invertible $2n \times 2n$ matrix over $\mathbb{F}_2$ and $a \in \mathbb{F}_2^{2n}$
- $\ell : \mathbb{F}_2^{2n} \rightarrow \mathbb{F}_2$ is affine

Again, this construction can be determined for any class of bent function

The constructions **commute**: $\widehat{\mathcal{M}_{2n}^\#} = \widehat{\mathcal{M}_{2n}}^\#$

We are interested in $\widehat{\mathcal{M}_{2n}}$, $\mathcal{M}_{2n}^\#$ and $\widehat{\mathcal{M}_{2n}}^\#$; we **study** $\mathcal{N}(f)$ and $\mathcal{N}(\mathcal{M}_{2n})$ because of

$$|\widehat{\mathcal{M}_{2n}}| = |\mathcal{N}(\mathcal{M}_{2n})| + |\mathcal{M}_{2n}| \text{ and } |\widehat{\mathcal{M}_{2n}}^\#| = |\mathcal{N}(\mathcal{M}_{2n}^\#)| + |\mathcal{M}_{2n}^\#|$$

An upper bound for $|\mathcal{M}_{2n}^\#|$ is

$$|\mathcal{M}_{2n}^\#| \leq (2^{2n} - 2^0) \cdot \dots \cdot (2^{2n} - 2^{2n-1}) |\mathcal{M}_{2n}|$$

since the class $\mathcal{M}_{2n}$ is closed relative to adding affine function and translations of arguments

An upper bound for $|\widehat{\mathcal{M}}_{2n}|$ is

$$|\widehat{\mathcal{M}}_{2n}| \leq 2^n(2^1 + 1) \cdot \dots \cdot (2^n + 1) |\mathcal{M}_{2n}|$$

This follows from the fact that quadratic bent functions have $\mathcal{N}(f)$ of maximum possible size among all bent functions (2014)

The considered extensions of $\mathcal{M}_{2n}$:

- $\mathcal{N}(\mathcal{M}_{2n})$: the closest bent functions to the class $\mathcal{M}_{2n}$
- $\widehat{\mathcal{M}}_{2n}$: the union of $\mathcal{N}(\mathcal{M}_{2n})$ and $\mathcal{M}_{2n}$
- $\mathcal{M}_{2n}^\#$: the completed Maiorana–McFarland class
- $\mathcal{N}(\mathcal{M}_{2n}^\#)$: the closest bent functions to the class $\mathcal{M}_{2n}^\#$
- $\widehat{\mathcal{M}}_{2n}^\#$: the union of $\mathcal{N}(\mathcal{M}_{2n}^\#)$ and $\mathcal{M}_{2n}^\#$

The base: studying $\mathcal{N}(f)$

The connection: the affinity on n -dimensional affine subspaces of $\mathbb{F}_2^{2n}$

Any bent function from **the Maiorana–McFarland class** $\mathcal{M}_{2n}$

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

is affine on each coset of $\mathbb{F}_2^n \times \{0\}$:

$$f(x, 0 \dots 00) = \langle x, \pi(0 \dots 00) \rangle \oplus \varphi(0 \dots 00)$$

$$f(x, 0 \dots 01) = \langle x, \pi(0 \dots 01) \rangle \oplus \varphi(0 \dots 01)$$

$$\vdots$$

$$f(x, 1 \dots 11) = \langle x, \pi(1 \dots 11) \rangle \oplus \varphi(1 \dots 11)$$

There are 2^n «natural» n -dimensional affine subspaces of $\mathbb{F}_2^{2n}$ such that f is affine on them (in fact, there are at least ℓ_{2n} such subspaces)

A question: what is the number of such affine subspaces in total? The answer is $|\mathcal{N}(f)|$

How to construct $\mathcal{N}(f)$?

$\mathcal{A}_{n,k}$ is the set of all k -dimensional affine subspaces of $\mathbb{F}_2^n$

$I = \{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ is called an **information set** of $L \in \mathcal{A}_{n,k}$ if

$$\{(x_{i_1}, \dots, x_{i_k}) : x \in L\} = \mathbb{F}_2^k.$$

Such I can be found for any $L \in \mathcal{A}_{n,k}$ using Gaussian elimination

Any coset of $L \in [\mathcal{A}_{n,k}]$ can be uniquely determined as $a^{\bar{I}} \oplus L$, where $a \in \mathbb{F}_2^{n-k}$

$\mathcal{I}$ is some **arbitrary fixed** mapping that for $L \in \mathcal{A}_{n,k}$ gives us its information set $I = \mathcal{I}(L)$

Proposition 1

Any $U \in \mathcal{A}_{2n,n}$ can be uniquely expressed as

$$\mathcal{U}_n^{\mathcal{I}}(L, R, H) = \{(H^{\mathcal{I}(R^\perp)}(y) \oplus z, y) : y \in L, z \in R\},$$

where $L \in \mathcal{A}_{n,k}$, $R \in [\mathcal{A}_{n,n-k}]$, and $H : L \rightarrow \mathbb{F}_2^k$ is affine, $k \in \{0, \dots, n\}$.

Theorem 1

Let $f_{\pi,\varphi} \in \mathcal{M}_{2n}$. Then $\mathcal{N}(f_{\pi,\varphi})$ consists of all $f_{\pi,\varphi} \oplus \text{Ind}_{\mathcal{U}_n^{\mathcal{I}}(L, [\pi(L)]^\perp, H)}$, where

- ① L and $\pi(L)$ are k -dimensional affine subspaces of $\mathbb{F}_2^n$,
- ② $H : L \rightarrow \mathbb{F}_2^k$ is affine,
- ③ $\langle H(x), \pi_I(x) \rangle \oplus \varphi(x)$ is affine on L , where $I = \mathcal{I}([\pi(L)])$.

Moreover, distinct (L, H) correspond to distinct bent functions.

Proposition 2 (2023)

Let $f \in \mathcal{M}_{2n}$. Then $|\mathcal{N}(f) \cap \mathcal{M}_{2n}| = \ell_{2n}$, where

$$\ell_{2n} = 2^{2n+1} - 2^n.$$

Moreover, the set $\mathcal{N}(f) \cap \mathcal{M}_{2n}$ correspond to all bent functions from the case of $\dim L \leq 1$.

The affinity of bent functions from $\mathcal{M}_{2n}$ on affine subspaces

The average $|\mathcal{N}(f)|$ among $f \in \mathcal{M}_{2n}$ is

$$E(\mathcal{M}_{2n}) = \frac{1}{|\mathcal{M}_{2n}|} \sum_{f \in \mathcal{M}_{2n}} |\mathcal{N}(f)|.$$

This is the average number of n -dimensional affine subspaces of $\mathbb{F}_2^{2n}$ such that $f \in \mathcal{M}_{2n}$ is affine on them.

Theorem 2

$$E(\mathcal{M}_{2n}) = \ell_{2n} + \sum_{k=2}^n (\mathcal{S}_n^k)^2 \frac{2^{k^2+2n+1} 2^k! (2^n - 2^k)!}{2^{2^k} 2^n!}.$$

Corollary 3

$$E(\mathcal{M}_{2n}) = \frac{10}{3}2^{2n} - 2^n + \frac{8}{3} + \frac{8}{2^n - 3} + 2^{(n+1)^2 - 2^n} + C_n, \text{ where } n \geq 2.$$

$2n$	C_n
8	17.9020979020979034
10	9.3590067076487955
12	7.2034599713804699
14	6.3945141111150132
16	6.0400809074314523
18	5.8737987726531991
20	5.7932190779699999
22	5.7535493917318199
24	5.7338671451801089

Corollary 4

The following estimation is correct for $n \geq 5$: $E(\mathcal{M}_{2n}) < \frac{10}{3}2^{2n} - 2^n + 29$.

Corollary 5

The following expressions are correct:

$$E(\mathcal{M}_{2n}) = \frac{10}{3}2^{2n} - 2^n + \frac{176}{21} + o(1),$$

$$E(\mathcal{M}_{2n}) = \ell_{2n} + \frac{4}{3}2^{2n} + \frac{176}{21} + o(1),$$

$$E(\mathcal{M}_{2n}) = \frac{5}{3}\ell_{2n} + \frac{2}{3}2^n + \frac{176}{21} + o(1).$$

$2n$	$E(\mathcal{M}_{2n})$	$\frac{10}{3}2^{2n}$
2	6	$13 + \frac{1}{3}$
4	60	$53 + \frac{1}{3}$
6	$465 + \frac{3}{5}$	$213 + \frac{1}{3}$
8	$1370 + \frac{74}{143}$	$853 + \frac{1}{3}$

Remark 1

It is known that there exists $f_n \in \mathcal{M}_{2n}$ such that $|\mathcal{N}(f_n)| = \ell_{2n} + o(\ell_{2n})$ (2024). This means that the average $|\mathcal{N}(f)| = E(\mathcal{M}_{2n})$ is asymptotically $\frac{5}{3}$ times greater than the minimum possible value of $|\mathcal{N}(f)|$.

Remark 2

In average, the construction $f \oplus \text{Ind}_U$, where U is n -dimensional affine subspace of $\mathbb{F}_2^{2n}$, generates $\frac{5}{3}2^{2n+1}$ bent functions for a given $f \in \mathcal{M}_{2n}$.

It is slightly more bent functions than 2^{2n+1} that are generated by trivial

$$f \oplus \ell, \text{ where } \ell \text{ is affine.}$$

This construction uses affine subspaces of $\mathbb{F}_2^{2n}$ whose dimensions are 0, $2n - 1$ and $2n$.

The classes $\mathcal{N}(\mathcal{M}_{2n})$ and $\widehat{\mathcal{M}}_{2n}$

Theorem 6

$|\mathcal{N}(\mathcal{M}_2)| = 0$ and for $n \geq 2$ the following holds:

$$|\mathcal{N}(\mathcal{M}_{2n})| = \left(\frac{2^{n-1}(2^n - 1)(2^n - 2)}{9(2^n - 3)} + \sum_{k=3}^n (\mathcal{S}_n^k)^2 \frac{2^{k^2+2n+1} 2^k! (2^n - 2^k)!}{2^{2^k} 2^n!} \right) |\mathcal{M}_{2n}|.$$

Corollary 7

$$\frac{|\mathcal{N}(\mathcal{M}_{2n})|}{|\mathcal{M}_{2n}|} = \frac{1}{18} 2^{2n} + \frac{1}{9} + \frac{1}{3 \cdot 2^n - 9} + 2^{(n+1)^2 - 2^n} + C_n \text{ for } n \geq 2.$$

Corollary 8

$$|\mathcal{N}(\mathcal{M}_{2n})| = \left(\frac{1}{18} 2^{2n} + \frac{367}{63} \right) |\mathcal{M}_{2n}| + o(|\mathcal{M}_{2n}|).$$

Remark 3

Since $|\widehat{\mathcal{M}}_{2n}| = |\mathcal{N}(\mathcal{M}_{2n})| + |\mathcal{M}_{2n}|$, expressions for $|\mathcal{N}(\mathcal{M}_{2n})|$ can be used for $|\widehat{\mathcal{M}}_{2n}|$.
 For instance, $|\widehat{\mathcal{M}}_{2n}| = \left(\frac{1}{18}2^{2n} + \frac{430}{63}\right)|\mathcal{M}_{2n}| + o(|\mathcal{M}_{2n}|)$.

$2n$	$ \mathcal{M}_{2n} $	$ \mathcal{N}(\mathcal{M}_{2n}) $	$ \widehat{\mathcal{M}}_{2n} $	$ \mathcal{B}_{2n} $
2	8	0	8	8
4	384	512	896	896
6	$\approx 2^{23.299}$	$\approx 2^{31.320}$	$\approx 2^{31.326}$	$\approx 2^{32.337}$
8	$\approx 2^{60.250}$	$\approx 2^{69.338}$	$\approx 2^{69.341}$	$\approx 2^{106.291}$

We note that

- $\widehat{\mathcal{M}}_2 = \mathcal{B}_2$
- $\widehat{\mathcal{M}}_4 = \mathcal{B}_4$
- almost half of bent functions from $\mathcal{B}_6$ belong to $\widehat{\mathcal{M}}_6$

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

The class $\mathcal{M}_{2n}^\#$

Let us introduce ϑ_{2n} :

$$\vartheta_{2n} = \sum_{k=0}^{n-1} (\mathcal{S}_n^k)^2 2^{(n-k)^2} 2^k! 2^{(2n-2k+1)2^k} \prod_{i=0}^{n-k-1} (2^{n-k} - 2^i)^{2^k},$$

where $\mathcal{S}_n^k$ is 2-binomial coefficient:

$$\mathcal{S}_n^k = \prod_{i=0}^{k-1} \frac{1 - 2^{n-i}}{1 - 2^{k-i}}.$$

This is the number of all k -dimensional linear subspaces of $\mathbb{F}_2^n$.

Theorem 9

The following estimations are correct:

$$\mathcal{S}_{2n}^n |\mathcal{M}_{2n}| - \mathcal{S}_{2n}^n \vartheta_{2n} \leq |\mathcal{M}_{2n}^\#| \leq \mathcal{S}_{2n}^n |\mathcal{M}_{2n}|.$$

Logarithms of the bounds for $|\mathcal{M}_{2n}^\#|$ from Theorem 9

$2n$	$\log_2(\text{LB of } \mathcal{M}_{2n}^\#)$	$\log_2(\text{UB of } \mathcal{M}_{2n}^\#)$	$\log_2 \mathcal{M}_{2n}^\# $
2	—	4.5849625007211561	3
4	—	13.7142455176661233	≈ 9.807
6	—	33.7452574251038300	≈ 32.337
8	77.8643407121388975	77.8654468090131644	≈ 77.865
10	176.3659472814000253	176.3659472814000537	?
12	397.7422108473157323	397.7422108473157323	?
14	894.9311554368803172	894.9311554368803172	?
16	2005.7769476615776512	2005.7769476615776512	?

Classification of $\mathcal{M}_8^\#$ was obtained by **P. Langevin** and **A. Polujan** (2024).

Proposition 3

The following lower bound is correct: $(2^n - 1)^2 2^{3 \cdot 2^{n-1} + 1} 2^{n-1}! \leq \vartheta_{2n}$. Also,

$$\vartheta_{2n} < 2^{3 \cdot 2^{n-1} + 2n + 1} 2^{n-1}! \text{ for any } n \geq 7. \quad (1)$$

Moreover, $\vartheta_{2n} = 2^{3 \cdot 2^{n-1} + 2n + 1} 2^{n-1}! (1 - o(1))$ and

$$|\mathcal{M}_{2n}^\#| > \mathcal{S}_{2n}^n (2^{2^n} 2^n! - 2^{3 \cdot 2^{n-1} + 2n + 1} 2^{n-1}!) \text{ for } n \geq 5.$$

Corollary 10

The following is correct: $|\mathcal{M}_{2n}^\#| = \mathcal{S}_{2n}^n |\mathcal{M}_{2n}| - o(2^n!)$. Note that

$$\mathcal{S}_{2n}^n = 2^{n^2} \prod_{i=0}^{n-1} \frac{1 - 2^{i-2n}}{1 - 2^{i-n}} \approx 3.46 \cdot 2^{n^2} \text{ for } n \geq 10.$$

$\mathcal{M}$ -subspaces of the function $f \in \mathcal{M}_{2n}^\#$ are

$$\mathcal{M}(f) = \{L \in \mathcal{A}_{2n,n} : f \text{ is affine on each coset of } L\}.$$

They are important for constructing bent functions outside $\mathcal{M}_{2n}^\#$ (**A. Polujan, A. Pott, E. Pasalic** et al., 2020 - 2025).

As a rule, the most interesting case is $|\mathcal{M}(f)| = 1$.

Corollary 11

The average value of $|\mathcal{M}(f)|$ for $f \in \mathcal{M}_{2n}$ is equal to the following:

$$\frac{1}{|\mathcal{M}_{2n}|} \sum_{f \in \mathcal{M}_{2n}} |\mathcal{M}(f)| = 1 + \frac{\vartheta_{2n}}{|\mathcal{M}_{2n}|}.$$

$2n$	The average $ \mathcal{M}(f) $	$2n$	The average $ \mathcal{M}(f) $
2	3	10	$1 + 2^{-46.501079}$
4	15	12	$1 + 2^{-133.377320}$
6	8.6	14	$1 + 2^{-341.189209}$
8	$1 + 2^{-10.349626}$	16	$1 + 2^{-822.845858}$

Corollary 12

The equality $|\mathcal{M}(f)| = 1$ holds for almost all bent functions from $\mathcal{M}_{2n}$ ($\mathcal{M}_{2n}^\#$). More precisely, there are at least

$$|\mathcal{M}_{2n}| - \vartheta_{2n} \text{ and } |\mathcal{M}_{2n}^\#| - \mathcal{S}_{2n}^n \vartheta_{2n}$$

bent functions $f \in \mathcal{M}_{2n}$ and $f \in \mathcal{M}_{2n}^\#$ respectively with $|\mathcal{M}(f)| = 1$.

The class $\widehat{\mathcal{M}}_{2n}^\#$

The average $|\mathcal{N}(f)|$ among $f \in \mathcal{M}_{2n}^\#$, $\mathcal{N}(\mathcal{M}_{2n}^\#)$ and $|\widehat{\mathcal{M}}_{2n}^\#|$

We estimate the $|\mathcal{N}(\mathcal{M}_{2n}^\#)|$ using

$$E(\mathcal{M}_{2n}^\#) = \frac{1}{|\mathcal{M}_{2n}^\#|} \sum_{f \in \mathcal{M}_{2n}^\#} |\mathcal{N}(f)|.$$

Theorem 13

Let $n \geq 5$. Then $E(\mathcal{M}_{2n}^\#) < E(\mathcal{M}_{2n})$. Moreover, $E(\mathcal{M}_{2n}^\#) = E(\mathcal{M}_{2n}) - o(1)$.

Conjecture 1 (Informal)

The Maiorana–McFarland class $\mathcal{M}_{2n}$ has the maximum possible $E(\mathcal{M}_{2n})$ among big enough classes of bent functions.

Corollary 14

Let $n \geq 5$. Then $|\mathcal{N}(\mathcal{M}_{2n}^\#)| < (E(\mathcal{M}_{2n}) - \ell_{2n})|\mathcal{M}_{2n}^\#|$. In particular,

$$|\mathcal{N}(\mathcal{M}_{2n}^\#)| < \left(\frac{4}{3}2^{2n} + 29\right)|\mathcal{M}_{2n}^\#| \text{ and } |\widehat{\mathcal{M}}_{2n}^\#| < \left(\frac{4}{3}2^{2n} + 30\right)|\mathcal{M}_{2n}^\#|.$$

Thank you for your attention!