УДК 519.7 DOI 10.17223/2226308X/15/6

# О НИЖНЕЙ ОЦЕНКЕ ЧИСЛА БЕНТ-ФУНКЦИЙ НА МИНИМАЛЬНОМ РАССТОЯНИИ ОТ БЕНТ-ФУНКЦИЙ ИЗ КЛАССА МЭЙОРАНА — МАКФАРЛАНДА[1]

Д. А. Быков

Исследуется построение бент-функций на некотором расстоянии от заданной бент-функции. Для функции $f$ из класса Мэйорана — МакФарланда $\mathcal{M}_{2n}$ доказан критерий того, что функция, полученная из $f$ прибавлением индикатора аффинного подпространства размерности $n$, является бент-функцией. Показано, что для простых $n \geqslant 5$ достигается нижняя оценка $2^{2n+1} - 2^n$ числа бент-функций на минимальном расстоянии от бент-функций из класса $\mathcal{M}_{2n}$. Найдены бент-функции, для которых оценка точна. Показано, что эта нижняя оценка не достигается для бент-функций из класса $\mathcal{M}_{2n}$, где перестановка, по которой построена бент-функция, не является APN-функцией. Для некоторых расстояний, в частности $2^{2n-1}$, получены нижние оценки числа бент-функций из класса $\mathcal{M}_{2n}$ на этих расстояниях от бент-функций из класса $\mathcal{C}$.

**Ключевые слова:** *бент-функции, булевы функции, минимальное расстояние, класс Мэйорана — МакФарланда, нижние оценки.*

## Введение

Пусть $\mathbb{F}_2^n$ — линейное пространство над полем $\mathbb{F}_2$, состоящее из двоичных векторов размерности $n$. Множество всех *булевых функций* от $n$ переменных $f : \mathbb{F}_2^n \to \mathbb{F}_2$ обозначим через $\mathcal{F}_n$. *Расстоянием* $\operatorname{dist}(f, g)$ между двумя булевыми функциями $f, g \in \mathcal{F}_n$ называется число позиций, в которых векторы значений этих функций различаются. Булева функция от чётного числа переменных $2n$, расстояние от которой до множества всех аффинных функций максимально и равно $2^{2n-1} - 2^{n-1}$, называется *бент-функцией*. Везде далее будем рассматривать бент-функции от $2n$ переменных. Обозначим множество всех бент-функций от $2n$ переменных через $\mathcal{B}_{2n}$. Класс бент-функций Мэйорана — МакФарланда $\mathcal{M}_{2n}$ состоит из функций вида

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y),$$

где $\varphi \in \mathcal{F}_n$ и $\pi$ — перестановка на $\mathbb{F}_2^n$. Напомним, что функции $f, g \in \mathcal{F}_n$ называются *EA-эквивалентными*, если существуют аффинная функция $h$, невырожденная матрица $A$ размера $n \times n$ с элементами из $\mathbb{F}_2$ и $b \in \mathbb{F}_2^n$, такие, что $f(x) = g(xA \oplus b) \oplus h(x)$ для всех $x \in \mathbb{F}_2^n$. Через *индикатор* $\operatorname{Ind}_S$ обозначим характеристическую функцию множества $S \subseteq \mathbb{F}_2^n$.

Бент-функции введены О. Ротхаусом в [1]. Они интересны как своими экстремальными значениями нелинейности, так и приложениями в криптографии, теории кодирования, теории символьных последовательностей. Однако есть много открытых вопросов об устройстве множества всех бент-функций, о соотнесении различных известных классов бент-функций. Например, классы $\mathcal{C}$ и $\mathcal{D}$, введённые в [2], лежат вне замыкания класса $\mathcal{M}_{2n}$ относительно EA-эквивалентности. Но это известно благодаря построенным примерам [2, 3] и непонятно, какая часть бент-функций из $\mathcal{C}$ и $\mathcal{D}$ лежит вне замыкания $\mathcal{M}_{2n}$.

Для построения бент-функции на некотором расстоянии от исходной бент-функции $f \in \mathcal{B}_{2n}$ можно воспользоваться универсальной конструкцией $f \mapsto f \oplus \operatorname{Ind}_S$. При этом

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).

часто удобно рассматривать не произвольное множество $S \subseteq \mathbb{F}_2^{2n}$, а, например, некоторое подпространство $U$. Так, в работе [2] для случая, когда $U$ — аффинное подпространство $\mathbb{F}_2^{2n}$ размерности $n$, доказано, что $f \oplus \mathrm{Ind}_U$ — бент-функция.

Для двух различных $f, g \in \mathcal{B}_{2n}$ известно, что $\mathrm{dist}(f, g) \geqslant 2^n$. В [4] показано, что все бент-функции на минимально возможном расстоянии $2^n$ от заданной бент-функции $f$ могут быть выражены как $f \oplus \mathrm{Ind}_U$, где $U$ — аффинное подпространство $\mathbb{F}_2^{2n}$, $\dim U = n$. Иными словами, в поиске всех бент-функций на расстоянии $2^n$ достаточно ограничиться прибавлением индикатора аффинного подпространства размерности $n$.

В [5] приведён вид всех бент-функций из $\mathcal{M}_{2n}$, лежащих на расстоянии $2^n$ от исходной бент-функции из $\mathcal{M}_{2n}$. Число таких бент-функций может быть использовано в качестве следующей оценки.

**Утверждение 1** (Н. Коломеец, 2017). Число всех бент-функций на минимальном расстоянии от бент-функций из $\mathcal{M}_{2n}$ можно оценить снизу как $2^{2n+1} - 2^n$. При этом все бент-функции, учитывающиеся в этой оценке, также лежат в классе $\mathcal{M}_{2n}$.

## 1. Число бент-функций на минимально возможном расстоянии $2^n$ от бент-функций из $\mathcal{M}_{2n}$

Рассмотрим $f \in \mathcal{M}_{2n}$ и конструкцию $f \mapsto f \oplus \mathrm{Ind}_U$, где $U$ — аффинное подпространство $\mathbb{F}_2^{2n}$, $\dim U = n$. Сначала построим критерий того, что $f \oplus \mathrm{Ind}_U$ является бент-функцией.

Пусть $E$ — линейное подпространство $\mathbb{F}_2^n$ размерности $k$. Тогда для $E$ существует единственная GJB-матрица $M$ — приведённая ступенчатая матрица полного ранга размера $k \times n$, строки которой составляют базис $E$. Через $\langle M \rangle$ обозначим линейную оболочку строк матрицы $M$.

В следующей теореме приведён критерий для функций $f(x, y) = \langle y, \pi(x) \rangle \oplus \varphi(x)$, другими словами, $f \notin \mathcal{M}_{2n}$, а $h(x, y) = f(y, x) \in \mathcal{M}_{2n}$. Такой переход нужен для удобного представления базисов подпространств с помощью GJB-матриц. Критерий для бент-функций из $\mathcal{M}_{2n}$ является следствием этой теоремы.

**Теорема 1.** Пусть $f(x, y) = \langle y, \pi(x) \rangle \oplus \varphi(x)$, такая, что $h(x, y) = f(y, x) \in \mathcal{M}_{2n}$; $U = (a, b) \oplus E$ — аффинное подпространство $\mathbb{F}_2^{2n}$, $\dim U = n$, где $a, b \in \mathbb{F}_2^n$; линейное подпространство $E$ имеет GJB-матрицу вида

$$M = \left( \begin{array}{c|c} L & T \\ \hline 0 & R \end{array} \right),$$

где $L$ является GJB-матрицей размера $(n - k) \times n$. Тогда

$$g(x, y) = \langle y, \pi(x) \rangle \oplus \varphi(x) \oplus \mathrm{Ind}_U(x, y)$$

является бент-функцией, если и только если выполнены следующие условия:

1) $\pi(a \oplus \langle L \rangle) = \pi(a) \oplus \langle R \rangle^{\perp}$;
2) $\langle uT \oplus b, \pi(uL \oplus a) \rangle \oplus \varphi(uL \oplus a)$ — аффинная функция от переменных $u = (u_1, \ldots, u_{n-k}) \in \mathbb{F}_2^{n-k}$.

Отметим, что в частном случае $U = U_1 \times U_2$, где $\dim U = n$, $U_1, U_2$ — аффинные подпространства $\mathbb{F}_2^n$, теорему 1 можно переписать в более простом виде. В определении класса $\mathcal{D}$ используются бент-функции $f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$ с $\varphi \equiv 0$, к которым прибавляется $\mathrm{Ind}_E$, где $E = E_1 \times E_2$; $\dim E = n$; $E_1, E_2$ — линейные подпространства $\mathbb{F}_2^n$. Поэтому теорема 1 обобщает определение класса $\mathcal{D}$, так как даёт критерий на бент-функции при произвольной $\varphi$ и аффинных подпространствах $U_1, U_2$.

Функция $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ называется *APN-функцией*, если для любых $a \neq 0, b \in \mathbb{F}_2^n$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более двух решений. Рассмотрим случай, когда нижняя оценка гарантированно не достигается.

**Теорема 2.** Пусть $f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$, где $\pi$ — перестановка, не являющаяся APN-функцией. Тогда число бент-функций, лежащих на минимальном расстоянии от $f$, строго больше нижней оценки $2^{2n+1} - 2^n$.

Таким образом, для функций $f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$, где $\pi$ не является APN-перестановкой, существует подпространство $U$ размерности $n$, такое, что бент-функция $f \oplus \mathrm{Ind}_U \notin \mathcal{M}_{2n}$.

Далее будем представлять булевы функции как функции из $\mathbb{F}_{2^n}$ в $\mathbb{F}_2$, зафиксировав в поле $\mathbb{F}_{2^n}$ некоторый базис над $\mathbb{F}_2$. Функция $\mathrm{tr} : \mathbb{F}_{2^n} \to \mathbb{F}_2$, определённая как $\mathrm{tr}(x) = x^{2^0} + x^{2^1} + \ldots + x^{2^{n-1}}$, называется *следом*. Любая $f \in \mathcal{F}_n$ представима в виде $f = \mathrm{tr}\left(\sum\limits_{k=0}^{2^n-1} c_k x^k\right)$. Такое представление не единственно, но его можно сделать таковым [6]. Функции класса $\mathcal{M}_{2n}$ в этом представлении записываются как

$$f(x, y) = \mathrm{tr}(x\pi(y)) + \varphi(y),$$

где $\varphi : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$; $\pi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — взаимно однозначная функция; $x, y \in \mathbb{F}_{2^n}$. В поле $\mathbb{F}_{2^n}$ функция обращения элемента $F(x) = x^{2^n-2}$ является взаимно однозначной. Отметим, что при нечётных $n$ это APN-перестановка.

**Теорема 3.** Пусть $n \geqslant 5$ — простое; функция $f(x, y) = \mathrm{tr}(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$, $x, y \in \mathbb{F}_{2^n}$, такова, что $\varphi$ не является функцией вида

$$\vartheta(y) = c_0 + \mathrm{tr}(\beta_1 y^{2^1-1} + \beta_2 y^{2^2-1} + \ldots + \beta_{n-1} y^{2^{n-1}-1}) + c_{2^n-1} y^{2^n-1} \in \mathcal{F}_n,$$

где $y \in \mathbb{F}_{2^n}$, $c_0, c_{2^n-1} \in \mathbb{F}_2$, $\beta_1, \beta_2, \ldots, \beta_{n-1} \in \mathbb{F}_{2^n}$. Тогда для $f$ существует ровно $2^{2n+1} - 2^n$ бент-функций, лежащих на минимальном расстоянии от неё, т. е. рассматриваемая оценка является достижимой.

**Пример 1.** Условию теоремы 3 при любом простом $n \geqslant 5$ удовлетворяют, в частности, функции $f(x, y) = \mathrm{tr}(xy^{2^n-2}) + \mathrm{tr}(y^5)$ и $g(x, y) = \mathrm{tr}(xy^{2^n-2}) + \mathrm{tr}(y^{11})$.

Не составляет труда посчитать число функций $f$ из теоремы 3.

**Следствие 1.** Пусть $n \geqslant 5$ — простое. Тогда число функций из $\mathcal{M}_{2n}$, для которых достигается нижняя оценка $2^{2n+1} - 2^n$, не меньше $2^{2^n} - 2^{n^2-n+2}$.

Известны некоторые бент-функции, для которых точно посчитано количество бент-функций на минимально возможном расстоянии $2^n$ от них:

— это количество равно нулю для неслабонормальных бент-функций. Такие бент-функции рассматривались в работах [7, 8];

— это количество равно $2^n(2^1+1)\ldots(2^n+1)$ для квадратичных бент-функций [9]. Это значение является также верхней оценкой числа бент-функций на расстоянии $2^n$ от исходной бент-функции, при этом достигается она только для квадратичных бент-функций [10].

Теорема 3 даёт точное число бент-функций, лежащих на минимальном расстоянии от ещё ряда бент-функций из $\mathcal{M}_{2n}$.

## 2. Число бент-функций из $\mathcal{M}_{2n}$ на некотором расстоянии от бент-функций из $\mathcal{C}$

Класс $\mathcal{C}$ введён в работе [2], он состоит из функций вида

$$f(x,y) = \langle x, \pi(y)\rangle \oplus \mathrm{Ind}_{L^\perp}(x),$$

где $L$ — линейное подпространство $\mathbb{F}_2^n$ и $\pi$ — перестановка на $\mathbb{F}_2^n$, такая, что для любого $a \in \mathbb{F}_2^n$ множество $\pi^{-1}(a \oplus L)$ — аффинное подпространство.

Рассмотрим конструкцию $f \mapsto f \oplus \mathrm{Ind}_S$ для бент-функций $f(x,y) = \langle x, \pi(y)\rangle \oplus \oplus \mathrm{Ind}_{L^\perp}(x) \in \mathcal{C}$ и множеств $S$, не обязательно являющихся подпространствами. В следующей теореме для оценки использованы бент-функции $g(x,y) = \langle x, \tau(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$, такие, что $\tau(y) = \pi(y) \oplus c$, $c \in \mathbb{F}_2^n$. Отметим, что число таких перестановок $\tau$ равно $2^n$ и мало по сравнению с числом всех перестановок $2^n!$.

**Теорема 4.** Количество бент-функций из класса $\mathcal{M}_{2n}$, лежащих на расстоянии $m$ от бент-функций $f(x,y) = \langle x, \pi(y)\rangle \oplus \mathrm{Ind}_{L^\perp}(x) \in \mathcal{C}$ от $2n$ переменных, таких, что $\dim L^\perp = k$, не менее

1) $\binom{2^n}{w}$, если $m \in \{2^k(w(2^{n-k}-2)+2^n) : w = 0,1,\ldots,2^n\}$;
2) $\binom{2^n}{w}(2^{n-k}-1)$, если $m \in \{2^{2n-1} + 2^k(2^n - 2w) : w = 0,1,\ldots,2^n\}$, где $0 \leqslant k < n$.

Если рассмотреть расстояние $2^{2n-1}$ отдельно, то для него можно получить гораздо бóльшую нижнюю оценку, чем даёт предыдущая теорема.

**Теорема 5.** На расстоянии $2^{2n-1}$ от бент-функций из класса $\mathcal{C}$ от $2n$ переменных лежит не менее $2^{2^n}(2^{n-1})!$ бент-функций из класса $\mathcal{M}_{2n}$.

## ЛИТЕРАТУРА


1. *Rothaus O.* On bent functions // J. Comb. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Carlet C.* Two new classes of bent functions // LNCS. 1993. V. 765. P. 77–101.
3. *Zhang F., Cepak N., Pasalic E., and Wei Y.* Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^\#$ // Discr. Appl. Math. 2020. V. 285. P. 458–472.
4. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4(6). С. 5–20.
5. *Kolomeec N.* The graph of minimal distances of bent functions and its properties // Des. Codes Cryptogr. 2017. V. 85. P. 395–410.
6. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
7. *Canteaut A., Daum M., Dobbertin H., and Leander G.* Finding nonnormal bent functions // Discr. Appl. Math. 2006. V. 154. Iss. 2. P. 202–218.
8. *Leander G. and McGuire G.* Construction of bent functions from near-bent functions // J. Comb. Theory. Ser. A. 2009. V. 116. No. 4. P. 960–970.
9. *Коломеец Н. А.* Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретн. анализ и исслед. опер. 2012. Т. 19. Вып. 1. С. 41–58.
10. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии $2^k$ от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. № 3(25). С. 28–39.