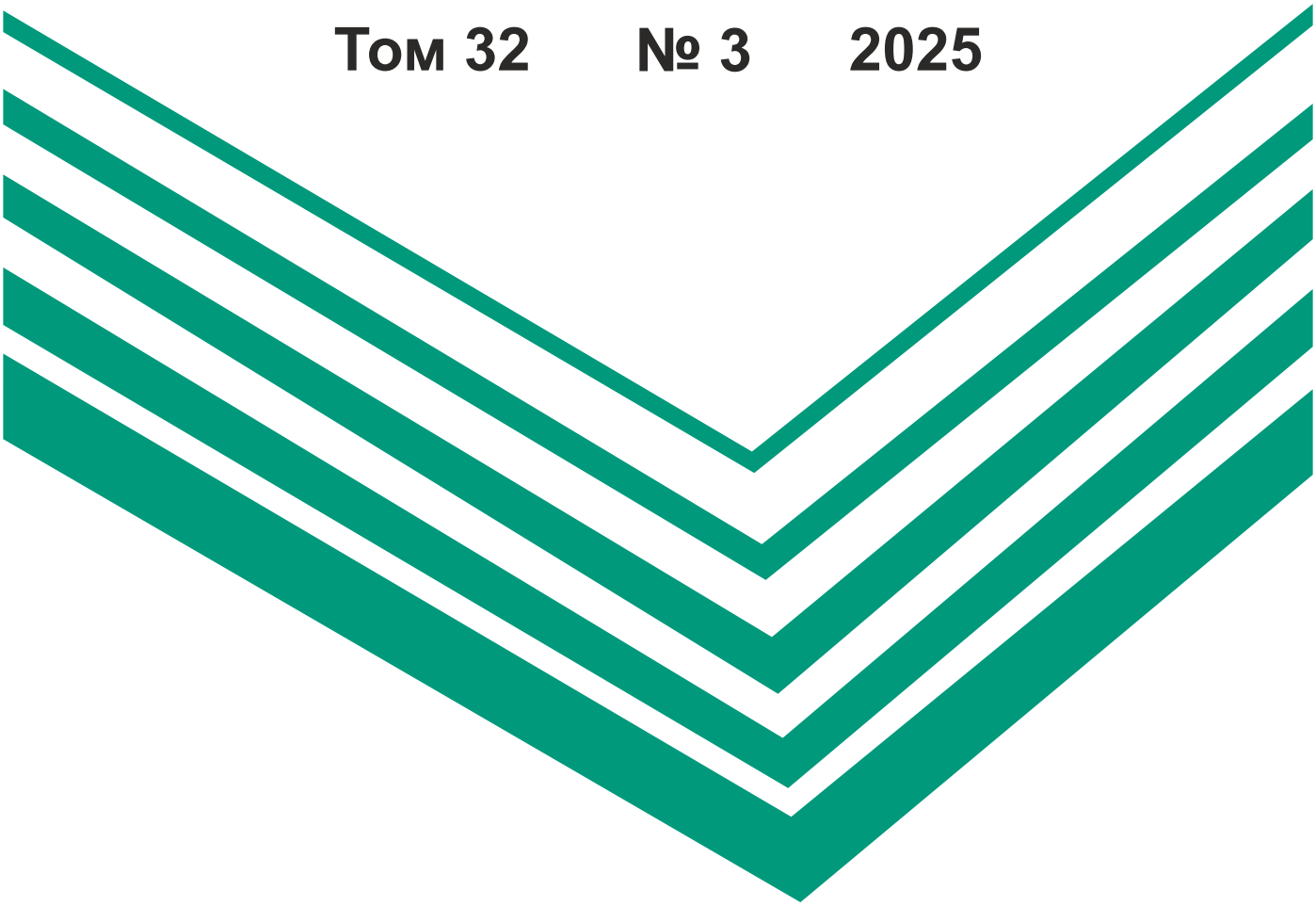
ISSN 2949-5598

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ

Том 32 № 3 2025



Новосибирск
Издательство Института математики

ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2025. Т. 32, № 3. С. 5–42

УДК 519.7 DOI: 10.33048/daio.2025.32.811

О БЛИЖАЙШИХ БЕНТ-ФУНКЦИЯХ К ЗАДАННОЙ БЕНТ-ФУНКЦИИ МЭЙОРАНА — МАКФАРЛАНДА

Д. А. Быков [a], *Н. А. Коломеец* [b]

Новосибирский гос. университет,
ул. Пирогова, 2, 630090 Новосибирск, Россия
E-mail: [a] den.bykov.2000i@gmail.com, [b] nkolomeec@gmail.com

Аннотация. Исследуются бент-функции от $2n$ переменных, ближайшие к заданной функции из класса Мэйорана — МакФарланда. Переформулирован критерий расположения таких бент-функций, и уточнён метод подсчёта их числа. Исследованы функции с числом ближайших бент-функций, близким к его нижней и точной верхней оценкам. Доказано существование бент-функций, у которых число ближайших бент-функций имеет ту же асимптотику, что и нижняя оценка. Приведены примеры функций из класса Мэйорана — МакФарланда, для которых рассчитанное число ближайших бент-функций близко к верхней оценке. Рассматривается также достижимость нижней оценки, а именно, усилены известные необходимые и достаточные условия. Показано, что нижняя оценка достигается при n, равном степени простого числа $p \geqslant 5$, а также при некоторых других n. Приведена полная классификация функций от 6 переменных из класса Мэйорана — МакФарланда по числу ближайших бент-функций. Табл. 1, библиогр. 40.

Ключевые слова: бент-функция, булева функция, аффинное подпространство, минимальное расстояние, класс Мэйорана — МакФарланда.

Введение

Бент-функции — булевы функции от чётного числа переменных, обладающие максимальной нелинейностью — впервые введены в рассмотрение в 1960-х гг. Их название появилось в работе Ротхауса [1], а в СССР В. А. Елисеев и О. П. Степченков называли их минимальными [2]. Бент-функции интересны своими приложениями в криптографии, алгебре, теории кодирования, теории символьных последовательностей и т. д. О них написаны обзоры и книги [2–7], а общую информацию о криптографических свойствах булевых функций можно найти в [8–14].

В данной работе рассматриваются метрические свойства бент-функций, а именно бент-функции, ближайшие относительно метрики Хэмминга к некоторой заданной бент-функции из класса Мэйорана — МакФарланда $\mathcal{M}_{2n}$ от $2n$ переменных, который независимо ввели Мэйорана и МакФарланд, аналогичную конструкцию предложил также В. А. Елисеев (см. [2, 15]). Этот класс состоит из бент-функций вида

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

где π — подстановка на $\mathbb{F}_2^n$, $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2$, и наряду с классом $\mathcal{PS}$ [16] является одной из базовых конструкций бент-функций. Известно [17], что все ближайшие к $f_{\pi,\varphi}$ бент-функции находятся на расстоянии 2^n и имеют вид

$$f_{\pi,\varphi} \oplus \mathrm{Ind}_L, \quad L \in \mathcal{LA}_n(f_{\pi,\varphi}), \tag{1}$$

где $\mathcal{LA}_n(f_{\pi,\varphi})$ — множество всех аффинных подпространств $L \subseteq \mathbb{F}_2^{2n}$ размерности n, на которых $f_{\pi,\varphi}$ аффинна. Конструкция (1), впервые описанная в [16] и применимая к любой бент-функции, позволяет строить бент-функции разных классов, поэтому она интересна и вне метрических свойств. На её основе построен класс $\mathcal{D}$ [18], выходящий за пределы замыканий $\mathcal{M}_{2n}$ и $\mathcal{PS}$ относительно EA-эквивалентности [18–20]. Свойства схожей с (1) конструкции для аффинных подпространств L произвольной размерности рассматривались в [18, 21–24], а построение бент-функций, не принадлежащих замыканию $\mathcal{M}_{2n}$, исследовалось также в [25–27]. Таким образом, мощность $\mathcal{LA}_n(f_{\pi,\varphi})$ характеризует как размер минимальной окрестности $f_{\pi,\varphi}$ (метрические свойства), так и число бент-функций, порождаемых конструкцией (1).

Для $|\mathcal{LA}_n(f_{\pi,\varphi})|$ справедливы оценки

$$\ell_{2n} = 2^{2n+1} - 2^n \leqslant |\mathcal{LA}_n(f_{\pi,\varphi})| \leqslant 2^n(2^1+1)(2^2+1)\dots(2^n+1) = \mathcal{U}_{2n}.$$

Верхняя оценка $\mathcal{U}_{2n}$ верна для произвольной бент-функции и точна: она достигается на всех квадратичных бент-функциях и только на них [29]. Нижняя оценка ℓ_{2n} впервые представлена в [28], она тесно связана и с пересечениями классов: все учтённые в ней бент-функции лежат в $\mathcal{M}_{2n}$, а все неучтённые — вне его [29]. Таким образом, её достижимость влечёт отсутствие ближайших к $f_{\pi,\varphi}$ бент-функций за пределами $\mathcal{M}_{2n}$. Этот вопрос исследуется в [30], где показано, что ℓ_{2n} достижима при простых $n \geqslant 5$. В то же время, для равенства $|\mathcal{LA}_n(f_{\pi,\varphi})| = \ell_{2n}$ необходимо, чтобы π была APN-подстановкой [31]. Однако вопрос существования таких подстановок при чётных $n \geqslant 8$ является открытым (the big APN problem) [32].

В рамках данной работы мы предлагаем ещё одну формулировку критерия для $L \in \mathcal{LA}_n(f_{\pi,\varphi})$ в конструкции (1), используя отличное от [30]

представление аффинных подпространств $\mathbb{F}_2^n \times \mathbb{F}_2^n$, и демонстрируем подсчёт $|\mathcal{LA}_n(f_{\pi,\varphi})|$ для некоторых $f_{\pi,\varphi}$. Например, все функции из $\mathcal{M}_6$ классифицированы по значению $|\mathcal{LA}_3(f_{\pi,\varphi})|$. Результаты позволяют усилить как необходимое, так и достаточное условия достижимости ℓ_{2n}, а также выделить бент-функции с близким к ℓ_{2n} или $\mathcal{U}_{2n}$ размером $\mathcal{LA}_n(f_{\pi,\varphi})$, для которых при $n \to \infty$ имеет место одно из равенств

$$|\mathcal{LA}_n(f_{\pi,\varphi})| = \ell_{2n} + o(\ell_{2n}), \quad |\mathcal{LA}_n(f_{\pi,\varphi})| = \frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n}).$$

Поскольку любая бент-функция $f_{\pi,\varphi} \in \mathcal{M}_{2n}$ «собрана» из 2^n аффинных ограничений на $\mathbb{F}_2^n \times \{y\}$ для $y \in \mathbb{F}_2^n$, функции с $|\mathcal{LA}_n(f_{\pi,\varphi})|$, близким к $\mathcal{U}_{2n}$ (ℓ_{2n}), можно считать наиболее «простыми» («сложными»).

Структура работы следующая. В разд. 1 приводятся необходимые определения. В разд. 2 переформулирован критерий из [30] расположения ближайших бент-функций к $f_{\pi,\varphi} \in \mathcal{M}_{2n}$ в более удобном для вычисления их числа виде (теорема 1). Отличие состоит в представлении аффинных подпространств $\mathbb{F}_2^n \times \mathbb{F}_2^n$, основанном на их пересечении с $\mathbb{F}_2^n \times \{0\}^n$ и проекции на $\{0\}^n \times \mathbb{F}_2^n$ (см. п. 2.1), и использовании специального линейного оператора $\mathcal{G}_\pi^L$ ($\mathcal{G}_\pi$) (п. 2.2), через образ и размер ядра которого выражается число ближайших к $f_{\pi,\varphi}$ бент-функций (следствие 1, см. также теорему 3). Его удобство обусловлено возможностью до определённой степени отделить свойства π от свойств φ. Важно, что допускается представление $f_{\pi,\varphi}$ как над $\mathbb{F}_2^n \times \mathbb{F}_2^n$, так и над $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$: во всех ключевых теоремах предполагается, что $f_{\pi,\varphi}(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y)$, где $\langle\cdot,\cdot\rangle_n$ — произвольная невырожденная симметричная билинейная форма на $\mathbb{F}_2^n$. Доказанная в п. 2.3 теорема 2 упрощает работу с $\mathcal{G}_\pi^L$ с помощью перехода к «естественной» билинейной форме, определённой на $\mathbb{F}_2^{\dim L} \times \mathbb{F}_2^{\dim L}$.

В разд. 3 найдены мощность ядра и образ оператора $\mathcal{G}_\pi$ для некоторых подстановок π: аффинных, зависящих от не более чем трёх переменных (п. 3.1), а также для функции инверсии элементов $\mathbb{F}_{2^n}$ (п. 3.2). Все полученные далее утверждения и теоремы демонстрируют применение результатов из разд. 2 и 3 к конкретным бент-функциям $f_{\pi,\varphi}$.

В разд. 4 изучается достижимость нижней оценки ℓ_{2n} числа ближайших к $f_{\pi,\varphi}$ бент-функций, для этого уточнена общая формула подсчёта их числа (теорема 3). Данная теорема позволила получить как следствие усиление результата [30] о необходимости для π быть APN-подстановкой при $|\mathcal{LA}_n(f_{\pi,\varphi})| = \ell_{2n}$: L и его образ $\pi(L)$ не должны быть одновременно аффинными подпространствами $\mathbb{F}_2^n$ размерности 3 (следствие 2). Усилено и достаточное условие достижимости ℓ_{2n} из [30]: доказано, что оценка гарантированно достигается не только при простых $n \geqslant 5$, но и при любых степенях таких простых чисел (теорема 4 и следствие 3).

В разд. 5 теорема 3 применяется для подсчёта числа ближайших к $f_{\pi,\varphi}$ бент-функций, близкого к его нижней ℓ_{2n} или верхней $\mathcal{U}_{2n}$ оценкам. В п. 5.1 доказано существование функции $f_{\pi,\varphi} \in \mathcal{M}_{2n}$, для которой $|\mathcal{LA}_n(f_{\pi,\varphi})| < 2^{2n+1} + 81 \cdot 2^n - 82$, причём неравенство превращается в равенство $\ell_{2n} + o(\ell_{2n})$ при $n \to \infty$ (теорема 5). Следствием является достижимость оценки ℓ_{2n} при некоторых других n (следствие 5). В качестве π здесь используется функция инверсии элементов $\mathbb{F}_{2^n}$.

В п. 5.2 для $f_\varphi(x, y) = \langle x, y\rangle \oplus \varphi(y)$ приведена формула мощности $\mathcal{LA}_n(f_\varphi)$, использующая нетривиальные параметры φ (следствие 6). Далее для $\varphi_m(y_1, \ldots, y_n) = y_1 \ldots y_m$, где $3 \leqslant m \leqslant n$ дано явное выражение для $|\mathcal{LA}_n(f_{\varphi_m})|$ (следствие 7, см. также утверждение 11 и замечание 4 о расширении класса функций φ). В случаях $m = 3$ и $m = n$ получены краткие формулы, по виду близкие к оценке $\mathcal{U}_{2n}$; из них следует, что при $n \to \infty$ величина $|\mathcal{LA}_n(f_{\varphi_m})|$ имеет порядок $o(\mathcal{U}_{2n})$ и $\frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$ соответственно (следствие 8). Показано также, что бент-функция f_τ, построенная с помощью транспозиции $\tau\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ и тождественно нулевой φ, имеет $|\mathcal{LA}_n(f_\tau)| = |\mathcal{LA}_n(f_{\varphi_n})|$ (утверждение 12 и замечание 5). Выдвинута гипотеза, что это максимальное возможное число ближайших бент-функций для неквадратичной бент-функции (гипотеза 1).

В разд. 6 показано, что из теоремы 3 следует классификация всех $f \in \mathcal{M}_6$ по мощности $\mathcal{LA}_3(f)$, которая в данном случае является полным инвариантом относительно EA-эквивалентности (теорема 6).

1. Определения

1.1. Булевы функции. Пусть $\mathbb{F}_{2^k}$ — конечное поле, состоящее из 2^k элементов, и $\mathbb{F}_2^n = \{(x_1, x_2, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{F}_2\}$ — векторное пространство размерности n над полем $\mathbb{F}_2$, сложение в котором обозначено через $\oplus$. Функция $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от n переменных. Функция $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ называется *векторной булевой функцией* и представляет собой упорядоченный набор m булевых функций от n переменных, каждая из которых называется *координатной*, а их нетривиальная линейная комбинация — *компонентной* функцией. Булевы функции будем рассматривать в том числе как частный случай векторных булевых функций.

Любая векторная булева функция $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ единственным образом представляется в виде *полинома Жегалкина* (алгебраической нормальной формы, АНФ):

$$F(x_1, x_2, \ldots, x_n) = \bigoplus_{a \in \mathbb{F}_2^n} g_a x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}, \quad g_a \in \mathbb{F}_2^m,\ 0^0 = 1. \tag{2}$$

Степенью векторной булевой функции называется степень её полинома Жегалкина. Функция F *линейная*, если $F(x \oplus y) = F(x) \oplus F(y)$ для

всех $x, y \in \mathbb{F}_2^n$. Прибавляя константу из $\mathbb{F}_2^m$ к линейным функциям, получим множество *аффинных* функций (функций степени не более 1). *Образ* множества $S \subseteq \mathbb{F}_2^n$ будем обозначать через $F(S) = \{F(s) \mid s \in S\}$.

Производной F по направлению $a \in \mathbb{F}_2^n$ называется векторная булева функция $\mathcal{D}_a F(x) = F(x) \oplus F(x \oplus a)$. *Порядком дифференциальной равномерности* $\delta(F)$ называется минимальное t, для которого при любых параметрах $a \in \mathbb{F}_2^n \setminus \{0\}$ и $b \in \mathbb{F}_2^m$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более t решений. При $n = m$ функции с $\delta(F) = 2$ называются APN-*функциями*, а взаимно однозначные APN-функции — APN-*подстановками*.

Расстояние Хэмминга между булевыми функциями $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ равно числу векторов, на которых их значения различаются. *Вес Хэмминга* $\mathrm{wt}(f)$ функции (вектора $x \in \mathbb{F}_2^n$) — число векторов (координат) со значением 1. Булева функция называется *уравновешенной*, если она принимает значения 0 и 1 на одинаковом числе векторов.

Функции f и g EA-*эквивалентны*, если $f(x) = g(A(x)) \oplus h(x)$ для всех $x \in \mathbb{F}_2^n$, где $A\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — обратимое аффинное преобразование и $h\colon \mathbb{F}_2^n \to \mathbb{F}_2$ аффинна. Функция f при чётном n называется *бент-функцией*, если она находится на максимальном расстоянии от множества всех аффинных булевых функций. Множество всех бент-функций замкнуто относительно EA-эквивалентности.

Обратим внимание, что большинство приводимых определений и фактов можно найти в [8].

1.2. Подпространства и ограничения функций. *Линейным подпространством* $\mathbb{F}_2^n$ называется непустое подмножество $L \subseteq \mathbb{F}_2^n$ такое, что для любых $x, y \in L$ выполнено $x \oplus y \in L$. Для $a \in \mathbb{F}_2^n$ множество $U = a \oplus L = \{a \oplus x \mid x \in L\}$ называется *аффинным подпространством* $\mathbb{F}_2^n$. Положим $[U] = L = a \oplus U$. *Размерность* аффинного подпространства U полагаем равной $\dim U = \dim[U]$. Множества всех линейных и аффинных подпространств $\mathbb{F}_2^n$ размерности k обозначим через $\mathcal{S}_n^k$ и $\mathcal{AS}_n^k$ соответственно.

Ограничением функции $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ на множество $S \subseteq \mathbb{F}_2^n$ называется $F|_S\colon S \to \mathbb{F}_2^m$ такая, что $F|_S(y) = F(y)$ для всех $y \in S$.

Пусть U и V — аффинные подпространства $\mathbb{F}_2^n$ и $\mathbb{F}_2^m$ соответственно. Функция $A\colon U \to V$ называется *аффинной*, если $A = A'|_U$ для некоторой аффинной функции $A'\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$. Через $[A]$ обозначим любую линейную функцию вида $\mathbb{F}_2^n \to \mathbb{F}_2^m$ такую, что $A = [A]|_U \oplus \mathrm{const}$. Например, подходящей является $[A] = A' \oplus A'(0)$. Введём следующие обозначения:

- $\mathcal{A}_U^V = \{f\colon U \to V \mid f \text{ аффинна}\}$ — множество всех аффинных функций из U в V;
- $\mathcal{A}_n^V = \mathcal{A}_{\mathbb{F}_2^n}^V$ и $\mathcal{A}_U^k = \mathcal{A}_U^{\mathbb{F}_2^k}$; в булевом случае $\mathcal{A}_n = \mathcal{A}_n^1$ и $\mathcal{A}_U = \mathcal{A}_U^1$.

Введём в рассмотрение также следующие фактор-пространства.

• $\widetilde{\mathcal{F}}_U = \mathcal{F}_U/\mathcal{A}_U$, где $\mathcal{F}_U = \{f\colon U \to \mathbb{F}_2\}$, $\mathcal{F}_n = \mathcal{F}_{\mathbb{F}_2^n}$. Соответствующее отношение эквивалентности обозначим через $\simeq$, так что $f \simeq g$ тогда и только тогда, когда $f \oplus g \in \mathcal{A}_U$, где $f, g \in \mathcal{F}_U$.

• $\mathcal{A}_U^n/\mathcal{A}_U^V$, где $V \subseteq \mathbb{F}_2^n$ — линейное подпространство. Соответствующее отношение эквивалентности обозначим через $\overset{V}{=}$, так что $F \overset{V}{=} G$ тогда и только тогда, когда $F \oplus G \in \mathcal{A}_U^V$, где $F, G \in \mathcal{A}_U^n$

С целью упрощения записи будем считать, что для $f \in \mathcal{F}_U$ также имеет место $f \in \widetilde{\mathcal{F}}_U$ (аналогично $F \in \mathcal{A}_U^n$ и $F \in \mathcal{A}_U^n/\mathcal{A}_U^V$), а для равенства в фактор-пространстве используем символ эквивалентности.

Характеристическую функцию множества S обозначим через Ind_S, где S может быть как подмножеством $\mathbb{F}_2^n$, так и $\widetilde{\mathcal{F}}_U$.

1.3. Алгебраическое представление булевых функций. Функцию $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ можно также рассмотреть как функцию $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, зафиксировав некоторый базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$. Многие свойства, например, алгебраическая степень, нахождение функций на определённом расстоянии, свойство быть бент-функцией и т. д., не зависят от выбора базиса. Любую такую функцию F можно однозначно представить в виде полинома над полем:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \quad \delta_0, \ldots, \delta_{2^n-1} \in \mathbb{F}_{2^n}.$$

Степень функции, отличной от константы 0, можно найти по формуле

$$\deg F = \max_{i \in \{0,\ldots,2^n-1\}\colon \delta_i \neq 0} \mathrm{wt}(i_{(2)}),$$

где $i_{(2)} \in \mathbb{F}_2^n$ — вектор двоичной записи i. Таким образом, аффинными являются функции следующего вида:

$$x \mapsto \alpha_0 x^{2^0} + \alpha_1 x^{2^1} + \cdots + \alpha_{n-1} x^{2^{n-1}} + \alpha_n, \quad \text{где } \alpha_0, \ldots, \alpha_n \in \mathbb{F}_{2^n}.$$

Булеву функцию можно представить как $\mathrm{tr}_1^n(F(x))$, где

$$\mathrm{tr}_1^n(x) = x^{2^0} + x^{2^1} + \cdots + x^{2^{n-1}}, \quad x \in \mathbb{F}_{2^n}.$$

Это линейная функция, значения которой лежат в $\mathbb{F}_2$. Будем пользоваться следующими связанными с ней свойствами:

$$\mathrm{tr}_1^n(x^2) \equiv \mathrm{tr}_1^n(x), \quad x^{k \cdot 2^i} \equiv x^{k \lll i}, \quad i \geqslant 0,\ k \in \{0, \ldots, 2^n - 1\}, \qquad (3)$$

где $k \lll i$ — число, двоичная запись которого является циклическим сдвигом двоичной записи $k_{(2)}$ на i позиций в сторону старших разрядов.

1.4. Класс Мэйорана — МакФарланда. Класс Мэйорана — МакФарланда $\mathcal{M}_{2n}$ от $2n$ переменных состоит из функций вида

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

где π — подстановка на $\mathbb{F}_2^n$ и $\varphi\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Все они являются бент-функциями. Здесь используем $\langle\cdot,\cdot\rangle_n$, поскольку рассматриваем как «обычные» функции вида $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, для которых

$$\langle x,y\rangle_n = \langle x,y\rangle = x_1y_1 \oplus \cdots \oplus x_ny_n, \quad x,y \in \mathbb{F}_2^n,$$

так и функции над полем вида $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$, для которых

$$\langle x,y\rangle_n = \mathrm{tr}_1^n(xy), \quad x,y \in \mathbb{F}_{2^n},$$

т. е. в последнем случае рассматриваем $\mathbb{F}_2^n$ как $\mathbb{F}_{2^n}$. Все полученные в работе результаты справедливы, если в качестве $\langle\cdot,\cdot\rangle_n$ взять любую симметричную невырожденную билинейную форму над $\mathbb{F}_2^n$ ($\mathbb{F}_{2^n}$), которая линейна по обоим аргументам, её значение не меняется при перестановке аргументов и $\langle a,x\rangle_n \equiv 0$ только при $a = 0 \in \mathbb{F}_2^n$ [33].

Ортогональное пространство к линейному подпространству $L \subseteq \mathbb{F}_2^n$ определяется относительно используемой билинейной формы:

$$L^\perp = \{y \in \mathbb{F}_2^n \mid \langle x,y\rangle_n = 0 \text{ для всех } x \in L\} \subseteq \mathbb{F}_2^n.$$

Отметим, что $\dim L^\perp = n - \dim L$.

1.5. Бент-функции на расстоянии 2^n и $\mathcal{M}_{2n}$. Минимальное расстояние между двумя различными бент-функциями от $2n$ переменных равно 2^n [17]. Критерий такого расположения даёт

Утверждение 1 [17]. *Пусть $f \in \mathcal{F}_{2n}$ — бент-функция и $U \subset \mathbb{F}_2^{2n}$, $|U| = 2^n$. Тогда $f \oplus \mathrm{Ind}_U$ является бент-функцией, если и только если U — аффинное подпространство $\mathbb{F}_2^{2n}$ и $f|_U$ аффинная.*

Для любой бент-функции $f \in \mathcal{M}_{2n}$ существуют бент-функции на расстоянии 2^n от f, которые будем называть *ближайшими*. В настоящей работе большое внимание уделяется известной [28] нижней оценке числа таких бент-функций, которая уточнена в [29].

Утверждение 2 [28, 29]. *Число ближайших к $f \in \mathcal{M}_{2n}$ бент-функций не меньше $\ell_{2n} = 2^{2n+1} - 2^n$, при этом в точности ℓ_{2n} из них принадлежат классу $\mathcal{M}_{2n}$.*

Известно [30], что нижняя оценка ℓ_{2n} достижима при простых $n \geqslant 5$. Для произвольных функций $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, подобной используемым при построении класса $\mathcal{M}_{2n}$ подстановкам, и $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$ положим:

- $\mathcal{L}_k(\pi) = \{U \in \mathcal{AS}_n^k \mid \pi(U) \in \mathcal{AS}_n^k\}$ и $\mathcal{L}(\pi) = \mathcal{L}_0(\pi) \cup \cdots \cup \mathcal{L}_n(\pi)$;
- $\mathcal{LA}_k(F) = \{U \in \mathcal{AS}_n^k \mid F|_U \text{ аффинна}\}$.

Например, построение всех ближайших к $f \in \mathcal{M}_{2n}$ бент-функций с помощью утверждения 1 эквивалентно нахождению множества $\mathcal{LA}_n(f)$, а число таких бент-функций равно $|\mathcal{LA}_n(f)|$. Далее также потребуется следующее известное свойство инверсии элементов конечного поля.

Утверждение 3 [34]. *Пусть* $\pi(x) = x^{2^n-2}$ *для* $x \in \mathbb{F}_{2^n}$ *и* $2 \leqslant k \leqslant n$. *Тогда если* $k \nmid n$, *то* $\mathcal{L}_k(\pi) = \varnothing$, *иначе* $\mathcal{L}_k(\pi) = \{s\mathbb{F}_{2^k} \mid s \in \mathbb{F}_{2^n} \setminus \{0\}\}$, *где* $s\mathbb{F}_{2^k} = \{sx \mid x \in \mathbb{F}_{2^k}\}$.

Заметную роль [30] в достижимости оценки ℓ_{2n} играют APN-подстановки, каждую из которых эквивалентно можно определить как подстановку π на $\mathbb{F}_2^n$ такую, что $\mathcal{L}_2(\pi) = \varnothing$ (см. [14]).

2. Описание ближайших к $f \in \mathcal{M}_{2n}$ бент-функций и подсчёт их числа

Переформулируем критерий расположения ближайших к $f \in \mathcal{M}_{2n}$ бент-функций, предложенный в [30], используя другое представление элементов $\mathcal{LA}_n(f)$ (п. 2.1), а также определив специальный линейный оператор (п. 2.2), свойства которого позволяют найти $|\mathcal{LA}_n(f)|$. Для изучения этих свойств можно использовать некоторые упрощения (п. 2.3).

2.1. Представление аффинных подпространств $\mathbb{F}_2^k \times \mathbb{F}_2^m$. В работе [30] для представления подпространств использовались базисные GJB-матрицы (приведённые ступенчатые матрицы). Однако не всегда удобно работать с базисами, особенно если функции представлены в алгебраическом виде. Рассмотрим схожее представление подпространств $\mathbb{F}_2^k \times \mathbb{F}_2^m$ на языке множеств, задействующее меньшие подпространства $\mathbb{F}_2^k$ и $\mathbb{F}_2^m$ (пересечение и проекцию), а также аффинные функции:

$$\mathcal{S}(U, V, H) = \big\{(x \oplus H(y), y) \in \mathbb{F}_2^k \times \mathbb{F}_2^m \mid x \in V,\, y \in U\big\}, \tag{4}$$

где

- U — аффинное подпространство $\mathbb{F}_2^m$,
- V — линейное подпространство $\mathbb{F}_2^k$,
- $H \in \mathcal{A}_U^k$, т. е. функция $H\colon U \to \mathbb{F}_2^k$ аффинная.

Утверждение 4. *Множество* $\mathcal{S}(U, V, H)$ *образует аффинное подпространство в* $\mathbb{F}_2^k \times \mathbb{F}_2^m$ *размерности* $\dim U + \dim V$. *Более того,*

1) *любое аффинное подпространство* $S \subseteq \mathbb{F}_2^k \times \mathbb{F}_2^m$ *представимо как* $S = \mathcal{S}(U, V, H)$ *с помощью проекции* U *и пересечения* V:

$$U = \big\{y \in \mathbb{F}_2^m \mid \text{существует } x \in \mathbb{F}_2^k \text{ такой, что } (x, y) \in S\big\},$$
$$V \times \{0\}^m = [S] \cap \big(\mathbb{F}_2^k \times \{0\}^m\big);$$

2) *представление* $S = \mathcal{S}(U, V, H)$ *единственно при* $H \in \mathcal{A}_U^k / \mathcal{A}_U^V$.

Доказательство. Нетрудно видеть, что $\mathcal{S}(U,V,H) \subseteq \mathbb{F}_2^k \times \mathbb{F}_2^m$ — аффинное подпространство и $\mathcal{S}(U,V,H) = (H(a),a) \oplus [\mathcal{S}(U,V,H)]$ для произвольно выбранного $a \in U$. При этом для каждого значения второй части $y \in U$ есть ровно $|H(y) \oplus V|$ различных значений первой части. Итого $|\mathcal{S}(U,V,H)| = |U| \cdot |V|$, т. е. $\dim \mathcal{S}(U,V,H) = \dim U + \dim V$.

Представление. Если $S = \mathcal{S}(U,V,H)$ для некоторой $H \in \mathcal{A}_U^k$, то подпространства U и V определяются однозначно по приведённым в условии формулам в силу очевидных свойств конструкции. Рассмотрим произвольное аффинное подпространство $S \subseteq \mathbb{F}_2^k \times \mathbb{F}_2^m$. Множества $U \subseteq \mathbb{F}_2^m$ и $V \subseteq \mathbb{F}_2^k$ однозначно задаются теми же формулами по S и являются аффинным и линейным подпространствами соответственно.

С целью подобрать подходящую аффинную функцию сначала найдём такую функцию $H\colon [U] \to \mathbb{F}_2^k$, что $[S] = \mathcal{S}([U],V,H)$. Пусть $C(y) = [S] \cap \big(\mathbb{F}_2^k \times \{y\}\big)$, $y \in [U]$. Очевидно, что $C(y)$ непусто и является смежным классом $V \times \{0\}^m = [S] \cap \big(\mathbb{F}_2^k \times \{0\}^m\big)$. Более того, $[S] = \bigcup\limits_{y \in [U]} C(y)$.

Пусть $y_1, \ldots, y_r \in \mathbb{F}_2^m$ образуют базис $[U]$, а $s_1, \ldots, s_r \in \mathbb{F}_2^k$ — любые векторы такие, что $(s_i, y_i) \in C(y_i)$ при $i \in \{1, \ldots, r\}$. Положим $H(y_i) = s_i$, $i \in \{1, \ldots, r\}$, а остальные значения H на $[U]$ определим из соотношения линейности. После этого произвольным образом продолжим функцию H до некоторой линейной функции $[H]\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ такой, что $H = [H]|_{[U]}$. Заметим, что $C(y) = (H(y),y) \oplus (V \times \{0\}^m)$. Действительно, если $y = y_{i_1} \oplus \cdots \oplus y_{i_t}$ для $0 \leqslant t \leqslant r$, то

$$(H(y),y) = (H(y_{i_1}),y_{i_1}) \oplus \cdots \oplus (H(y_{i_t}),y_{i_t}) \in [S],$$

поскольку $(H(y_{i_1}),y_{i_1}), \ldots, (H(y_{i_t}),y_{i_t})$ лежат в линейном $[S]$. Таким образом, $(H(y),y) \in C(y)$, т. е. $C(y) = (H(y),y) \oplus (V \times \{0\}^m)$. Это также означает, что $[S] = \mathcal{S}([U],V,H)$.

Далее, возьмём произвольно $(b,a) \in S$, т. е. $S = (b,a) \oplus [S]$. Получаем $S = \mathcal{S}(U,V,H')$ для $H'(x) = [H](x) \oplus [H](a) \oplus b$ при $x \in U = a \oplus [U]$.

Единственность. Если $S = \mathcal{S}(U,V,H) = \mathcal{S}(U',V',H')$, то по построению $U' = U$ и $V' = V$. Далее, подпространства $\mathcal{S}(U,V,H)$ и $\mathcal{S}(U,V,H')$ совпадают тогда и только тогда, когда для любого $y \in U$ смежные классы $H(y) \oplus V$ и $H'(y) \oplus V$ совпадают. Это эквивалентно тому, что $H(y) \oplus H'(y) \in V$, $y \in U$, т. е. $H \oplus H'$ — аффинная функция вида $U \to V$, откуда $H \overset{V}{=} H'$. Утверждение 4 доказано.

Замечание 1. Функции множества $\mathcal{A}_U^R$ являются представителями классов эквивалентности из $\mathcal{A}_U^k / \mathcal{A}_U^V$, где $R \subseteq \mathbb{F}_2^k$ — произвольное линейное подпространство размерности $k - \dim V$ такое, что $R \cap V = \{0\}$. Действительно, в этом случае $\mathbb{F}_2^k$ раскладывается в прямую сумму подпространств V и R, а равенство $R \cap V = \{0\}$ обеспечивает попарную

неэквивалентность представителей. Таким образом, любую аффинную функцию $H\colon U \to \mathbb{F}_2^k$ можно представить в виде суммы функций из множеств $\mathcal{A}_U^R$ и $\mathcal{A}_U^V$. Такое линейное подпространство R можно легко построить, например зная информационные координаты V [35].

Замечание 2. Линейное подпространство $\mathbb{F}_2^k \times \mathbb{F}_2^m$ также может быть представлено конструкцией $\mathcal{S}(U, V, H)$. Для этого достаточно применить линейные подпространство U и функцию H.

Далее в основном будем рассматривать пространство $\mathbb{F}_2^n \times \mathbb{F}_2^n$, т. е. $k = m = n$, поскольку именно на нём задаются бент-функции из класса Мэйорана —МакФарланда $\mathcal{M}_{2n}$.

2.2. Бент-функции, ближайшие к $f \in \mathcal{M}_{2n}$. Рассмотрим функцию $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ и подпространство $U \in \mathcal{AS}_n^k$ такие, что $\pi(U) \in \mathcal{AS}_n^k$; положим $V = [\pi(U)]^\perp \in \mathcal{S}_n^{n-k}$. Линейный оператор $\mathcal{G}_\pi^U\colon \mathcal{A}_U^n/\mathcal{A}_U^V \to \widetilde{\mathcal{F}}_U$ определим следующим образом:

$$\mathcal{G}_\pi^U(H)\colon x \mapsto \langle H(x), \pi(x)\rangle_n, \quad x \in U. \tag{5}$$

Для удобства обозначим отношение $\overset{V}{=}$ на $\mathcal{A}_U^n/\mathcal{A}_U^V$ через $\overset{\pi}{=}$. Заметим, что при $U = \mathbb{F}_2^n$ не требуется использовать фактор-пространство входных аргументов, в этом случае будем обозначать $\mathcal{G}_\pi^{\mathbb{F}_2^n}$ через $\mathcal{G}_\pi\colon \mathcal{A}_n^n \to \widetilde{\mathcal{F}}_n$.

Утверждение 5. *Линейный оператор $\mathcal{G}_\pi^U$ определён корректно.*

Доказательство. Пусть $H, H'\colon U \to \mathbb{F}_2^n$ аффинные и $H \overset{\pi}{=} H'$, т. е. $H' = H \oplus \Delta$, где $\Delta\colon U \to [\pi(U)]^\perp$ аффинная. Тогда

$$\begin{aligned}\langle H'(x), \pi(x)\rangle_n &= \\ &= \langle H(x) \oplus \Delta(x), \pi(x)\rangle_n = \langle H(x), \pi(x)\rangle_n \oplus \langle \Delta(x), \pi(x)\rangle_n = \\ &= \langle H(x), \pi(x)\rangle_n \oplus \langle \Delta(x), \pi(a)\rangle_n \oplus \langle \Delta(x), \pi(a) \oplus \pi(x)\rangle_n,\end{aligned}$$

где $a \in U$. Тем самым $\pi(a) \oplus \pi(x) \in [\pi(U)]$, а в силу $\Delta(x) \in [\pi(U)]^\perp$ получаем

$$\langle \Delta(x), \pi(a) \oplus \pi(x)\rangle_n \equiv 0.$$

Поскольку $\pi(a)$ не зависит от x, а Δ аффинная, функция $\langle \Delta(x), \pi(a)\rangle_n$ также аффинная. Следовательно, $H \overset{\pi}{=} H'$ влечёт

$$\mathcal{G}_\pi^U(H) = \langle H(x), \pi(x)\rangle_n \simeq \langle H'(x), \pi(x)\rangle_n = \mathcal{G}_\pi^U(H').$$

Линейность оператора очевидна. Утверждение 5 доказано.

Используя ядро $\operatorname{Ker} \mathcal{G}_\pi^U = \{H \in \mathcal{A}_U^n/\mathcal{A}_U^V \mid \mathcal{G}_\pi^U(H) \simeq 0\}$ и образ $\operatorname{Im} \mathcal{G}_\pi^U = \mathcal{G}_\pi^U\left(\mathcal{A}_U^n/\mathcal{A}_U^V\right)$ оператора $\mathcal{G}_\pi^U$, переформулируем критерий из [30]. Заметим, что это можно сделать ещё одним схожим способом [35].

Теорема 1. *Пусть* $f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$ *и* $L \subseteq \mathbb{F}_2^{2n}$. *Тогда* $f \oplus \mathrm{Ind}_L$ *— ближайшая бент-функция к* f, *если и только если*

$$L = \mathcal{S}(U, [\pi(U)]^\perp, H \oplus H_0),$$

где $U \in \mathcal{L}(\pi)$, $H \in \operatorname{Ker} \mathcal{G}_\pi^U$ *и* $\mathcal{G}_\pi^U(H_0) \simeq \varphi|_U$. *Произвольная пара* $U \in \mathcal{L}(\pi)$ *и* $H \oplus H_0 \in \mathcal{A}_U^n / \mathcal{A}_U^{[\pi(U)]^\perp}$ *однозначно определяет подходящее* L.

Доказательство. Заметим, что $\dim L = \dim U + \dim[\pi(U)]^\perp = n$, поскольку $U \subseteq \mathbb{F}_2^n$. В силу утверждения 1 достаточно проанализировать аффинность функции f на подпространстве $L \in \mathcal{AS}_{2n}^n$, которое в общем случае для подходящих подпространств V, U и функции H' имеет вид

$$L = \mathcal{S}(U, V, H') = \{(x \oplus H'(y), y) \mid x \in V,\ y \in U\}.$$

Для произвольных $x \in V$, $y \in U$ имеем

$$f|_L(x,y) = \langle x \oplus H'(y), \pi(y)\rangle_n \oplus \varphi(y) = \\ = \langle x, \pi(y)\rangle_n \oplus \langle H'(y), \pi(y)\rangle_n \oplus \varphi(y). \quad (6)$$

С одной стороны, если подпространство U и функции H, H_0 выбраны, как указано в условии теоремы, а $V = [\pi(U)]^\perp$ и $H' = H \oplus H_0$, то при помощи (6) нетрудно проверить, что f аффинна на L.

С другой стороны, если $f|_L$ аффинна, то из (6) при $a \in V$ следует, что

$$\mathcal{D}_{(a,0)} f|_L(x,y) = \langle a, \pi(y)\rangle \equiv \mathrm{const},$$

Зафиксируем произвольный $u \in U$ и рассмотрим $\pi'(y) = \pi(y) \oplus \pi(u)$. После подстановки получаем

$$\mathcal{D}_{(a,0)} f|_L(x,y) = \langle a, \pi'(y)\rangle \oplus \langle a, \pi(u)\rangle \equiv \mathrm{const},$$

откуда $\langle a, \pi'(y)\rangle \equiv \mathrm{const}$. При этом $\pi'(u) = 0$ и $\langle a, \pi'(u)\rangle = 0$, так что $\langle a, \pi'(y)\rangle \equiv 0$. Из произвольности $a \in V$ следует, что $\pi'(U) \subseteq V^\perp$. Однако по утверждению 4 выполняется $\dim U = n - \dim V = \dim V^\perp$, значит, $\pi'(U) = V^\perp$ и $\pi(U) = \pi(u) \oplus V^\perp$. Другими словами, имеем $U \in \mathcal{L}(\pi)$ и $V = [\pi(U)]^\perp$.

В этом случае согласно (6) аффинность $f|_L$ сводится к аффинности функции $\langle H'(y), \pi(y)\rangle_n \oplus \varphi(y)$. В свою очередь, это можно записать как $\mathcal{G}_\pi^U(H') \simeq \varphi|_U$, где $\varphi|_U$ рассматривается уже как функция из $\widetilde{\mathcal{F}}_U$. Так как оператор $\mathcal{G}_\pi^U$ линейный, последнее эквивалентно тому, что $H' = H \oplus H_0$, где $H \in \operatorname{Ker} \mathcal{G}_\pi^U$ и $\mathcal{G}_\pi^U(H_0) \simeq \varphi|_U$. Осталось заметить, что согласно утверждению 4 представление L единственно при выборе $H' \in \mathcal{A}_U^n / \mathcal{A}_U^V$. Теорема 1 доказана.

Из доказанного критерия и линейности $\mathcal{G}_\pi^U$ напрямую вытекает следствие о числе ближайших к $f \in \mathcal{M}_{2n}$ бент-функций, которое согласно утверждению 1 равно $|\mathcal{LA}_n(f)|$.

Следствие 1. *Если* $f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$, *то*

$$|\mathcal{LA}_n(f)| = \sum_{L \in \mathcal{L}(\pi)} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\pi^L}(\varphi|_L) \cdot \left|\mathrm{Ker}\ \mathcal{G}_\pi^L\right|.$$

Далее докажем дополнительные свойства оператора $\mathcal{G}_\pi^U$, а в разд. 4–6 продемонстрируем удобство формулы из следствия 1, которую уточним в теореме 3. Заметим, что свойства чисел $|\mathcal{L}_2(\pi)|$ и $|\mathcal{L}(\pi)|$ исследовались в работах [36–38].

2.3. Свойства $\mathcal{G}_\pi^U$ и переход к $\mathcal{G}_{\pi'}$. Поиск ядра и образа $\mathcal{G}_\pi^U$ представляется непростой задачей из-за использования ограничений функций на $U \in \mathcal{AS}_n^k$. Например, нужно следить за однозначностью представления функций. Однако, мы покажем, что можно обойти ограничения функций, рассматривая свойства оператора $\mathcal{G}_{\pi'}$ для некоторой подстановки $\pi'\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$.

Теорема 2. *Пусть функция* $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ *и подпространство* $U \in \mathcal{AS}_n^k$ *таковы, что* $\pi(U) \in \mathcal{AS}_n^k$, *а также*

- *функция* $\pi'\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ *определена равенством* $\pi' = B \circ \pi \circ A$, *где* $A\colon \mathbb{F}_2^k \to U$ *и* $B\colon \pi(U) \to \mathbb{F}_2^k$ *обратимы и аффинны;*
- $\mathcal{G}_\pi^U$ *и* $\mathcal{G}_{\pi'}$ *определены относительно* $\langle\cdot,\cdot\rangle_n$ *и* $\langle\cdot,\cdot\rangle_k$ *соответственно;*
- *функция* $[B]^*\colon \mathbb{F}_2^k \to \mathbb{F}_2^n$ *сопряжённая к* $[B]$, *т. е.*

$$\langle [B]^*(x), y\rangle_n = \langle x, [B](y)\rangle_k, \quad x \in \mathbb{F}_2^k,\ y \in \mathbb{F}_2^n.$$

Тогда

$$\mathrm{Ker}\ \mathcal{G}_\pi^U = [B]^* \circ \mathrm{Ker}\ \mathcal{G}_{\pi'} \circ A^{-1} = \{[B]^* \circ H \circ A^{-1} \mid H \in \mathrm{Ker}\ \mathcal{G}_{\pi'}\},$$
$$\mathrm{Im}\ \mathcal{G}_\pi^U = \mathrm{Im}\ \mathcal{G}_{\pi'} \circ A^{-1} = \{\varphi \circ A^{-1} \mid \varphi \in \mathrm{Im}\ \mathcal{G}_{\pi'}\},$$

при этом $\left|\mathrm{Ker}\ \mathcal{G}_\pi^U\right| = \left|\mathrm{Ker}\ \mathcal{G}_{\pi'}\right|$ *и* $\left|\mathrm{Im}\ \mathcal{G}_\pi^U\right| = \left|\mathrm{Im}\ \mathcal{G}_{\pi'}\right|$.

Доказательство. Пусть $V = [B]^*\big(\mathbb{F}_2^k\big)$ — линейное подпространство в $\mathbb{F}_2^n$, т. е. $[B]^*\colon \mathbb{F}_2^k \to V$. Докажем от противного, что $V \cap [\pi(U)]^\perp = \{0\}$. Пусть, напротив, $[B]^*(a) \in [\pi(U)]^\perp$ для некоторого $a \in \mathbb{F}_2^k \setminus \{0\}$. Выберем $u \in \pi(U)$; для любого $y \in [\pi(U)]$ имеем

$$\langle a, [B](u \oplus y)\rangle_k = \langle [B]^*(a), u \oplus y\rangle_n = \\ = \langle [B]^*(a), u\rangle_n \oplus \langle [B]^*(a), y\rangle_n = \langle [B]^*(a), u\rangle_n.$$

Заметим, что $[B]|_{\pi(U)} = B \oplus \mathrm{const}$. В силу обратимости B получаем $[B](\pi(U)) = B(\pi(U)) \oplus \mathrm{const} = \mathbb{F}_2^k \oplus \mathrm{const} = \mathbb{F}_2^k$. Таким образом, для любого $x \in \mathbb{F}_2^k$

$$\langle a, x\rangle_k = \langle [B]^*(a), u\rangle_n,$$

что противоречит невырожденности формы $\langle\cdot,\cdot\rangle_k$, поскольку $a \neq 0$.

Докажем, что $\dim V = k$, т. е. обратимость $[B]^*$. Действительно, если $[B]^*(x_1) = [B]^*(x_2)$ при $x_1, x_2 \in \mathbb{F}_2^k$ и $x_1 \neq x_2$, то из равенств

$$\langle [B]^*(x_1), y\rangle_n = \langle x_1, [B](y)\rangle_k, \quad \langle [B]^*(x_2), y\rangle_n = \langle x_2, [B](y)\rangle_k$$

вытекает, что для любого $y \in \mathbb{F}_2^n$

$$\langle x_1 \oplus x_2, [B](y)\rangle_k = 0.$$

Это противоречит невырожденности формы $\langle\cdot,\cdot\rangle_k$, поскольку $x_1 \oplus x_2 \neq 0$ и $[B](\pi(U)) = \mathbb{F}_2^k$. Тем самым функция $[B]^*\colon \mathbb{F}_2^k \to V$ обратима.

Обратимость A и $[B]^*$ позволяет любую функцию $H' \in \mathcal{A}_U^V$ представить в виде $H' = [B]^* \circ H \circ A^{-1}$ для некоторой $H \in \mathcal{A}_k^k$. В силу доказанных свойств V и замечания 1 именно такие функции можно рассматривать в качестве попарно неэквивалентных представителей фактор-пространства $\mathcal{A}_U^n / \mathcal{A}_U^{[\pi(U)]^\perp}$.

Осталось заметить, что для функции $\varphi = \mathcal{G}_{\pi'}(H)$ и любого $x \in \mathbb{F}_2^k$ по построению справедливы равенства

$$\begin{aligned}\varphi(x) &= \langle H(x), B(\pi(A(x)))\rangle_k \simeq \langle H(x), [B](\pi(A(x)))\rangle_k = \\ &= \langle [B]^*(H(x)), \pi(A(x))\rangle_n = \langle [B]^*(H(A^{-1}(y)))), \pi(y)\rangle_n = \varphi'(y),\end{aligned}$$

где $y = A(x) \in U$. Поскольку $A\big(\mathbb{F}_2^k\big) = U$, функция $\varphi'(y) = \varphi(A^{-1}(y))$ определена на всём U и $\varphi' = \mathcal{G}_\pi^U(H')$. При этом $\varphi' \overset{\pi}{=} 0$ тогда и только тогда, когда $\varphi \simeq 0$, что означает эквивалентность условий $H \in \operatorname{Ker} \mathcal{G}_{\pi'}$ и $H' \in \operatorname{Ker} \mathcal{G}_\pi^U$. Теорема 2 доказана.

Таким образом, теорема 2 позволяет использовать естественную билинейную форму, не ограничивая её область определения. Например, можно работать с $\mathrm{tr}_1^k(\cdot)$ над $\mathbb{F}_{2^k}$ вместо сужения $\mathrm{tr}_1^n(\cdot)$ на $U \in \mathcal{AS}_n^k$. Более того, можно переходить к другой билинейной форме, не меняя начального U. Полезными также являются следующие свойства.

Утверждение 6. *Пусть функции $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ и $B \in \mathcal{A}_n^n$ обратимы. Тогда $\operatorname{Im} \mathcal{G}_\pi^U = \operatorname{Im} \mathcal{G}_{B\circ\pi}^U$ для любого подпространства $U \in \mathcal{L}(\pi)$.*

Доказательство прямо следует из теоремы 2.

Утверждение 7. *Пусть $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ обратима, $\varphi \in \mathcal{F}_n$, $L, U \in \mathcal{L}(\pi)$ и $L \subseteq U$. Тогда если $\varphi|_U \in \operatorname{Im} \mathcal{G}_\pi^U$, то $\varphi|_L \in \operatorname{Im} \mathcal{G}_\pi^L$.*

Доказательство. Условие $\varphi|_U \in \operatorname{Im} \mathcal{G}_\pi^U$ означает, что существует функция $H \in \mathcal{A}_U^n$ такая, что $\mathcal{G}_\pi^U(H) \simeq \varphi|_U$, т. е. $\mathcal{G}_\pi^U(H) = \varphi|_U \oplus h$, где $h \in \mathcal{A}_U$. Рассмотрим сужение $H|_L$. Очевидно, что оно также будет аффинным, т. е. $H|_L \in \mathcal{A}_L^n$. Тогда для соответствующего фактор-пространства $\mathcal{G}_\pi^L(H|_L) = \varphi|_L \oplus h|_L$, но $h|_L$ также аффинна, т. е. $\mathcal{G}_\pi^L(H|_L) \simeq \varphi|_L$. Утверждение 7 доказано.

Замечание 3. Если для $f(x,y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$ справедливо $\varphi \in \operatorname{Im} \mathcal{G}_\pi$, то $\varphi|_U \in \operatorname{Im} \mathcal{G}_\pi^U$ для любого $U \in \mathcal{L}(\pi)$, что упрощает формулу из следствия 1. Вместе с тем, это означает EA-эквивалетность бент-функций f и $f'(x',y') = \langle x', \pi(y')\rangle_n$: достаточно сделать замену $x' = x \oplus H(y)$ и $y' = y$ для $\mathcal{G}_\pi(H) \simeq \varphi$, и получим f' с точностью до аффинной части.

3. Ядро и образ $\mathcal{G}_\pi$ для некоторых π

Найдём ядро (или мощность ядра) и образ оператора $\mathcal{G}_\pi$ для некоторых функций π. Остановимся на аффинных функциях и функциях от малого числа переменных в представлении над $\mathbb{F}_2^n$, а также функции инверсии элементов конечного поля, продемонстрировав алгебраический подход.

3.1. Аффинные подстановки и подстановки от 3 переменных. Свойства оператора $\mathcal{G}_\pi$ несложно определить для аффинных подстановок $\pi \in \mathcal{A}_n^n$. Заметим, что при $n \in \{1,2\}$ все подстановки на $\mathbb{F}_2^n$ аффинны. При $n = 1$ это очевидно, а при $n = 2$ достаточно вспомнить, что $\deg \pi < n$ для любой подстановки $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ (вообще говоря, при $n \geqslant 2$; см., например, [8]).

Рассматривая подстановки на $\mathbb{F}_2^n$, удобно пользоваться матричным представлением для функции $H \in \mathcal{A}_n^n$: $H(x) = xA \oplus a$, где A — невырожденная двоичная матрица порядка n и $a \in \mathbb{F}_2^n$, при этом

$$\mathcal{G}_\pi(H)\colon x \mapsto \langle xA \oplus a, \pi(x)\rangle, \quad |\operatorname{Ker} \mathcal{G}_\pi| \cdot |\operatorname{Im} \mathcal{G}_\pi| = 2^{n^2+n}. \tag{7}$$

Утверждение 8. *Пусть $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — взаимно однозначная аффинная функция. Тогда*

$$\operatorname{Im} \mathcal{G}_\pi = \{\varphi \in \widetilde{\mathcal{F}}_n \mid \deg \varphi \leqslant 2\}, \quad |\operatorname{Ker} \mathcal{G}_\pi| = 2^{\frac{n(n+3)}{2}}.$$

Доказательство. 1. В силу утверждения 6 можно считать без ограничения общности, что π — тождественное отображение, поэтому образ аффинной функции $H \in \mathcal{A}_n^n$ под действием оператора $\mathcal{G}_\pi$ представляет собой булеву функцию $\langle xA \oplus a, x\rangle \in \widetilde{\mathcal{F}}_n$, где A — невырожденная двоичная матрица порядка n и $a \in \mathbb{F}_2^n$. Ясно, что так можно получить любую квадратичную функцию, при этом степень получившейся функции не может быть больше 2.

2. Имеем $|\mathrm{Ker}\ \mathcal{G}_\pi| = 2^{n^2+n-\dim \mathrm{Im}\ \mathcal{G}_\pi} = 2^{n^2+n-n(n-1)/2} = 2^{\frac{n(n+3)}{2}}$ в силу (7). Утверждение 8 доказано.

Перейдём к произвольным подстановкам $\pi\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$.

Утверждение 9. *Пусть* $\pi\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$ *— взаимно однозначная неаффинная функция. Тогда* $\mathrm{Im}\ \mathcal{G}_\pi = \widetilde{\mathcal{F}_3}$ *и* $|\mathrm{Ker}\ \mathcal{G}_\pi| = 256$.

Доказательство. 1. В силу того, что π взаимно однозначна и неаффинна, $\deg \pi = 2$. Таким образом, её полином Жегалкина можно представить в следующем виде:

$$\pi(x_1,x_2,x_3) = \begin{bmatrix} Q_1^1 \\ Q_2^1 \\ Q_3^1 \end{bmatrix}^\top x_2x_3 + \begin{bmatrix} Q_1^2 \\ Q_2^2 \\ Q_3^2 \end{bmatrix}^\top x_1x_3 + \begin{bmatrix} Q_1^3 \\ Q_2^3 \\ Q_3^3 \end{bmatrix}^\top x_1x_2 + xB + b,$$

где $Q_j^i \in \mathbb{F}_2$, $i,j \in \{1,2,3\}$, B — двоичная матрица порядка 3 и $b \in \mathbb{F}_2^3$. Поскольку $\deg \pi = 2$, существует вектор коэффициентов

$$q = (q_1,q_2,q_3) \in \left\{\left(Q_1^1,Q_1^2,Q_1^3\right),\ \left(Q_2^1,Q_2^2,Q_2^3\right),\ \left(Q_3^1,Q_3^2,Q_3^3\right)\right\},$$

с весом Хэмминга $\mathrm{wt}(q) \neq 0$, которому соответствует координатная функция f функции π, т. е.

$$f(x_1,x_2,x_3) = q_1x_2x_3 \oplus q_2x_1x_3 \oplus q_3x_1x_2 \oplus \langle a,x\rangle \oplus c,$$

где $a \in \mathbb{F}_2^3$ и $c \in \mathbb{F}_2$. Так как π обратима, все её компонентные функции уравновешенные, включая f [8]. Далее будем считать, что в $\langle xT \oplus s, \pi(x)\rangle$ функция $xT \oplus s \in \mathcal{A}_3^3$ имеет ненулевую координатную функцию только в координате, соответствующей f, т. е. $\langle xT \oplus s, \pi(x)\rangle = h(x)\cdot f(x)$, где $h \in \mathcal{A}_3$.

Случай 1: $\mathrm{wt}(q) = 1$. Без ограничения общности положим $q_3 = 1$. Заметим, что $x_1x_2 \oplus a_1x_1 \oplus a_2x_2 = (x_1 \oplus a_2)(x_2 \oplus a_1) \oplus a_1a_2$. Поскольку свободный член в полиноме Жегалкина f влияет только на аффинную часть $h(x)\cdot f(x)$, можно его не рассматривать. После замены

$$y_1 = x_1 \oplus a_2, \quad y_2 = x_2 \oplus a_1, \quad y_3 = x_3$$

функция f принимает вид

$$f(x_1,x_2,x_3) = y_1y_2 \oplus a_3y_3,$$

при этом f уравновешенна, так что $a_3 = 1$. Далее,

$$\begin{aligned} 1\cdot f(x) &= y_1y_2 \oplus y_3,\\ y_1\cdot f(x) &= y_1y_2 \oplus y_1y_3,\\ y_2\cdot f(x) &= y_1y_2 \oplus y_2y_3,\\ y_3\cdot f(x) &= y_1y_2y_3 \oplus y_3, \end{aligned}$$

т. е. $\{y_1y_2, y_1y_3, y_2y_3, y_1y_2y_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$. Отсюда получаем $\{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$, так как все функции из этого множества выражаются через функции y_1, y_2, y_3 и их суммы (с точностью до аффинной части). Тем самым $\operatorname{Im} \mathcal{G}_\pi = \widetilde{\mathcal{F}}_3$.

Случай 2: $\operatorname{wt}(q) = 2$. Без ограничения общности положим $q_1 = 0$. Сделав линейную замену

$$z_1 = x_1, \quad z_2 = x_2 \oplus x_3, \quad z_3 = x_3,$$

получим

$$f(x_1, x_2, x_3) = z_1z_2 \oplus a'_1z_1 \oplus a'_2z_2 \oplus a'_3z_3 \oplus c',$$

где $a' \in \mathbb{F}_2^3$ и $c' \in \mathbb{F}_2$. Далее действуя аналогично случаю 1 приходим к тому, что $\{z_1z_2, z_1z_3, z_2z_3, z_1z_2z_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$. Вместе с тем

$$z_1z_3 = x_1x_3, \quad z_1z_2 = x_1x_2 \oplus x_1x_3,$$
$$z_2z_3 = x_2x_3 \oplus x_3, \quad z_1z_2z_3 = x_1x_2x_3 \oplus x_1x_3.$$

Следовательно, $\{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$.

Случай 3: $\operatorname{wt}(q) = 3$, т. е. $q = (1, 1, 1)$. Здесь квадратичная часть f равна функции голосования $g(x_1, x_2, x_3) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$, при этом $g(x_1 \oplus 1, x_2, x_3) = g(x_1, x_2, x_3) \oplus x_2 \oplus x_3$. Тем самым, сделав замену

$$y_1 = x_1 \oplus s_1, \quad y_2 = x_2 \oplus s_2, \quad y_3 = x_3 \oplus s_3$$

для подходящего $s \in \mathbb{F}_2^3$, получим $f(x) = g(y)$ либо $f(x) = g(y) \oplus y_3$ (с точностью до константы). Однако $\operatorname{wt}(g(y) \oplus y_3) = 2$, а сама g уравновешенная. Таким образом, $f(x) = g(y)$. Далее,

$$(y_1 \oplus y_2 \oplus y_3) \cdot f(x) = y_1y_2y_3,$$
$$(y_1 \oplus 1) \cdot f(x) = y_2y_3 \oplus y_1y_2y_3,$$
$$(y_2 \oplus 1) \cdot f(x) = y_1y_3 \oplus y_1y_2y_3,$$
$$(y_3 \oplus 1) \cdot f(x) = y_1y_2 \oplus y_1y_2y_3,$$

откуда вытекает, что $\{y_1y_2, y_1y_3, y_2y_3, y_1y_2y_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$ и, следовательно, $\{x_1x_2, x_1x_3, x_2x_3, x_1x_2x_3\} \subseteq \operatorname{Im} \mathcal{G}_\pi$.

2. Имеем $|\operatorname{Ker} \mathcal{G}_\pi| = 2^{3^2+3-\dim \operatorname{Im} \mathcal{G}_\pi} = 2^{12-4} = 256$. Утверждение 9 доказано.

3.2. Инверсия элемента конечного поля. Применив теорему 6 из [30], можно найти образ оператора $\mathcal{G}_\sigma$ при простом $n \geqslant 5$, где σ — функция обращения элементов $\mathbb{F}_{2^n}$. При этом заметим, что $\operatorname{Im} \mathcal{G}_\sigma$ будет таким при любом n.

Утверждение 10. *Пусть* $\sigma(x) = x^{2^n-2}$ *для* $x \in \mathbb{F}_{2^n}$. *Тогда*

$$\operatorname{Ker} \mathcal{G}_\sigma = \left\{\alpha x + \beta x^2 + \gamma x^{2^{n-1}} + \gamma^2 \mid \alpha, \beta, \gamma \in \mathbb{F}_{2^n},\ \operatorname{tr}_1^n(\alpha) = 0\right\},$$

$$\operatorname{Im}\mathcal{G}_\sigma = \big\{\operatorname{tr}_1^n(c_2x^{2^2-1}+\cdots+c_{n-1}x^{2^{n-1}-1})+c_nx^{2^n-1} \mid c_2,\ldots,c_{n-1}\in\mathbb{F}_{2^n},\ c_n\in\mathbb{F}_2\big\},$$

при этом $|\operatorname{Ker}\mathcal{G}_\sigma| = 2^{3n-1}$ *и* $|\operatorname{Im}\mathcal{G}_\sigma| = 2^{(n-1)^2}$.

Доказательство. Любая аффинная функция $H\colon \mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ представима единственным образом в виде

$$H(x) = \alpha_0x^{2^0}+\alpha_1x^{2^1}+\cdots+\alpha_{n-1}x^{2^{n-1}}+\alpha_n,\quad \alpha_0,\ldots,\alpha_n\in\mathbb{F}_{2^n}.$$

Рассмотрим $\mathcal{G}_\sigma$:

$$\operatorname{tr}_1^n(x^{2^n-2}H(x)) = \operatorname{tr}_1^n(\alpha_0x^{2^n-1}+\alpha_1x^{2^1-1}+\cdots+\alpha_{n-1}x^{2^{n-1}-1}+\alpha_nx^{2^n-2}).$$

Согласно (3) имеем

$$\operatorname{tr}_1^n(\alpha_nx^{2^n-2}) = \operatorname{tr}_1^n\big(\big(\alpha_n^{2^{n-1}}x^{2^{n-1}-1}\big)^2\big) = \operatorname{tr}_1^n\big(\alpha_n^{2^{n-1}}x^{2^{n-1}-1}\big),$$
$$\operatorname{tr}_1^n(\alpha_0x^{2^n-1}) = \alpha_0^{2^0}x^{(2^n-1)\lll 0}+\cdots+\alpha_0^{2^{n-1}}x^{(2^n-1)\lll(n-1)} = \operatorname{tr}_1^n(\alpha_0)x^{2^n-1}.$$

Слагаемое $\operatorname{tr}_1^n(\alpha_1x^{2^1-1})$ линейно, поэтому элементами $\operatorname{Im}\mathcal{G}_\sigma$ являются функции вида

$$\operatorname{tr}_1^n(\alpha_2x^{2^2-1})+\cdots+\operatorname{tr}_1^n(\alpha_{n-2}x^{2^{n-2}-1})+ \\ +\operatorname{tr}_1^n\big(\big(\alpha_{n-1}+\alpha_n^{2^{n-1}}\big)x^{2^{n-1}-1}\big)+\operatorname{tr}_1^n(\alpha_0)x^{2^n-1}. \quad (8)$$

Для нахождения $\operatorname{Ker}\mathcal{G}_\sigma$ требуется определить все $\alpha_0,\ldots,\alpha_n$, для которых функция (8) аффинна. Раскрыв все tr_1^n с переменной и с помощью (3) записав общий полином, получим x в степенях $(2^j-1)\lll i$, где $j\in\{2,\ldots,n-1\}$ и $i\in\{0,\ldots,n-1\}$, причём

$$((2^j-1)\lll i)_{(2)} = (0,\ldots,0,\underbrace{1,\ldots,1}_{j})\lll i.$$

Это означает, что все эти степени попарно различны и не равны 2^n-1, причём их вес больше 1. Тогда единственный способ получить аффинную функцию в (8) — приравнять все коэффициенты нулю, т. е. положить $\alpha_2=\alpha_3=\cdots=\alpha_{n-2}=0$, $\alpha_{n-1}=\alpha_n^{2^{n-1}}$ (отсюда $\alpha_{n-1}^2=\alpha_n$) и $\operatorname{tr}_1^n(\alpha_0)=0$. Таким образом, коэффициенты α_1 и α_{n-1} можно выбрать из $\mathbb{F}_{2^n}$ произвольным образом, для α_0 подходит ровно половина элементов $\mathbb{F}_{2^n}$ в силу линейности tr_1^n, а $\alpha_n=\alpha_{n-1}^2$. Тем самым выражения для ядра $\operatorname{Ker}\mathcal{G}_\sigma$ и его мощности доказаны. Мощность образа, очевидно, находится по формуле $|\operatorname{Im}\mathcal{G}_\sigma| = 2^{n^2+n-(3n-1)} = 2^{(n-1)^2}$. Утверждение 10 доказано.

4. Достижимость нижней оценки ℓ_{2n} числа ближайших бент-функций

В этом разделе усилим результаты [30] о достижимости нижней оценки ℓ_{2n} (см. табл. 1 для $n \leqslant 10$), а также уточним формулу из следствия 1. Напомним, что при $|\mathcal{LA}_n(f)| = \ell_{2n}$ все ближайшие к $f \in \mathcal{M}_{2n}$ бент-функции также лежат в классе $\mathcal{M}_{2n}$.

Таблица 1

Достижимость нижней оценки ℓ_{2n} при $n \leqslant 10$

$2n$	Достижимость ℓ_{2n}	Комментарий
2	Достижима	$\ell_2 = \mathcal{U}_2 = 6$
4	Не достижима	См. [30] или теорему 3
6	Не достижима	Теорема 6
8	Не достижима	См. [30]
10	Достижима	См. [30]
12	Достижима	Эксп. данные для APN-подстановки из [39]
14	Достижима	См. [30]
16	Неизвестно	The big APN problem
18	Неизвестно	Выполнимо ли условие следствия 2?
20	Неизвестно	The big APN problem

4.1. Необходимое условие достижимости ℓ_{2n}. В [30] доказано, что для достижимости ℓ_{2n} необходимо в построении $f \in \mathcal{M}_{2n}$ использовать APN-подстановку, т. е. подстановку π, для которой $\mathcal{L}_2(\pi) = \varnothing$. Далее усилим это условие, уточнив формулу из следствия 1.

Теорема 3. *Пусть $f(x, y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$. Тогда*

$$|\mathcal{LA}_n(f)| = \sum_{k=0}^{n} S_k, \quad S_k = \sum_{L \in \mathcal{L}_k(\pi)} \operatorname{Ind}_{\operatorname{Im} \mathcal{G}_\pi^L}(\varphi|_L) \cdot \left|\operatorname{Ker} \mathcal{G}_\pi^L\right|, \quad 0 \leqslant k \leqslant n,$$

и, в частности,

$$S_0 + S_1 = \ell_{2n}, \quad S_2 = 2^5 \cdot |\mathcal{L}_2(\pi)|,$$
$$S_3 = 2^8 \cdot |\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi)| + 2^9 \cdot |\{L \in \mathcal{LA}_3(\pi) \mid \deg \varphi|_L \leqslant 2\}|.$$

Доказательство. По теореме 2 будем рассматривать подстановку $\pi' \colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ и функцию $\varphi' \in \widetilde{\mathcal{F}}_k$ вместо π и $\varphi|_L$, где $\operatorname{Im} \mathcal{G}_\pi^L = \operatorname{Im} \mathcal{G}_{\pi'} \circ A^{-1}$ для обратимой $A \in \mathcal{A}_k^L$.

При $k \in \{0, 1, 2\}$ подстановка π' аффинна на любом подпространстве $L \in \mathcal{L}_k(\pi)$. Согласно утверждению 8 имеем равенства $\operatorname{Im} \mathcal{G}_{\pi'} = \widetilde{\mathcal{F}}_k$

и $\left|\operatorname{Ker} \mathcal{G}_{\pi'}\right| = 2^{k(k+3)/2}$, т. е. $\operatorname{Im} \mathcal{G}_{\pi}^{L} = \widetilde{\mathcal{F}}_L$. Таким образом,

$$S_0 + S_1 = 2^n \cdot 2^0 + 2^n \cdot \frac{2^n - 1}{2} \cdot 2^2 = \ell_{2n},$$
$$S_2 = |\mathcal{L}_2(\pi)| \cdot 2^5.$$

Если $k = 3$ и π' не аффинна, то $\operatorname{Im} \mathcal{G}_{\pi'} = \widetilde{\mathcal{F}}_3$ и $|\operatorname{Ker} \mathcal{G}_{\pi'}| = 2^8$ в силу утверждения 9, а следовательно, соответствующая часть суммы S_3 равна $|\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi)| \cdot 2^8$.

Если $k = 3$ и подстановка π' аффинна, то $\operatorname{Im} \mathcal{G}_{\pi'} = \{g \in \widetilde{\mathcal{F}}_3 \mid \deg g \leqslant 2\}$ и $|\operatorname{Ker} \mathcal{G}_{\pi'}| = 2^9$ из утверждения 8. При этом $\operatorname{Im} \mathcal{G}_{\pi}^{L} = \operatorname{Im} \mathcal{G}_{\pi'} \circ A^{-1} = \{g \in \widetilde{\mathcal{F}}_L \mid \deg g \leqslant 2\}$, так как степень функции инвариантна относительно обратимого аффинного преобразования $A \in \mathcal{A}_3^L$. Тем самым оставшаяся часть суммы S_3 равна $|\{L \in \mathcal{LA}_3(\pi) \mid \deg \varphi|_L \leqslant 2\}| \cdot 2^9$, что в совокупности даёт искомое число. Теорема 3 доказана.

Сформулируем в виде следствия усиление необходимого условия.

Следствие 2. *Пусть* $f(x, y) = \langle x, \pi(y)\rangle_n \oplus \varphi(y) \in \mathcal{M}_{2n}$, *при этом* $\mathcal{L}_2(\pi) \cup \mathcal{L}_3(\pi) \neq \varnothing$. *Тогда* $|\mathcal{LA}_n(f)| > \ell_{2n}$.

Доказательство. Воспользуемся теоремой 3. Если $\mathcal{L}_2(\pi) \neq \varnothing$ или $\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi) \neq \varnothing$, то очевидно, что $|\mathcal{LA}_n(f)| > \ell_{2n}$. Вместе с тем, если найдётся $L \in \mathcal{LA}_3(\pi)$, то произвольное его аффинное подпространство $U \in \mathcal{AS}_n^2$ принадлежит $\mathcal{LA}_2(\pi) = \mathcal{L}_2(\pi)$, т. е. и в этом случае оценка не достигается. Следствие 2 доказано.

Заметим, что описание подпространств из множества $\mathcal{LA}_n(f)$, построенных при помощи $\mathcal{L}_2(\pi)$, можно найти в [35]. Там же доказано, что $|\mathcal{LA}_n(f)| \geqslant \ell_{2n} + 2^5 \cdot |\mathcal{L}_2(\pi)|$.

4.2. Достаточное условие достижимости ℓ_{2n}. Покажем, как можно построить $f \in \mathcal{M}_{2n}$ с $|\mathcal{LA}_n(f)| = \ell_{2n}$. Определим следующее множество функций из $\mathbb{F}_{2^m}$ в $\mathbb{F}_2$:

$$\mathcal{R}_m = \big\{c_0 + \operatorname{tr}_1^m(c_1 y^{2^1-1} + \cdots + c_{m-1} y^{2^{m-1}-1}) + c_m y^{2^m-1} \mid c_1, \ldots, c_{m-1} \in \mathbb{F}_{2^m},\ c_0, c_m \in \mathbb{F}_2\big\},$$

Нетрудно видеть, что это все функции, эквивалентные ($\simeq$) функциям из множества $\operatorname{Im} \mathcal{G}_\sigma$, приведённого в утверждении 10, поскольку мы добавили произвольную аффинную часть

$$c_0 + \operatorname{tr}_1^m(c_1 x^{2^1-1}) = c_0 + \operatorname{tr}_1^m(c_1 x).$$

Для $\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, $m \mid n$ и $s \in \mathbb{F}_{2^n}$ определим функцию $\varphi_s^m\colon \mathbb{F}_{2^m} \to \mathbb{F}_2$ по правилу

$$\varphi_s^m\colon y \mapsto \varphi(sy), \quad y \in \mathbb{F}_{2^m},$$

т. е. φ_s^m построена по $\varphi|_{s\mathbb{F}_{2^m}}$.

Теорема 4. *Пусть $n = p^k$, где $p \geqslant 5$ простое и $k \geqslant 1$. Для функции $f_\varphi(x, y) = \operatorname{tr}_1^n(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$ равенство $|\mathcal{LA}_n(f_\varphi)| = \ell_{2n}$ имеет место тогда и только тогда, когда $\varphi_s^p \notin \mathcal{R}_p$ для всех $s \in \mathbb{F}_{2^n} \setminus \{0\}$.*

Доказательство. Пусть $\sigma\colon y \mapsto y^{2^n-2}$, $y \in \mathbb{F}_2^n$. Согласно утверждению 3

$$\mathcal{L}_{p^i}(\sigma) = \{s\mathbb{F}_{2^{p^i}} \mid s \in \mathbb{F}_{2^n} \setminus \{0\}\}, \quad i \in \{1, \dots, k\},$$

и $\mathcal{L}_m(\sigma) = \varnothing$ при всех $m \in \{2, \dots, p^k\} \setminus \{p^i\}_{i=1}^k$. Воспользуемся теоремой 3 для вычисления $\mathcal{LA}_n(f_\varphi)$. Определим функцию $A_s\colon \mathbb{F}_{2^{p^i}} \to s\mathbb{F}_{2^{p^i}}$ по правилу $A_s(x) = sx$ для $x \in \mathbb{F}_{2^{p^i}}$. Тогда

$$\varphi|_{s\mathbb{F}_{2^{p^i}}} = \varphi_s^{p^i} \circ A_s^{-1}, \tag{9}$$

а в силу теоремы 2 и утверждения 10 имеем

$$\left[\operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}\right]_\simeq = \mathcal{R}_{p^i} \circ A_s^{-1}, \tag{10}$$

где $\left[\operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}\right]_\simeq$ — множество функций $g\colon s\mathbb{F}_{2^{p^i}} \to \mathbb{F}_2$, эквивалентных ($\simeq$) функциям из $\operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}$.

Пусть $\varphi_s^p \in \mathcal{R}_p$ для некоторого $s \in \mathbb{F}_{2^n} \setminus \{0\}$. Тогда в силу (9) и (10) справедливо $\varphi|_{s\mathbb{F}_{2^{p^i}}} \in \operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}$. Так как $2^{p^i} > 1$, то $|\mathcal{LA}_n(f_\varphi)| > \ell_{2n}$ по теореме 3.

Пусть $\varphi_s^p \notin \mathcal{R}_p$ для всех $s \in \mathbb{F}_{2^n} \setminus \{0\}$. По теореме 3 неравенство $|\mathcal{LA}_n(f_\varphi)| > \ell_{2n}$ возможно только в случае существования $s \in \mathbb{F}_{2^n} \setminus \{0\}$ и $i \in \{1, \dots, k\}$ таких, что $\varphi|_{s\mathbb{F}_{2^{p^i}}} \in \operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^{p^i}}}$, но тогда и $\varphi|_{s\mathbb{F}_{2^p}} \in \operatorname{Im} \mathcal{G}_\sigma^{s\mathbb{F}_{2^p}}$ в силу утверждения 7, поскольку $s\mathbb{F}_{2^p} \subseteq s\mathbb{F}_{2^{p^i}}$ ($\mathbb{F}_{2^p}$ является подполем $\mathbb{F}_{2^{p^i}}$, так как $p \mid p^i$). Отсюда в силу (9) и (10) получаем $\varphi_s^p \in \mathcal{R}_p$; противоречие. Теорема 4 доказана.

Функции φ, о которых идёт речь в теореме 4, нетрудно перечислить конструктивно.

Следствие 3. *Если $m \mid n = p^k$, где $p \geqslant 5$ простое и $k \geqslant 1$, то существует ровно*

$$2\,(2^{2^m-1} - 2^{m^2-m+1})^{\frac{2^n-1}{2^m-1}}$$

функций $\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$, для которых $\varphi_s^m \notin \mathcal{R}_m$ при всех $s \in \mathbb{F}_{2^n} \setminus \{0\}$.

Доказательство. Заметим, что

$$\mathbb{F}_{2^n} = s_1\mathbb{F}_{2^m} \cup \cdots \cup s_t\mathbb{F}_{2^m}$$

для подходящих $s_1, \ldots, s_t \in \mathbb{F}_{2^n}$ и $t = \frac{2^n-1}{2^m-1}$, причём различные $s_i\mathbb{F}_{2^m}$ пересекаются только по нулевому элементу. Следовательно, функцию φ можно «собрать» из функций $\varphi^m_{s_1}, \ldots, \varphi^m_{s_t}$, единственным общим значением которых является значение в нуле.

Значение $\varphi(0) \in \{0, 1\}$ зададим произвольно — для этого имеется два варианта. Таким образом фиксируем

$$\varphi^m_{s_1}(0) = \cdots = \varphi^m_{s_t}(0) = \varphi(0).$$

Остальные значения функции $\varphi^m_{s_1}, \ldots, \varphi^m_{s_t}$ принимают независимо. Заметим также, что $h \in \mathcal{R}_m$ равносильно $h + 1 \in \mathcal{R}_m$, или, что то же самое, $h \in \mathcal{F}_{\mathbb{F}_{2^m}} \setminus \mathcal{R}_m$ равносильно $h + 1 \in \mathcal{F}_{\mathbb{F}_{2^m}} \setminus \mathcal{R}_m$. Тем самым в зависимости от $\varphi(0)$ в качестве подходящей функции $\varphi^m_{s_i}$ можем выбрать одну из половины $\mathcal{F}_{\mathbb{F}_{2^m}} \setminus \mathcal{R}_m$, т. е. имеем

$$2^{2^m-1} - 2^{m^2-m+1}$$

вариантов, так как $|\mathcal{R}_m| = 2^{(m-1)^2} \cdot 2^{m+1}$ по утверждению 10. Поскольку функции из $\mathcal{R}_m$ имеют алгебраическое представление и ограничения касаются только представленных степеней, сделать это нетрудно. Осталось заметить, что нужно задать ровно t таких функций. Следствие 3 доказано.

Равенство $|\mathcal{LA}_n(f_\varphi)| = \ell_{2n}$ также может выполняться для некоторых других составных n и аналогично заданной функции $f_\varphi \in \mathcal{M}_{2n}$ (см. следствие 5 в п. 5.1).

5. Число ближайших бент-функций, близкое к его оценкам

Здесь продемонстрируем другое применение формулы из теоремы 3 (следствия 1). Сосредоточимся на подстановках, размерность ядра и образ которых найдены в разд. 3. Условно разделим их на две части: одни, для которых число ближайших к $f \in \mathcal{M}_{2n}$ бент-функций $|\mathcal{LA}_n(f)|$ близко к нижней оценке ℓ_{2n}, и другие, для которых это число близко к точной верхней оценке

$$\mathcal{U}_{2n} = 2^n(2^1 + 1)(2^2 + 1)\ldots(2^n + 1). \tag{11}$$

Напомним, что верхняя оценка достигается на квадратичных бент-функциях (в том числе из $\mathcal{M}_{2n}$) и только на них [29]. Минимальное значение $|\mathcal{LA}_n(f)|$ из полученных далее равно $\ell_{2n} + o(\ell_{2n})$ при $n \to \infty$, а максимальное — $\frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$ при $n \to \infty$.

5.1. Число ближайших бент-функций, близкое к ℓ_{2n}. Бент-функцию $f \in \mathcal{M}_{2n}$ будем строить с помощью инверсии элементов конечного поля $\mathbb{F}_{2^n}$.

Следствие 4. *Пусть* $f(x,y) = \mathrm{tr}_1^n(xy^{2^n-2})$, *где* $x, y \in \mathbb{F}_{2^n}$. *Тогда*

$$|\mathcal{LA}_n(f)| = 2^{3n-1} + 2^{2n+1} - 2^n + \sum_{\substack{1<k<n:\\ k \mid n}} \frac{2^n-1}{2^k-1} \cdot 2^{3k-1}.$$

Доказательство. По теореме 3 для $k \in \{0,1\}$ имеем $2^{2n+1} - 2^n$ бент-функций. Для $2 \leqslant k \leqslant n$ по утверждению 3 нужно рассмотреть только $k \mid n$, причём $\mathcal{L}_k(\pi) = \{s\mathbb{F}_{2^k} \mid s \in \mathbb{F}_{2^n} \setminus \{0\}\}$. Нетрудно видеть, что $|\mathcal{L}_k(\sigma)| = \frac{2^n-1}{2^k-1}$ для $\sigma\colon x \mapsto x^{2^n-2}$, $x \in \mathbb{F}_{2^n}$. С помощью теоремы 2 для каждого из этих подпространств перейдём к функции обращения в подполе $\mathbb{F}_{2^k}$: положим $\sigma_s = A \circ \pi \circ A\colon \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, где $A\colon x \mapsto sx$, т. е. $\sigma_s\colon x \mapsto x^{2^n-2} = x^{2^k-2}$. Поскольку $\varphi \equiv 0$, её ограничение всегда принадлежит $\mathrm{Im}\ \mathcal{G}_{\sigma_s}$. Наконец, $|\mathrm{Ker}\ \mathcal{G}_{\sigma_s}| = 2^{3k-1}$ по утверждению 10. Следствие 4 доказано.

Число из следствия 4 заметно больше нижней оценки. Однако для любого n существует бент-функция $f \in \mathcal{M}_{2n}$, для которой $|\mathcal{LA}_n(f)|$ имеет ту же асимптотику, что и ℓ_{2n}.

Теорема 5. *Существует функция* $f(x,y) = \mathrm{tr}_1^n(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$, *для которой* $|\mathcal{LA}_n(f)| < 2^{2n+1} + 81 \cdot 2^n - 82$, *т. е.* $|\mathcal{LA}_n(f)| = \ell_{2n} + o(\ell_{2n})$ *при* $n \to \infty$.

Доказательство. Используя теорему 3, для функции $\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ найдём число бент-функций, ближайших к $f(x,y) = \mathrm{tr}_1^n(x\sigma(y)) + \varphi(y)$, $\sigma(y) = y^{2^n-2}$, и не учтённых в оценке ℓ_{2n}. При этом усреднив его по множеству всех таких функций φ, получим

$$\begin{aligned}
M_n &= 2^{-2^n} \sum_{\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2} \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\sigma^L}(\varphi|_L) \cdot \left|\mathrm{Ker}\ \mathcal{G}_\sigma^L\right| = \\
&= 2^{-2^n} \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} \left|\mathrm{Ker}\ \mathcal{G}_\sigma^L\right| \sum_{\varphi\colon \mathbb{F}_{2^n} \to \mathbb{F}_2} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\sigma^L}(\varphi|_L) = \\
&= 2^{-2^n} \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} \left|\mathrm{Ker}\ \mathcal{G}_\sigma^L\right| \cdot \left|\mathrm{Im}\ \mathcal{G}_\sigma^L\right| \cdot 2^{k+1} \cdot 2^{2^n-2^k} = \\
&= \sum_{k=2}^{n} \sum_{L \in \mathcal{L}_k(\sigma)} 2^{k^2+k} \cdot 2^{k+1} \cdot 2^{-2^k} = \sum_{k=2}^{n} |\mathcal{L}_k(\sigma)| \cdot 2^{(k+1)^2-2^k}.
\end{aligned}$$

Здесь $\sum\limits_{\varphi} \mathrm{Ind}_{\mathrm{Im}\ \mathcal{G}_\sigma^L}(\varphi|_L) = \left|\mathrm{Im}\ \mathcal{G}_\sigma^L\right| \cdot 2^{k+1} \cdot 2^{2^n-2^k}$ в силу того, что в образ $\mathrm{Im}\ \mathcal{G}_\sigma^L$ включены функции с точностью до аффинной части, а вне подпространства L функцию φ можно задать произвольным образом.

Далее воспользуемся утверждением 3:

$$M_n = \sum_{k\geqslant 2:\ k\,|\,n} \frac{2^n-1}{2^k-1} 2^{(k+1)^2-2^k} = (2^n-1) \sum_{k\geqslant 2:\ k\,|\,n} \frac{2^{(k+1)^2-2^k}}{2^k-1}. \qquad (12)$$

Приведём значения $N_k = \frac{2^{(k+1)^2-2^k}}{2^k-1}$ для малых k:

$$N_2 = \frac{32}{3}, \quad N_3 = \frac{256}{7}, \quad N_4 = \frac{512}{15},$$
$$N_5 = \frac{16}{31}, \quad N_6 = \frac{1}{63\cdot 2^{15}}, \quad N_7 = \frac{1}{127\cdot 2^{64}}.$$

Оценим M_n сверху:

$$M_n < (2^n-1)\left(\sum_{k=2}^{5} N_k + \sum_{k=6}^{\infty} 2^{(k+1)^2-2^k-k+1}\right) < 82\,(2^n-1). \qquad (13)$$

Действительно, вторая часть суммы не превосходит $2N_6$, так как очевидно, что $N_{k+1} < \frac{1}{2}N_k$ при $k \geqslant 6$, при этом $N_2 + N_3 + N_4 + N_5 = 10 + \frac{2}{3} + 36 + \frac{4}{7} + 34 + \frac{2}{15} + \frac{16}{31} < 82 - 2N_6$.

Поскольку M_n — среднее значение по всем функциям φ, хотя бы для одной из них усредняемое число не превосходит M_n, в противном случае среднее значение было бы больше. Теорема 5 доказана.

Таким образом, при любом n можно найти бент-функцию $f \in \mathcal{M}_{2n}$, для которой среди её ближайших бент-функций не более $82\,(2^n-1)$ лежат вне $\mathcal{M}_{2n}$ (см. утверждение 2). В некоторых случаях теорема 5 влечёт достижимость ℓ_{2n}.

Следствие 5. *Пусть m — минимальный нетривиальный делитель n, $m \geqslant 6$ и $n \leqslant 2^m - m^2 - m - 3$. Тогда найдётся бент-функция $f(x,y) = \mathrm{tr}_1^n(xy^{2^n-2}) + \varphi(y) \in \mathcal{M}_{2n}$, для которой справедливо $|\mathcal{LA}_n(f)| = \ell_{2n}$.*

Доказательство. Поскольку $m \geqslant 6$, в силу (12) и (13) справедливо

$$M_n < (2^n-1)\sum_{k=m}^{\infty} 2^{(k+1)^2-2^k-k+1} < 2^n \cdot 2 \cdot 2^{(m+1)^2-2^m-m+1}.$$

Тем самым при $n \leqslant 2^m + m - (m+1)^2 - 2 = 2^m - m^2 - m - 3$ получаем $M_n < 1$. Однако M_n — среднее значение, поэтому усредняемое число хотя бы для одной из функции φ не превосходит M_n и, следовательно, равно 0. Следствие 5 доказано.

Условию на n из следствия 5 удовлетворяют числа $11 \cdot 13$, $11 \cdot 11 \cdot 13$, $11 \cdot 17$ и т. п., что дополняет результаты п. 4.2.

5.2. Число ближайших бент-функций, близкое к $\mathcal{U}_{2n}$. Для удобства в качестве подстановки π будем рассматривать тождественное отображение, т. е. речь пойдёт о функциях вида $f(x,y) = \langle x, y\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$. Можно легко расширить этот подкласс без изменения $|\mathcal{LA}_n(f)|$.

Утверждение 11. *Пусть бент-функции $f, g \in \mathcal{M}_{2n}$ имеют вид*

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

подстановка π аффинна и $\deg(\varphi \oplus \psi) \leqslant 2$. Тогда f и g имеют одинаковое число ближайших к ним бент-функций.

Доказательство. По утверждению 8 в $\operatorname{Im} \mathcal{G}_\pi^L$ лежат все функции $h\colon L \to \mathbb{F}_2$ степени не выше 2, $\left|\operatorname{Ker} \mathcal{G}_\pi^L\right|$ зависит только от размерности L, а любое $L \in \mathcal{S}_n^k$ принадлежит $\mathcal{L}_k(\pi)$, поэтому по формуле из теоремы 3 получаем равенство $|\mathcal{LA}_n(f)| = |\mathcal{LA}_n(g)|$. Утверждение 11 доказано.

Мощность $\mathcal{LA}_n(f)$ можно вычислить через ограничения функции φ на подпространства $L \in \mathcal{AS}_n^k$, которые имеют степень не выше 2.

Следствие 6. *Пусть $f(x,y) = \langle x, y\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$. Тогда*

$$|\mathcal{LA}_n(f)| = \sum_{k=0}^{n} \left|\left\{L \in \mathcal{AS}_n^k \mid \deg \varphi|_L \leqslant 2\right\}\right| \cdot 2^{\frac{k(k+3)}{2}}.$$

Доказательство. По условию $\pi\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — тождественное отображение. Воспользуемся теоремой 2. Для этого рассмотрим обратимую аффинную функцию $A\colon \mathbb{F}_2^k \to L$ и положим $B = A^{-1}$, так что получим $\varphi' = \varphi|_L \circ A$, а $\pi' = A^{-1} \circ \pi|_L \circ A\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ — также тождественное отображение. По утверждению 8 имеем $\operatorname{Im} \mathcal{G}_{\pi'} = \{\varphi' \in \widetilde{\mathcal{F}}_k \mid \deg \varphi' \leqslant 2\}$ и $|\operatorname{Ker} \mathcal{G}_{\pi'}| = 2^{\frac{k(k+3)}{2}}$, но степени $\varphi' = \varphi|_L \circ A$ и $\varphi|_L$ совпадают, так как A — невырожденное аффинное преобразование. Финальная формула получается из теоремы 3. Следствие 6 доказано.

Напрямую воспользоваться формулой из следствия 6 трудно, однако это можно сделать для следующего узкого класса бент-функций.

Следствие 7. *Пусть $f(x,y) = \langle x, y\rangle \oplus y_1 y_2 \dots y_m \in \mathcal{M}_{2n}$, $3 \leqslant m \leqslant n$. Тогда*

$$|\mathcal{LA}_n(f)| =$$
$$= \sum_{k=0}^{n} \left(2^{n-k} \cdot \left|\mathcal{S}_n^k\right| - \sum_{t=t_*(k)}^{t^*(k)} \left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t+1)(n-m-t)} \right) \cdot 2^{\frac{k(k+3)}{2}} =$$

$$= \mathcal{U}_{2n} - \sum_{k=0}^{n} \sum_{t=t_*(k)}^{t^*(k)} \left|\mathcal{S}_{n-m}^{t}\right| \cdot \left|\mathcal{S}_{m}^{k-t}\right| \cdot 2^{(k-t+1)(n-m-t)} \cdot 2^{\frac{k(k+3)}{2}},$$

где $t_*(k) = \max\{0,\, k-m\}$, $t^*(k) = \min\{n-m,\, k-3\}$ *для* $k \in \{0, \ldots, n\}$.

Доказательство. Чтобы применить формулу из следствия 6, для каждого $k \in \{0, \ldots, n\}$ найдём число подпространств $L \in \mathcal{AS}_n^k$, для которых $\deg \varphi|_L \leqslant 2$ при $\varphi(y) = y_1 \ldots y_m$. Подсчитаем число L, для которых $\deg \varphi|_L \geqslant 3$, а затем вычтем его из $2^{n-k}\left|\mathcal{S}_n^k\right|$ — числа всех подпространств размерности k.

Без ограничения общности конъюнкцию $y_1 \ldots y_m$ заменим конъюнкцией $y_{n-m+1} \ldots y_n$, являющейся характеристической функцией подпространства $Z = \mathbb{F}_2^{n-m} \times \{1\}^m \in \mathcal{AS}_n^{n-m}$. Заметим, что $\varphi|_L(y) = 1$, если и только если $y \in L \cap Z = T$, причём это пересечение либо пусто, либо принадлежит $\mathcal{AS}_n^t$ для некоторого $t \in \{0, \ldots, n-m\}$. Таким образом, функция $\varphi|_L$ характеристическая для T, а её степень равна $k-t$. Значит, нам нужны подпространства T размерности $t \leqslant k-3$, точнее $t \leqslant \min\{k-3,\, n-m\}$.

Подсчитаем число $L \in \mathcal{AS}_n^k$ таких, что $\dim L \cap Z = t \leqslant k-3$. Нетрудно видеть, что оно равно числу подпространств $[L] \in \mathcal{S}_n^k$, пересекающихся с $[Z]$ по подпространству размерности t, умноженному на 2^{n-m-t} — именно столькими способами можно выбрать аффинное подпространство пространства L с фиксированной линейной частью.

Воспользуемся представлением линейных подпространств из п. 2.1: $L = \mathcal{S}(U, V, H) \subseteq \mathbb{F}_2^{n-m} \times \mathbb{F}_2^m$, где $U \in \mathcal{S}_m^{k-r}$, $V \in \mathcal{S}_{n-m}^r$ и $H \in \mathcal{A}_U^{n-m}/\mathcal{A}_U^V$ линейная (см. замечание 2). Согласно утверждению 4 имеем равенство $V \times \{0\}^m = [L] \cap [Z]$, т. е. $r = t$. Таких V ровно $\left|\mathcal{S}_{n-m}^t\right|$. Далее, $\left|\mathcal{S}_m^{k-t}\right|$ способами можем выбрать подпространство U и $2^{(k-t)(n-m-t)}$ способами — одну из попарно неэквивалентных функций H (см. замечание 1), так что в итоге получаем

$$\left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t)(n-m-t)}$$

вариантов выбора $[L]$. Отсюда находим число способов выбрать L:

$$2^{n-m-t} \cdot \left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t)(n-m-t)} = \left|\mathcal{S}_{n-m}^t\right| \cdot \left|\mathcal{S}_m^{k-t}\right| \cdot 2^{(k-t+1)(n-m-t)},$$

при этом $t \geqslant k-m$, поскольку $\dim U = \dim L - \dim V = k - t \leqslant m$ (см. утверждение 4). Полученное выражение суммируем по t от $\max\{0, k-m\}$ до $\min\{k-3,\, n-m\}$ и вычтем из $|\mathcal{AS}_n^k| = 2^{n-k}\left|\mathcal{S}_n^k\right|$. В результате приходим к первому равенству для $|\mathcal{LA}_n(f)|$ из условия теоремы.

Осталось заметить, что

$$\sum_{k=0}^{n} 2^{n-k} \cdot \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}} = \mathcal{U}_{2n}. \tag{14}$$

Действительно, с одной стороны, по теореме 3 левая часть (14) равна $|\mathcal{LA}_n(g)|$ для квадратичной функции $g(x,y)=\langle x,y\rangle$ от $2n$ переменных. С другой стороны, $|\mathcal{LA}_n(g)|=\mathcal{U}_{2n}$ согласно [28]. Следствие 7 доказано.

Замечание 4. В условии следствия 7

1) вместо $y_1\dots y_m$ можно взять Ind_S для любого $S\in\mathcal{AS}_n^{n-m}$;

2) при $m=n$ и $m=n-1$ формулы справедливы для бент-функций $f(x,y)=\langle x,y\rangle\oplus\varphi(y)\in\mathcal{M}_{2n}$ таких, что $\mathrm{wt}(\varphi)=1$ и $\mathrm{wt}(\varphi)=2$ соответственно.

Формулы из следствия 7 весьма полезны, поскольку дают представление $|\mathcal{LA}_n(f)|$ через гауссовы коэффициенты

$$\left|\mathcal{S}_n^k\right|=\prod_{i=0}^{k-1}\frac{2^n-2^i}{2^k-2^i},\quad 0\leqslant k\leqslant n.$$

Для $m\in\{3,n\}$ можно получить ещё более простые выражения.

Следствие 8. *Пусть бент-функции $f_3,f_n\in\mathcal{M}_{2n}$, $n\geqslant 3$, имеют вид*

$$f_3(x,y)=\langle x,y\rangle\oplus y_1y_2y_3,\quad f_n(x,y)=\langle x,y\rangle\oplus y_1y_2\dots y_n.$$

Тогда

$$|\mathcal{LA}_n(f_3)|=\mathcal{U}_{2n}-2^{4n-3}(2^1+1)(2^2+1)\dots(2^{n-3}+1),$$

$$|\mathcal{LA}_n(f_n)|=(2^n-1)\prod_{k=2}^{n}(2^k+1)+\frac{32}{3}(2^{2n-1}+1)-3\cdot 2^{n+2}-3,$$

при этом $|\mathcal{LA}_n(f_3)|=o(\mathcal{U}_{2n})$, $|\mathcal{LA}_n(f_n)|=\frac{1}{3}\mathcal{U}_{2n}+o(\mathcal{U}_{2n})$ при $n\to\infty$.

Доказательство. Легко видеть, что при $3\leqslant k\leqslant n$

$$\sum_{t=t_*(k)}^{t^*(k)}\left|\mathcal{S}_{n-m}^t\right|\cdot\left|\mathcal{S}_m^{k-t}\right|\cdot 2^{(k-t+1)(n-m-t)}=\begin{cases}\left|\mathcal{S}_{n-3}^{k-3}\right|\cdot 2^{4(n-k)} & \text{для } m=3,\\ \left|\mathcal{S}_n^k\right| & \text{для } m=n,\end{cases}$$

а при $0\leqslant k\leqslant 2$ эта сумма равна нулю.

Случай 1: $m=3$. В силу следствия 7

$$|\mathcal{LA}_n(f_3)|=\mathcal{U}_{2n}-\sum_{k=3}^{n}\left|\mathcal{S}_{n-3}^{k-3}\right|\cdot 2^{4(n-k)}\cdot 2^{\frac{k(k+3)}{2}}.$$

Заменой индекса $k\to k+3$ сумма в правой части приводится к виду

$$\sum_{k=3}^{n}\left|\mathcal{S}_{n-3}^{k-3}\right|\cdot 2^{4(n-k)}\cdot 2^{\frac{k(k+3)}{2}}=\sum_{k=0}^{n-3}\left|\mathcal{S}_{n-3}^{k}\right|2^{4(n-k-3)}\cdot 2^{\frac{(k+3)(k+6)}{2}}=$$

$$= \sum_{k=0}^{n-3} \left|\mathcal{S}_{n-3}^k\right| \cdot 2^{4(n-3)-4k+3(k+3)} \cdot 2^{\frac{k(k+3)}{2}} = 2^{3n} \sum_{k=0}^{n-3} \left|\mathcal{S}_n^k\right| \cdot 2^{n-3-k} \cdot 2^{\frac{k(k+3)}{2}} \overset{(14)}{=}$$

$$\overset{(14)}{=} 2^{3n}\,\mathcal{U}_{2(n-3)} = 2^{3n} \cdot 2^{n-3}(2^1+1)(2^2+1)\dots(2^{n-3}+1),$$

откуда $|\mathcal{LA}_n(f_3)| = \mathcal{U}_{2n} - 2^{3n}\,\mathcal{U}_{2(n-3)} = o(\mathcal{U}_{2n})$ при $n \to \infty$.

Случай 2: $m = n$. В силу следствия 7 имеем

$$|\mathcal{LA}_n(f_n)| = 2^n(2^1+1)\dots(2^n+1) - \sum_{k=0}^{n} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}} + \sum_{k=0}^{2} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}},$$

где последнее слагаемое равно

$$1 + (2^n-1)\cdot 2^2 + \frac{(2^n-1)(2^n-2)}{(2^2-1)(2^2-2)} \cdot 2^5 = \frac{32}{3}(2^{2n-1}+1) - 3\cdot 2^{n+2} - 3.$$

Упростим второе слагаемое

$$P(n) = \sum_{k=0}^{n} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}}.$$

Аналогично выводу равенства (14) в [28], применим очевидное свойство

$$\left|\mathcal{S}_n^k\right| = \left|\mathcal{S}_{n-1}^k\right| + 2^{n-k}\left|\mathcal{S}_{n-1}^{k-1}\right|, \quad 1 \leqslant k \leqslant n,$$

где по определению $\left|\mathcal{S}_{n-1}^n\right| = 0$. Поскольку $\left|\mathcal{S}_n^0\right| = \left|\mathcal{S}_{n-1}^0\right| = 1$, получаем

$$P(n) = \sum_{k=0}^{n} \left|\mathcal{S}_n^k\right| \cdot 2^{\frac{k(k+3)}{2}} =$$

$$= \sum_{k=0}^{n-1} \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{k(k+3)}{2}} + \sum_{k=1}^{n} 2^{n-k} \cdot \left|\mathcal{S}_{n-1}^{k-1}\right| \cdot 2^{\frac{k(k+3)}{2}} =$$

$$= \{k \to k+1\} = P(n-1) + \sum_{k=0}^{n-1} 2^{n-1-k} \cdot \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{(k+1)(k+4)}{2}} =$$

$$= P(n-1) + 2^{n+1} \sum_{k=0}^{n-1} \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{k^2+5k+4-2k-4}{2}} =$$

$$= P(n-1) + 2^{n+1} \sum_{k=0}^{n-1} \left|\mathcal{S}_{n-1}^k\right| \cdot 2^{\frac{k(k+3)}{2}} = (1+2^{n+1})P(n-1).$$

Таким образом, $P(n) = (2^{n+1}+1)P(n-1)$ и $P(0) = 1$, откуда

$$P(n) = (2^2+1)(2^3+1)\dots(2^{n+1}+1),$$

$$2^n(2^1+1)\dots(2^n+1) - P(n) = (2^2+1)\dots(2^n+1)(3\cdot 2^n - 2^{n+1} - 1).$$

Суммируя найденные слагаемые, приходим к требуемой формуле для $|\mathcal{LA}_n(f_n)|$, из которой нетрудно видеть, что $|\mathcal{LA}_n(f_n)| = \frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$ при $n \to \infty$. Следствие 8 доказано.

Заметим, что $|\mathcal{LA}_n(f_n)| > |\mathcal{LA}_n(f_3)|$ при $n \geqslant 4$, хотя в этом случае $\deg f_3 = 3 < \deg f_n = n$, и вообще $|\mathcal{LA}_n(f_3)| = o(|\mathcal{LA}_n(f_n)|)$ при $n \to \infty$.

Интересно, что имеется ещё одна неквадратичная бент-функция, для которой ожидаемое число ближайших бент-функций велико, имеет их столько же, сколько и f_n.

Утверждение 12. *Пусть $f_\tau(x, y) = \langle x, \tau(y)\rangle \in \mathcal{M}_{2n}$, где τ — транспозиция на $\mathbb{F}_2^n$, переставляющая векторы $(1, \ldots, 1, 0)$ и $(1, \ldots, 1, 1)$ друг с другом. Тогда $|\mathcal{LA}_n(f_\tau)| = |\mathcal{LA}_n(f_n)|$.*

Доказательство. Нетрудно видеть, что

$$\tau(y) = y \oplus (0, \ldots, 0, y_1 \ldots y_{n-1}).$$

Действительно, если $(y_1, \ldots, y_{n-1}) \neq (1, \ldots, 1)$, то $\tau(y) = y$. Иначе получаем $\tau(1, \ldots, 1, 0) = (1, \ldots, 1, 0 \oplus 1)$ и $\tau(1, \ldots, 1, 1) = (1, \ldots, 1, 1 \oplus 1)$, что соответствует определению τ. Следовательно,

$$f_\tau(x, y) = \langle x, y\rangle \oplus x_n(y_1 \ldots y_{n-1}) = x_1y_1 \oplus \cdots \oplus x_ny_n \oplus y_1 \ldots y_{n-1}x_n.$$

Таким образом, переставив переменные x_n и y_n, получим в точности f_n и $|\mathcal{LA}_n(f_\tau)| = |\mathcal{LA}_n(f_n)|$. Утверждение 12 доказано.

Замечание 5. В условии утверждения 12 можно считать, что τ — произвольная транспозиция на $\mathbb{F}_2^n$, поскольку все f_τ EA-эквивалентны друг другу и, следовательно, имеют одинаковые $|\mathcal{LA}_n(f_\tau)|$. Для доказательства достаточно привести транспозицию τ к указанной в утверждении при помощи композиции $A \circ \tau \circ B$, где $A, B\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ — некоторые обратимые аффинные преобразования. Также в условии утверждения 12 вместо транспозиции можно рассматривать саму приведённую композицию для произвольных транспозиции τ и обратимых аффинных A, B.

Согласно следствиям 1, 8 и утверждению 12 функции f_n и f_τ дают наиболее интуитивно очевидные способы построить бент-функции с максимально возможной $|\mathcal{LA}_n(f)|$ среди неквадратичных функций $f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y) \in \mathcal{M}_{2n}$: либо выбираем тождественную (аффинную) подстановку π и минимально отличающуюся от тождественно нулевой функцию φ, либо, наоборот, выбираем тождественно нулевую φ и минимально отличающуюся от тождественной (аффинной) π. Эти рассуждения, а также принцип построения $\mathcal{M}_{2n}$, позволяют сделать предположение.

Гипотеза 1. *Пусть f — бент-функция от $2n$ переменных и $\deg f \geqslant 3$. Тогда $|\mathcal{LA}_n(f)| \leqslant |\mathcal{LA}_n(f_n)|$.*

6. Классификация бент-функций из $\mathcal{M}_6$

Теорема 3 (следствие 1) позволяет классифицировать $f \in \mathcal{M}_6$ на основе $|\mathcal{LA}_3(f)|$. Начнём с мощности $\mathcal{L}_2(\pi)$ для подстановок π на $\mathbb{F}_2^3$. Обратим также внимание, что возможные значения $|\mathcal{L}_{n-1}(\pi)|$ для подстановок π на $\mathbb{F}_2^n$ (без классификации π) были получены в работе [36].

Утверждение 13. *Пусть $\pi\colon \mathbb{F}_2^3 \to \mathbb{F}_2^3$ взаимно однозначна. Тогда*

$$|\mathcal{L}_2(\pi)| = \begin{cases} 0, & \text{если } \delta(\pi) = 2, \\ 2, & \text{если } \delta(\pi) = 4, \\ 6, & \text{если } \delta(\pi) = 8 \text{ и } \pi \notin \mathcal{A}_3^3, \\ 14, & \text{если } \pi \in \mathcal{A}_3^3. \end{cases}$$

Других взаимно однозначных функций π нет.

Доказательство. 1. По одному из определений APN-подстановки π выполнено $\mathcal{L}_2(\pi) = \varnothing$.

2. Пусть $\delta(\pi) = 4$. Все $L \in \mathcal{L}_2(\pi)$ являются гиперплоскостями в $\mathbb{F}_2^3$, т. е. $L \in \mathcal{L}_2(\pi)$ тогда и только тогда, когда его сдвиг $\mathbb{F}_2^3 \setminus L \in \mathcal{L}_2(\pi)$.

Далее от противного: пусть есть различные $L, U \in \mathcal{L}_2(\pi)$, не являющиеся сдвигами друг друга. В этом случае $|V = L \cap U| = 2$. Обозначим $V = \{a,\, a \oplus v\}$, $a, v \in \mathbb{F}_2^3$ и $\pi(V) = \{\pi(a),\, \pi(a) \oplus v')\}$, $v' \in \mathbb{F}_2^3$. Тогда $L \setminus V = \{b,\, b \oplus v\}$ и $U \setminus V = \{c,\, c \oplus v\}$ для некоторых $b, c \in \mathbb{F}_2^3$, так как L и U — аффинные подпространства $\mathbb{F}_2^3$ и сумма всех их элементов должна быть равна 0. То же самое верно и для образов: $\pi(L) \setminus \pi(V) = \{b', b' \oplus v'\}$ и $\pi(U) \setminus \pi(V) = \{c', c' \oplus v'\}$, $b', c' \in \mathbb{F}_2^3$. В результате уравнение $\pi(x) \oplus \pi(x \oplus v) = v'$ имеет как минимум шесть решений a, $a \oplus v$, b, $b \oplus v$, c, $c \oplus v$, а это противоречит тому, что $\delta(\pi) = 4$. При этом $\delta(\pi) \neq 2$, откуда $|\mathcal{L}_2(\pi)| > 0$. Следовательно, $\mathcal{L}_2(\pi) = \{L,\, \mathbb{F}_2^3 \setminus L\}$ для некоторого L.

3. Пусть $\delta(\pi) = 8$ и π не аффинна, т. е. производная π по некоторому ненулевому направлению является константой, или, другими словами, подстановка π имеет непустую линейную структуру. Все такие функции можно аффинными преобразованиями привести к следующей (см., например, [8]):

$$\pi'(x) = qx_1x_2 + sx_3 + t = \pi(xB \oplus b), \quad x \in \mathbb{F}_2^3,$$

где $q, s, t \in \mathbb{F}_2^3$, $q \neq 0$, двоичная матрица B невырожденная и имеет порядок 3, $b \in \mathbb{F}_2^3$. Ясно, что $|\mathcal{L}_2(\pi)| = |\mathcal{L}_2(\pi')|$, поэтому далее вместо π будем рассматривать π'.

Очевидно, что $L \in \mathcal{L}_2(\pi)$ тогда и только тогда, когда $\pi|_L$ аффинна. Значит, в полиноме Жегалкина $\pi|_L$ нет квадратичного слагаемого x_1x_2. Тем самым $\mathcal{L}_2(\pi)$ состоит из всех таких $L \in \mathcal{AS}_3^2$, на которых функция $g(x) = x_1x_2$ аффинна.

Производное подпространство $L \in \mathcal{AS}_3^2$ можно задать уравнением $a_1x_1 \oplus a_2x_2 \oplus a_3x_3 = c$, причём различным парам $a \in \mathbb{F}_2^3$, $c \in \mathbb{F}_2$ соответствуют различные подпространства. Нам подходят L, заданные уравнениями $x_1 = c$, $x_2 = c$ и $x_1 \oplus x_2 = c$. Действительно, если $a_3 = 1$, то $L = \{(x_1, x_2, a_1x_1 \oplus a_2x_2 \oplus c) \in \mathbb{F}_2^3 \mid x_1, x_2 \in \mathbb{F}_2\}$ и $g|_L$ не аффинна. Таким образом, $\mathcal{L}_2(\pi)$ состоит из $3 \cdot 2 = 6$ элементов.

4. Очевидно, так как подстановка π аффинна на всех аффинных подпространствах размерности 2, которых в $\mathbb{F}_2^3$ имеется $7 \cdot 2 = 14$.

5. В силу взаимной однозначности функции π получаем $\deg \pi \leqslant 2$, поэтому её производные $\pi(x) \oplus \pi(x \oplus a)$ по всем направлениям $a \in \mathbb{F}_2^3$ аффинны. Тем самым число решений уравнений $\pi(x) \oplus \pi(x \oplus a) = b$ принадлежит множеству $\{0, 2, 4, 8\}$. Поскольку $\delta(\pi) \geqslant 2$, рассмотрены все возможные случаи. Утверждение 13 доказано.

Приведём классификацию функций $f \in \mathcal{M}_6$ относительно $|\mathcal{LA}_3(f)|$.

Теорема 6. *Пусть* $f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y) \in \mathcal{M}_6$. *Тогда*

$$|\mathcal{LA}_3(f)| = \begin{cases} 376, & \text{если } \delta(\pi) = 2, \\ 440, & \text{если } \delta(\pi) = 4, \\ 568, & \text{если } \delta(\pi) = 8 \text{ и } \pi \notin \mathcal{A}_3^3, \\ 568, & \text{если } \pi \in \mathcal{A}_3^3 \text{ и } \deg \varphi = 3, \\ 1080 = \mathcal{U}_6, & \text{если } \pi \in \mathcal{A}_3^3 \text{ и } \deg \varphi \leqslant 2. \end{cases}$$

Доказательство. По теореме 3

$$|\mathcal{LA}_3(f)| = \ell_6 + 2^5 \cdot |\mathcal{L}_2(\pi)| + 2^8 \cdot |\mathcal{L}_3(\pi) \setminus \mathcal{LA}_3(\pi)| + \\ + 2^9 \cdot |\{L \in \mathcal{LA}_3(\pi) \mid \deg \varphi|_L \leqslant 2\}|. \quad (15)$$

Здесь $\ell_6 = 120$, а $|\mathcal{L}_2(\pi)|$ найдена в утверждении 13. Далее, $\mathcal{L}_3(\pi) = \{\mathbb{F}_2^3\}$, так как $n = 3$. Наконец, очевидно, что $\mathcal{LA}_3(\pi) = \mathcal{L}_3(\pi)$, если π аффинна, и $\mathcal{LA}_3(\pi) = \varnothing$ иначе. Подстановкой найденных чисел в формулу (15) получаем требуемое равенство. Теорема 6 доказана.

Теорема 6 даёт также классификацию функций из $\mathcal{M}_6$ относительно EA-эквивалентности (см., например, работу [40] о методах классификации булевых функций в общем случае). Действительно, число $|\mathcal{LA}_n(f)|$ бент-функций на расстоянии 2^n от f является инвариантом функции $f \in \mathcal{M}_{2n}$ относительно EA-эквивалентности. При этом в [1] доказано, что множество бент-функций от 6 переменных разбивается на 4 класса EA-эквивалентности. Таким образом, эти 4 класса представлены в теореме 6, и каждому из них соответствует своё значение $|\mathcal{LA}_3(f)|$.

Заключение

Предложенный в работе подход к перечислению бент-функций, ближайших к заданной функции из класса Мэйорана — МакФарланда $\mathcal{M}_{2n}$, обладает следующими достоинствами.

• Обеспечивает возможность подсчёта их точного числа для ряда функций с определёнными симметриями.

• Позволяет расширить известные необходимое и достаточное условия достижимости нижней оценки ℓ_{2n} для их числа.

• На основе свойств класса $\mathcal{M}_{2n}$ для функции степени 3 и выше выдвинута гипотеза, ограничивающая число ближайших к ней бент-функций величиной $\frac{1}{3}\mathcal{U}_{2n} + o(\mathcal{U}_{2n})$.

Остаётся простор для дальнейших исследований, в ходе которых возможно установить другие примечательные свойства этого класса бент-функций (см., например, [35]).

Финансирование работы

Исследование выполнено при поддержке Математического центра в Академгородке (соглашение № 075–15–2025–349 с Министерством науки и высшего образования Российской Федерации). Дополнительных грантов на проведение или руководство этим исследованием получено не было.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Литература

1. **Rothaus O.** On "bent" functions // J. Comb. Theory. Ser. A. 1976. V. 20, No. 3. P. 300–305. DOI: 10.1016/0097-3165(76)90024-8.
2. **Tokareva N. N.** Bent functions: Results and applications to cryptography. Amsterdam: Acad. Press, 2015. 220 p. DOI: 10.1016/c2014-0-02922-x.
3. **Токарева Н. Н.** Бент-функции: результаты и приложения. Обзор работ // Прикл. дискрет. математика. 2009. № 1. С. 15–37. DOI: 10.17223/20710410/3/2.
4. **Токарева Н. Н.** Обобщения бент-функций. Обзор работ // Дискрет. анализ и исслед. операций. 2010. Т. 17, № 1. С. 34–64.
5. **Helleseth T., Kholosha A.** Bent functions and their connections to combinatorics // Surveys in combinatorics 2013. Cambridge: Camb. Univ. Press, 2013. P. 91–126. (Lond. Math. Soc. Lect. Notes Ser.; V. 409). DOI: 10.1017/CBO9781139506748.004.
6. **Dobbertin H., Leander G.** A survey of some recent results on bent functions // Sequences and their applications — SETA 2004. Proc. Int. Conf. (Seoul, Korea, Oct. 24–28, 2005). Heidelberg: Springer, 2005. P. 1–29. (Lect. Notes Comput. Sci.; V. 3486). DOI: 10.1007/11423461_1.

7. **Mesnager S.** Bent functions: Fundamentals and results. Cham: Springer, 2018. 570 p. DOI: 10.1007/978-3-319-32595-8.
8. **Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. 584 с.
9. **Logachev O. A., Salnikov A. A., Yashchenko V. V.** Boolean functions in coding theory and cryptography. Providence, RI: AMS, 2012. 334 p.
10. **Агибалов Г. П.** Избранные теоремы начального курса криптографии. Томск: Изд. дом ТГУ, 2005. 112 с.
11. **Панкратова И. А.** Булевы функции в криптографии. Томск: Изд. дом ТГУ, 2014. 88 с.
12. **Токарева Н. Н.** Симметричная криптография: Краткий курс. Новосибирск: НГУ, 2012. 234 с.
13. **Cusick T. W., Stanica P.** Cryptographic Boolean functions and applications. Amsterdam: Acad. Press, 2017. 275 p. DOI: 10.1016/c2016-0-00852-5.
14. **Carlet C.** Boolean functions for cryptography and coding theory. Cambridge: Camb. Univ. Press, 2020. 562 p. DOI: 10.1017/9781108606806.
15. **McFarland R. L.** A family of difference sets in non-cyclic groups // J. Comb. Theory. Ser. A. 1973. V. 15, No. 1. P. 1–10. DOI: 10.1016/0097-3165(73)90031-9.
16. **Dillon J. F.** Elementary Hadamard difference sets: PhD thesis. College Park, 1974.
17. **Коломеец Н. А., Павлов А. В.** Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. математика. 2009. № 4. С. 5–20.
18. **Carlet C.** Two new classes of bent functions // Advances in cryptology — EUROCRYPT'93. Proc. Workshop on the Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 77–101. (Lect. Notes Comput. Sci.; V. 765). DOI: 10.1007/3-540-48285-7_8.
19. **Zhang F., Pasalic E., Cepak N., Wei Y.** Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class // Codes, cryptology and information security. Proc. 2nd Int. Conf. (Rabat, Morocco, Apr. 10–12, 2017). Cham: Springer, 2017. P. 298–313. (Lect. Notes Comput. Sci.; V. 10194). DOI: 10.1007/978-3-319-55589-8_20.
20. **Zhang F., Cepak N., Pasalic E., Wei Y.** Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$ // Discrete Appl. Math. 2020. V. 285. P. 458–472. DOI: 10.1016/j.dam.2020.06.012.
21. **Kudin S., Pasalic E.** A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$ // Des. Codes Cryptogr. 2022. V. 90, No. 8. P. 1783–1796. DOI: 10.1007/s10623-022-01079-3.
22. **Kudin S., Pasalic E., Cepak N., Zhang F.** Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class // Cryptogr. Commun. 2022. V. 14, No. 1. P. 101–116. DOI: 10.1007/s12095-021-00523-w.

23. Bapić A, Pasalic E., Zhang F., Hodžić S. Constructing new superclasses of bent functions from known ones // Cryptogr. Commun. 2022. V. 14, No. 6. P. 1229–1256. DOI: 10.1007/s12095-022-00566-7.

24. Pasalic E., Bapić A., Zhang F., Wei Y. Explicit infinite families of bent functions outside the completed Maiorana–McFarland class // Des. Codes Cryptogr. 2023. V. 91, No. 7. P. 2365–2393. DOI: 10.1007/s10623-023-01204-w.

25. Pasalic E., Polujan A., Kudin S., Zhang F. Design and analysis of bent functions using $\mathcal{M}$-subspaces // IEEE Trans. Inf. Theory. 2024. V. 70, No. 6. P. 4464–4477. DOI: 10.1109/TIT.2024.3352824.

26. Kudin S., Pasalic E., Polujan A., Zhang F. The algebraic characterization of $\mathcal{M}$-subspaces of bent concatenations and its application // IEEE Trans. Inf. Theory. 2025. V. 71, No. 5. P. 3999–4011. DOI: 10.1109/TIT.2025.3547533.

27. Polujan A. A., Pott A. Cubic bent functions outside the completed Maiorana–McFarland class // Des. Codes Cryptogr. 2020. V. 88, No. 9. P. 1701–1722. DOI: 10.1007/s10623-019-00712-y.

28. Коломеец Н. А. Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискрет. анализ и исслед. операций. 2012. Т. 19, № 1. С. 41–58.

29. Kolomeec N. The graph of minimal distances of bent functions and its properties // Des. Codes Cryptogr. 2017. V. 85, No. 3. P. 395–410. DOI: 10.1007/s10623-016-0306-4.

30. Быков Д. А., Коломеец Н. А. О нижней оценке числа бент-функций на минимальном расстоянии от бент-функции из класса Мэйорана — Мак-Фарланда // Дискрет. анализ и исслед. операций. 2023. Т. 30, № 3. С. 57–80.

31. Nyberg K. Differentily uniform mappings for cryptography // Advances in cryptology — EUROCRYPT'93. Proc. Workshop Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 55–64. (Lect. Notes Comput. Sci.; V. 765). DOI: 10.1007/3-540-48285-7_6.

32. Carlet C. Open questions on nonlinearity and on APN functions // Arithmetic of finite fields. Rev. Sel. Pap. 5th Int. Workshop (Gebze, Turkey, Sept. 27–28, 2014). Cham: Springer, 2015. P. 83–107. (Lect. Notes Comput. Sci.; V. 9061). DOI: 10.1007/978-3-319-16277-5_5.

33. Jacobson N. Basic algebra. V. I. Mineola, NY: Dover Publ., 2009. 528 p.

34. Kolomeec N. A., Bykov D. A. On the image of an affine subspace under the inverse function within a finite field // Des. Codes Cryptogr. 2024. V. 92, No. 2. P. 467–476. DOI: 10.1007/s10623-023-01316-3.

35. Kolomeec N. A., Bykov D. A. On the Maiorana–McFarland class extensions. Ithaca, NY, 2025. 29 p. (e-Print Archive / Cornell Univ.; arXiv:2503.21440). DOI: 10.48550/arXiv.2503.21440.

36. Clark W. E., Hou X., Mihailovs A. The affinity of a permutation of a finite vector space // Finite Fields Appl. 2007. V. 13. P. 80–112. DOI: 10.1016/j.ffa.2005.07.004.

37. Li S., Meidl W., Polujan A., Pott A., Riera C., Stănică P. Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application // IEEE Trans. Inf. Theory. 2020. V. 66, No. 11. P. 7101–7112. DOI: 10.1109/TIT.2020.3002993.

38. Коломеец Н. А. О подстановках, разрушающих структуру подпространств определённых размерностей // Прикл. дискрет. математика. 2024. № 65. С. 5–20. DOI: 10.17223/20710410/65/1.

39. Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J. An APN permutation in dimension six // Finite fields: Theory and applications. Proc. 9th Int. Conf. (Dublin, Ireland, July 13–17, 2009). Providence, RI: AMS, 2010. P. 33–42. (Contemp. Math.; V. 518). DOI: 10.1090/conm/518/10194.

40. Черёмушкин А. В. Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. Т. 4. М.: Физматлит, 2001. С. 273–314.

Быков Денис Александрович
Коломеец Николай Александрович

Статья поступила
27 августа 2024 г.
После доработки —
26 марта 2025 г.
Принята к публикации
22 июня 2025 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2025. Vol. 32, No. 3. P. 5–42

UDC 519.7 DOI: 10.33048/daio.2025.32.811

ON THE BENT FUNCTIONS CLOSEST TO A GIVEN MAIORANA–MCFARLAND BENT FUNCTION

D. A. Bykov[a] and *N. A. Kolomeec*[b]

Novosibirsk State University,
2 Pirogov Street, 630090 Novosibirsk, Russia
E-mail: [a] den.bykov.2000i@gmail.com, [b] nkolomeec@gmail.com

Abstract. Bent functions of $2n$ variables closest to a given bent function in the Maiorana–McFarland class are considered. The known criterion for their construction is revised and the method of calculating their number is refined. We investigate functions such that the number of closest bent functions is approximate to its lower and sharp upper bounds. The existence of bent functions whose number of closest bent functions has the same asymptotics as the lower bound is proven. Examples of functions in the Maiorana–McFarland class are given for which the calculated number of closest bent functions is close to the upper bound. Attainability of the lower bound is considered, and known necessary and sufficient conditions are refined. We show that the lower bound is attained for n equaled to a power of a prime $p \geqslant 5$, as well as for some other n. A complete classification of functions of 6 variables in the Maiorana–McFarland class using the number of closest bent functions is obtained. Tab. 1, bibliogr. 40.

Keywords: bent function, Boolean function, affine subspace, minimum distance, Maiorana–McFarland class.

References

1. **O. Rothaus,** On "bent" functions, *J. Comb. Theory, Ser. A*, **20** (3), 300–305 (1976), DOI: 10.1016/0097-3165(76)90024-8.
2. **N. N. Tokareva,** *Bent Functions: Results and Applications to Cryptography* (Acad. Press, Amsterdam, 2015), DOI: 10.1016/c2014-0-02922-x.
3. **N. N. Tokareva,** Bent functions: Results and applications. A survey, *Prikl. Diskretn. Mat.*, No. 1, 15–37 (2009) [Russian], DOI: 10.17223/20710410/3/2.

English transl.: *Journal of Applied and Industrial Mathematics* **19** (3) (2025).

4. **N. N. Tokareva,** Generalizations of bent functions. A survey, *Diskretn. Anal. Issled. Oper.* **17** (1), 34–64 (2010) [Russian] [*J. Appl. Ind. Math.* **5** (1), 110–129 (2011), DOI: 10.1134/S1990478911010133].
5. **T. Helleseth** and **A. Kholosha,** Bent functions and their connections to combinatorics, in *Surveys in Combinatorics 2013* (Camb. Univ. Press, Cambridge, 2013), pp. 91–126 (Lond. Math. Soc. Lect. Notes Ser., Vol. 409), DOI: 10.1017/CBO9781139506748.004.
6. **H. Dobbertin** and **G. Leander,** A survey of some recent results on bent functions, in *Sequences and Their Applications — SETA 2004*, Proc. Int. Conf. (Seoul, Korea, Oct. 24–28, 2005) (Springer, Heidelberg, 2005), pp. 1–29 (Lect. Notes Comput. Sci., Vol. 3486), DOI: 10.1007/11423461_1.
7. **S. Mesnager,** *Bent Functions: Fundamentals and Results* (Springer, Cham, 2018), DOI: 10.1007/978-3-319-32595-8.
8. **O. A. Logachev, A. A. Salnikov, S. V. Smyshlyaev,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptography* (MTsNMO, Moscow, 2012) [Russian].
9. **O. A. Logachev, A. A. Salnikov,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptography* (AMS, Providence, RI, 2012).
10. **G. P. Agibalov,** *Selected Theorems of an Introductory Cryptography Course* (Izd. Dom TGU, Tomsk, 2005) [Russian].
11. **I. A. Pankratova,** *Boolean Functions in Cryptography* (Izd. Dom TGU, Tomsk, 2014) [Russian].
12. **N. N. Tokareva,** *Symmetric Cryptography: A Brief Course* (NGU, Novosibirsk, 2012) [Russian].
13. **T. W. Cusick** and **P. Stanica,** *Cryptographic Boolean Functions and Applications* (Acad. Press, Amsterdam, 2017), DOI: 10.1016/c2016-0-00852-5.
14. **C. Carlet,** *Boolean Functions for Cryptography and Coding Theory* (Camb. Univ. Press, Cambridge, 2020), DOI: 10.1017/9781108606806.
15. **R. L. McFarland,** A family of difference sets in non-cyclic groups, *J. Comb. Theory, Ser. A*, **15** (1), 1–10 (1973), DOI: 10.1016/0097-3165(73)90031-9.
16. **J. F. Dillon,** Elementary Hadamard difference sets, *PhD Thesis* (College Park, 1974).
17. **N. A. Kolomeec** and **A. V. Pavlov,** Properties of bent functions with minimal distance, *Prikl. Diskretn. Mat.*, No. 4, 5–20 (2009) [Russian].
18. **C. Carlet,** Two new classes of bent functions, in *Advances in Cryptology — EUROCRYPT'93*, Proc. Workshop on the Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 77–101 (Lect. Notes Comput. Sci., Vol. 765), DOI: 10.1007/3-540-48285-7_8.
19. **F. Zhang, E. Pasalic, N. Cepak,** and **Y. Wei,** Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana–McFarland class, in *Codes, Cryptology and Information Security*, Proc. 2nd Int. Conf. (Rabat, Morocco, Apr. 10–12, 2017) (Springer, Cham, 2017), pp. 298–313 (Lect. Notes Comput. Sci., Vol. 10194), DOI: 10.1007/978-3-319-55589-8_20.

20. **F. Zhang, N. Cepak, E. Pasalic,** and **Y. Wei,** Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$, *Discrete Appl. Math.* **285**, 458–472 (2020), DOI: 10.1016/j.dam.2020.06.012.

21. **S. Kudin** and **E. Pasalic,** A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$, *Des. Codes Cryptogr.* **90** (8), 1783–1796 (2022), DOI: 10.1007/s10623-022-01079-3.

22. **S. Kudin, E. Pasalic, N. Cepak,** and **F. Zhang,** Permutations without linear structures inducing bent functions outside the completed Maiorana–McFarland class, *Cryptogr. Commun.* **14** (1), 101–116 (2022), DOI: 10.1007/s12095-021-00523-w.

23. **A Bapić, E. Pasalic, F. Zhang, S. Hodžić** Constructing new superclasses of bent functions from known ones, *Cryptogr. Commun.* **14** (6), 1229–1256 (2022), DOI: 10.1007/s12095-022-00566-7.

24. **E. Pasalic** and **A. Bapić, F. Zhang, Y. Wei** Explicit infinite families of bent functions outside the completed Maiorana–McFarland class, *Des. Codes Cryptogr.* **91** (7), 2365–2393 (2023), DOI: 10.1007/s10623-023-01204-w.

25. **E. Pasalic, A. Polujan, S. Kudin,** and **F. Zhang,** Design and analysis of bent functions using $\mathcal{M}$-subspaces, *IEEE Trans. Inf. Theory* **70** (6), 4464–4477 (2024), DOI: 10.1109/TIT.2024.3352824.

26. **S. Kudin, E. Pasalic, A. Polujan,** and **F. Zhang,** The algebraic characterization of $\mathcal{M}$-subspaces of bent concatenations and its application, *IEEE Trans. Inf. Theory* **71** (5), 3999–4011 (2025), DOI: 10.1109/TIT.2025.3547533.

27. **A. A. Polujan** and **A. Pott,** Cubic bent functions outside the completed Maiorana–McFarland class, *Des. Codes Cryptogr.* **88** (9), 1701–1722 (2020), DOI: 10.1007/s10623-019-00712-y.

28. **N. A. Kolomeec,** Enumeration of the bent functions of least deviation from a quadratic bent function, *Diskretn. Anal. Issled. Oper.* **19** (1), 41–58 (2012) [Russian] [*J. Appl. Ind. Math.* **6** (3), 306–317 (2012), DOI: 10.1134/S1990478912030052].

29. **N. Kolomeec,** The graph of minimal distances of bent functions and its properties, *Des. Codes Cryptogr.* **85** (3), 395–410 (2017), DOI: 10.1007/s10623-016-0306-4.

30. **D. A. Bykov** and **N. A. Kolomeec,** On a lower bound for the number of bent functions at the minimum distance from a bent function in the Maiorana–McFarland class, *Diskretn. Anal. Issled. Oper.* **30** (3), 57–80 (2023) [Russian] [*J. Appl. Ind. Math.* **17** (3) 507–520 (2023)].

31. **K. Nyberg,** Differentily uniform mappings for cryptography, in *Advances in Cryptology — EUROCRYPT'93*, Proc. Workshop Theory and Application of Cryptographic Techniques (Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 55–64 (Lect. Notes Comput. Sci., Vol. 765), DOI: 10.1007/3-540-48285-7_6.

32. **C. Carlet,** Open questions on nonlinearity and on APN functions, in *Arithmetic of Finite Fields*, Rev. Sel. Pap. 5th Int. Workshop (Gebze, Turkey, Sept. 27–28, 2014) (Springer, Cham, 2015), pp. 83–107 (Lect. Notes Comput. Sci., Vol. 9061), DOI: 10.1007/978-3-319-16277-5_5.

33. N. Jacobson, *Basic Algebra*, V. I (Dover Publ., Mineola, NY, 2009).
34. N. A. Kolomeec and **D. A. Bykov,** On the image of an affine subspace under the inverse function within a finite field, *Des. Codes Cryptogr.* **92** (2), 467–476 (2024), DOI: 10.1007/s10623-023-01316-3.
35. N. A. Kolomeec and **D. A. Bykov,** On the Maiorana–McFarland class extensions (Ithaca, NY, 2025) (e-Print Archive / Cornell Univ., arXiv:2503.21440), DOI: 10.48550/arXiv.2503.21440.
36. W. E. Clark, X. Hou, and **A. Mihailovs,** The affinity of a permutation of a finite vector space, *Finite Fields Appl.* **13**, 80–112 (2007), DOI: 10.1016/j.ffa.2005.07.004.
37. S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, and **P. Stănică,** Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application, *IEEE Trans. Inf. Theory* **66** (11), 7101–7112 (2020), DOI: 10.1109/TIT.2020.3002993.
38. N. A. Kolomeec, On permutations that break subspaces of specified dimensions, *Prikl. Diskretn. Mat.*, No. 65, 5–20 (2024) [Russian], DOI: 10.17223/20710410/65/1.
39. K. A. Browning, J. F. Dillon, M. T. McQuistan, and **A. J. Wolfe,** An APN permutation in dimension six, in *Finite Fields: Theory and Applications*, Proc. 9th Int. Conf. (Dublin, Ireland, July 13–17, 2009) (AMS, Providence, RI, 2010), pp. 33–42 (Contemp. Math., Vol. 518), DOI: 10.1090/conm/518/10194.
40. A. V. Cheryomushkin, Methods for affine and linear classification of Boolean functions, in *Transactions on Discrete Mathematics*, Vol. 4 (Fizmatlit, Moscow, 2001) [Russian], pp. 273–314.

Denis A. Bykov
Nikolay A. Kolomeec

Received August 27, 2024
Revised March 26, 2025
Accepted June 22, 2025