

СВОЙСТВА ПОДФУНКЦИЙ САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ¹

А. В. Куценко

Бент-функция называется самодуальной, если она совпадает со своей дуальной бент-функцией. Исследованы подфункции самодуальных бент-функций, полученные фиксацией первой переменной, а также первых двух переменных. Для описания подфункций от $n - 1$ переменной введено понятие самодуальности почти бент-функции от нечётного числа переменных. Доказано, что между множествами самодуальных бент-функций от n переменных и почти бент-функций от $n - 1$ переменной существует взаимно однозначное соответствие. Получено достаточное условие того, что подфункции от $n - 2$ переменных самодуальной бент-функции являются бент-функциями. Предложен ряд новых итеративных конструкций бент-функций. Получена новая итеративная нижняя оценка числа самодуальных бент-функций.

Ключевые слова: самодуальная бент-функция, подфункция, почти бент-функция, отношение Рэлея.

Через $\mathbb{F}_2^n$ обозначим линейное пространство всех двоичных векторов длины n над полем $\mathbb{F}_2$. Булевой функцией от n переменных называется отображение вида $\mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Множество всех булевых функций от n переменных обозначается через $\mathcal{F}_n$. Характеристическим вектором (характеристической последовательностью) булевой функции $f \in \mathcal{F}_n$ называется вектор

$$F \equiv (-1)^f = ((-1)^{f(0)}, (-1)^{f(1)}, \dots, (-1)^{f(2^n-1)}) \in \{\pm 1\}^{2^n},$$

где $(f(0), f(1), \dots, f(2^n - 1)) \in \mathbb{F}_2^{2^n}$ — вектор значений функции f . Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y \rangle$ обозначим значение $\bigoplus_{i=1}^n x_i y_i$. Преобразование Уолша — Адамара булевой функции f от n переменных называется целочисленной функцией $W_f : \mathbb{F}_2^n \rightarrow \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}, \quad y \in \mathbb{F}_2^n.$$

Булева функция g от нечётного числа переменных m называется почти бент-функцией, если $W_g(y) \in \{0, \pm 2^{(m+1)/2}\}$ для каждого $y \in \mathbb{F}_2^m$. Булева функция f от чётного числа переменных n называется почти бент-функцией, если $W_f(y) \in \{0, \pm 2^{(n+2)/2}\}$ для каждого $y \in \mathbb{F}_2^n$.

Булева функция f от чётного числа переменных n называется бент-функцией, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [1]. Для множества бент-функций от n переменных используется обозначение $\mathcal{B}_n$. Для каждой $f \in \mathcal{B}_n$ из соотношения $W_f(y) = (-1)^{\tilde{f}(y)} 2^{n/2}$ однозначным образом определяется дуальная к ней бент-функция $\tilde{f} \in \mathcal{B}_n$, значения которой находятся из соответствия для каждого $y \in \mathbb{F}_2^n$. Бент-функция f называется самодуальной (антисамодуальной), если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). Множество самодуальных бент-функций от n переменных обозначаются через $\mathcal{SB}_n^+$.

Открытой проблемой является полная характеристизация и описание класса самодуальных бент-функций. Данные вопросы исследовались в ряде работ. В частности, в [2]

¹Работа выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2022-281.

приведена аффинная классификация самодуальных бент-функций от 2, 4, 6 переменных и всех квадратичных самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность. В работе [3] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных относительно преобразования, сохраняющего самодуальность, можно найти в [4]. В работах [5, 6] представлены конструкции самодуальных бент-функций.

В настоящей работе исследованы подфункции самодуальных бент-функций, полученные фиксацией первой переменной, а также первых двух переменных. Другими словами, если $\mathbf{f}$ — вектор значений булевой функции f , то упомянутые подфункции есть в точности булевы функции с векторами значений f_i в представлении $\mathbf{f} = (f_0, f_1, \dots, f_{2^k-1})$ для $k = 1, 2$ соответственно. Предложены новые конструкции, а также новая итеративная нижняя оценка числа самодуальных бент-функций.

1. Подфункции от $n - 1$ переменной

Известно, что подфункции от $n - 1$ переменной каждой бент-функции являются почти бент-функциями, при этом носители их спектров Уолша — Адамара не пересекаются [7].

Отношением Рэлея булевой функции f от n переменных называется число

$$S_f = \sum_{x, y \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(y) \oplus \langle x, y \rangle} = \sum_{y \in \mathbb{F}_2^n} (-1)^{f(y)} W_f(y).$$

Применительно к бент-функциям данная характеристика изучалась в работе [8]. Она представляет интерес в силу того, что число S_f полностью характеризует расстояние Хэмминга между бент-функцией и дуальной к ней. Заметим, что задача поиска максимального (минимального) значения отношения Рэлея решена лишь для случая чётного числа переменных. Для нечётного случая она является открытой проблемой.

Известно [2], что для каждой булевой функции f от чётного числа n переменных справедливо $|S_f| \leq 2^{3n/2}$, при этом равенство достигается в том и только в том случае, когда f — самодуальная $(+2^{3n/2})$ или антисамодуальная $(-2^{3n/2})$ бент-функция. Нетрудно видеть, что в случае чётного числа переменных экстремальные значения отношения Рэлея достигаются лишь на тех булевых функциях, для которых $(-1)^{f(y)} W_f(y) = 2^{n/2}$ или $(-1)^{f(y)} W_f(y) = -2^{n/2}$ при каждом $y \in \mathbb{F}_2^n$.

Введём следующее понятие самодуальности почти бент-функции от нечётного числа переменных. Пусть m — нечётное положительное число. Почти бент-функцию g от m переменных будем называть *самодуальной*, если

$$(-1)^{g(y)} W_g(y) \geq 0 \text{ для любого } y \in \mathbb{F}_2^m.$$

В свою очередь, функция g называется *антисамодуальной* почти бент-функцией, если

$$(-1)^{g(y)} W_g(y) \leq 0 \text{ для любого } y \in \mathbb{F}_2^m.$$

Содержательно оба определения описывают ситуации, когда знаки коэффициентов Уолша — Адамара и значения характеристического вектора почти бент-функции согласованы. Можно показать, что

Утверждение 1. Пусть g — почти бент-функция от m переменных, тогда

$$|S_g| \leq 2^{(3m-1)/2},$$

при этом равенство достигается, если и только если g — самодуальная $(+2^{(3m-1)/2})$ или антисамодуальная $(-2^{(3m-1)/2})$ почти бент-функция.

То есть (анти-)самодуальные почти бент-функции от нечётного числа переменных на множестве почти бент-функций, так же как и самодуальные бент-функции на множестве булевых функций от чётного числа переменных, являются экстремальными объектами в спектральном смысле.

Понятия самодуальности для чётного и нечётного числа переменных тесно связаны, что показывает следующая

Теорема 1. Между множествами самодуальных бент-функций от $n \geq 4$ переменных и множеством (анти-)самодуальных почти бент-функций от $n - 1$ переменных существует взаимно однозначное соответствие.

Упомянутая связь устанавливается на основе отображения, которое каждой самодуальной бент-функции ставит в соответствие её подфункцию, получаемую фиксацией первой координаты.

Таким образом, подфункциями от $n - 1$ переменной, получаемыми фиксацией первой координаты, являются самодуальные почти бент-функции, и только они.

2. Свойства подфункций от $n - 2$ переменных

Известно [9], что для каждой бент-функции от n переменных все её подфункции от $n - 2$ переменных имеют одинаковые спектры Уолша — Адамара. Более того, все подфункции являются бент-функциями, либо все являются почти бент-функциями, либо их спектры Уолша — Адамара состоят из чисел $0, \pm 2^{(n-2)/2}, \pm 2^{n/2}$.

Случай, когда все подфункции являются бент-функциями, ведёт к итеративной конструкции бент функции от $n + 2$ переменных на основе четырёх бент-функций от n переменных. В работе [10] найдены необходимые и достаточные условия того, что конкатенация векторов значений четырёх бент-функций от n переменных даёт вектор значений бент-функции от $n + 2$ переменных.

Известны две итеративные конструкции самодуальных бент-функций от $n + 2$ переменных, в основе которых лежит конкатенация четырёх векторов значений бент-функций от n переменных. Они представлены ниже:

- конструкция **C1**: $(h, \tilde{h}, \tilde{h}, h \oplus 1)$, где h — бент-функция от n переменных [2];
- конструкция **C2**: $(f, g \oplus 1, g, f)$, где f — самодуальная, а g — антисамодуальная бент-функции от n переменных [11].

Сумма мощностей данных непересекающихся конструкций **C1** и **C2** даёт нижнюю оценку $|\mathcal{B}_{n-2}| + |\mathcal{SB}_{n-2}^+|^2$ числа самодуальных бент-функций. Прямые вычисления показывают, что данная оценка превосходит другие известные оценки.

Очевидно, что для обеих конструкций характеристические векторы подфункций образуют линейно зависимые множества. В настоящей работе доказано утверждение, обобщающее данный факт:

Теорема 2. Если характеристические векторы подфункций f_0, f_1, f_2, f_3 самодуальной бент-функции f линейно зависимы, то данные подфункции являются бент-функциями.

Теорема 2 даёт достаточное условие того, что все подфункции, полученные фиксацией первых двух переменных, являются бент-функциями.

Отметим, что для случая $n = 4$ данное условие также является достаточным.

3. Новые конструкции и оценка числа самодуальных бент-функций

В настоящей работе мы предлагаем три новых конструкции **С3**, **С4** и **С5** самодуальных бент-функций. В данных конструкциях используются бент-функции от $n - 4$ переменных. Пусть h — бент-функция от $n - 4$ переменных, f — самодуальная и g — антисамодуальная бент-функции от $n - 4$ переменных. Опишем конструкции:

— **С3**: вектор значений функции имеет вид

$$(h, g, g \oplus 1, h, \tilde{h}, f, f \oplus 1, \tilde{h}, \tilde{h}, f \oplus 1, f, \tilde{h}, h \oplus 1, g, g \oplus 1, h \oplus 1);$$

все подфункции от $n - 2$ переменных являются бент-функциями;

— **С4**: вектор значений функции имеет вид

$$(h, g, \tilde{h}, f, g \oplus 1, h, f \oplus 1, \tilde{h}, \tilde{h}, f \oplus 1, h \oplus 1, g, f, \tilde{h}, g \oplus 1, h \oplus 1);$$

подфункции от $n - 2$ переменных являются бент-функциями тогда и только тогда, когда $h \oplus \tilde{h} \oplus f \oplus g = 0$. Таким образом, данная конструкция даёт класс самодуальных бент-функций, которые нельзя представить в виде конкатенации четырёх бент-функций;

— **С5**: вектор значений функции имеет вид

$$(h, h \oplus 1, \tilde{h}, \tilde{h}, h, h, \tilde{h} \oplus 1, \tilde{h}, \tilde{h}, \tilde{h}, h \oplus 1, h, \tilde{h} \oplus 1, \tilde{h}, h \oplus 1, h \oplus 1);$$

все подфункции от $n - 2$ переменных являются бент-функциями.

На основе анализа данных конструкций получена

Теорема 3. Число самодуальных бент-функций от $n \geq 6$ переменных не меньше чем

$$|\mathcal{B}_{n-2}| + |\mathcal{SB}_{n-2}^+|^2 + |\mathcal{B}_{n-4}| \left(2|\mathcal{SB}_{n-4}^+|^2 + 1 \right) - 2|\mathcal{SB}_{n-4}^+|.$$

Таким образом, известная итеративная нижняя оценка увеличивается на слагаемое, соответствующее самодуальным бент-функциям от $n - 4$ переменных.

4. Линейная независимость характеристических векторов подфункций

Конструкции, предложенные в работе, позволяют однозначно ответить на вопрос о возможности обращения теоремы 2 для случая $n \geq 6$.

Теорема 4. Для каждого чётного $n \geq 6$ существуют самодуальные бент-функции от n переменных, подфункции которых образуют линейно независимые множества векторов.

Таким образом, обращение теоремы 2 не имеет места при $n \geq 6$, то есть линейная зависимость характеристических векторов не является необходимым условием, а обеспечивает лишь *достаточное* условие того, что подфункции от $n - 2$ переменных являются бент-функциями.

ЛИТЕРАТУРА

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. Carlet C., Danielsen L. E., Parker M. G., and Solé P. Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. V. 1. P. 384–399.
3. Hou X.-D. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. No. 2. P. 183–198.

4. Feulner T., Sok L., Solé P., and Wassermann A. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. No. 1. P. 395–406.
5. Luo G., Cao X., and Mesnager S. Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. 2019. V. 11. No. 6. P. 1261–1273.
6. Li Y., Kan H., Mesnager S., et al. Generic constructions of (Boolean and vectorial) bent functions and their consequences // IEEE Trans. Inform. Theory. 2022. V. 68. No. 4. P. 2735–2751.
7. Wolfmann A. Special bent and near-bent functions // Adv. Math. Commun. 2014. V. 8. No. 1. P. 21–33.
8. Danielsen L. E., Parker M. G., and Solé P. The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.
9. Canteaut A. and Charpin P. Decomposing bent functions // IEEE Trans. Inf. Theory. 2003. V. 49. No. 8. P. 2004–2019.
10. Preneel B., Van Leekwijck W., Van Linden L., et al. Propagation characteristics of Boolean functions // LNCS. 1990. V. 473. P. 161–173.
11. Kutsenko A. Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.

УДК 519.7

DOI 10.17223/2226308X/15/8

ГЕНЕРАЦИЯ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ С НЕВЫРОЖДЕННЫМИ КООРДИНАТНЫМИ ФУНКЦИЯМИ

И. А. Панкратова, Е. А. Рубан, С. В. Чикалова

Предложен алгоритм генерации обратимой векторной булевой функции, все координатные функции которой существенно зависят от всех переменных.

Ключевые слова: векторные булевы функции, подстановки, существенная зависимость функции от переменных.

Обозначим через $P_2(n)$ множество всех булевых функций от n переменных. Говорят, что переменная x_i , $1 \leq i \leq n$, *существенна для функции* $f(x_1, \dots, x_n) \in P_2(n)$ (f существенно зависит от переменной x_i), если найдётся пара наборов $a, b \in \mathbb{Z}_2^n$, соседних по i -й координате, такая, что $f(a) \neq f(b)$; будем называть такую пару наборов *доказывающей существенность переменной x_i для функции f* (или просто *доказывающей парой*, если из контекста ясно, о каких переменной и функции идёт речь). Переменная, от которой функция не зависит существенно, называется *фиктивной для этой функции*; функции, существенно зависящие от всех переменных, — *невырожденными*.

Векторной булевой функцией $((n, m) -)$ называется отображение $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$. Такую функцию можно рассматривать как упорядоченный набор из m булевых функций f_i , $i = 1, \dots, m$, которые называются *координатными функциями*: $F = (f_1 \dots f_m)$.

Оценим вероятность того, что случайно сгенерированная векторная булева функция невырожденная. По формуле включений и исключений определим D_n — количество функций в $P_2(n)$, имеющих фиктивные переменные:

$$D_n = \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} 2^{2^{n-i}}.$$

Вероятность того, что булева функция от n переменных невырожденная, равна

$$P_n = 1 - D_n / 2^{2^n}. \quad (1)$$