УДК 519.7 DOI 10.17223/2226308X/15/7

СВОЙСТВА ПОДФУНКЦИЙ САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ[1]

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 $\mathbb{F}_2^n \to \mathbb{F}_2$. 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

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

где $(f(0), f(1), \ldots, f(2^n-1)) \in \mathbb{F}_2^{2^n}$ — вектор значений функции f. Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначим значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, 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 $W_f(y) \in \left\{0, \pm 2^{(m+1)/2}\right\}$ для каждого $y \in \mathbb{F}_2^n$. Булева функция f от чётного числа переменных n называется *почти бент-функцией*, если $W_f(y) \in \left\{0, \pm 2^{(n+2)/2}\right\}$ 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 $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$ однозначным образом определяется *дуальная* к ней бент-функция $\widetilde{f} \in \mathcal{B}_n$, значения которой находятся из соответствия для каждого $y \in \mathbb{F}_2^n$. Бент-функция f называется *самодуальной* (*антисамодуальной*), если $f = \widetilde{f}$ (соответственно $f = \widetilde{f} \oplus 1$). Множество самодуальных бент-функций от n переменных обозначаются через $\mathcal{SB}_n^+$.

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

[1]Работа 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 $\mathbf{f} = (f_0, f_1, \ldots, f_{2^k-1})$ 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 $|S_f| \leqslant 2^{3n/2}$, при этом равенство достигается в том и только в том случае, когда f — самодуальная $\left(+2^{3n/2}\right)$ или антисамодуальная $\left(-2^{3n/2}\right)$ 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

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

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

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

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

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

при этом равенство достигается, если и только если g — самодуальная $\left(+2^{(3m-1)/2}\right)$ или антисамодуальная $\left(-2^{(3m-1)/2}\right)$ 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 следущая

Теорема 1. Между множествами самодуальных бент-функций от $n \geqslant 4$ 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**: $\left(h, \widetilde{h}, \widetilde{h}, h \oplus 1\right)$, 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 $|\mathcal{B}_{n-2}| + \left|\mathcal{SB}^{+}_{n-2}\right|^2$ числа самодуальных бент-функций. Прямые вычисления показывают, что данная оценка превосходит другие известные оценки.

Очевидно, что для обоих 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 **C3**, **C4** и **C5** 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:

— **C3**: вектор значений функции имеет вид

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

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

— **C4**: вектор значений функции имеет вид

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

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

— **C5**: вектор значений функции имеет вид

$$\big(h, h\oplus 1, \widetilde{h}, \widetilde{h}, h, h, \widetilde{h}\oplus 1, \widetilde{h}, \widetilde{h}, \widetilde{h}, h\oplus 1, h, \widetilde{h}\oplus 1, \widetilde{h}, h\oplus 1, h\oplus 1\big);$$

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

На основе анализа данных конструкций получена

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

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

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 $n\geqslant 6$.

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

Таким образом, обращение теоремы 2 не имеет места при $n\geqslant 6$, 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.