УДК 519.7 DOI 10.17223/2226308X/11/13

О НЕКОТОРЫХ СВОЙСТВАХ САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Найдены необходимые и достаточные условия самодуальности бент-функций, построенных с помощью итеративной конструкции $\mathcal{BI}$ (Канто А., Шарпин П., 2003), позволяющей при выполнении определённых условий, используя четыре бент-функции от n переменных, построить бент-функцию от $n+2$ переменных. Получено, что количество самодуальных бент-функций от $n+2$ переменных, которые могут быть построены с помощью данной конструкции, оценивается снизу суммой числа бент-функций от n переменных и квадрата мощности множества самодуальных бент-функций от n переменных. Предложена итеративная конструкция самодуальных бент-функций. Доказано, что существуют самодуальные бент-функции всех возможных для бент-функций степеней. Доказано, что минимальное расстояние Хэмминга между самодуальными бент-функциями равно $2^{n/2}$. Доказано, что множества самодуальных и антисамодуальных бент-функций являются метрически регулярными.

Ключевые слова: *булева функция, бент-функция, итеративная конструкция бент-функций, самодуальная бент-функция, метрически регулярное множество.*

Булевой функцией f называется любое отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Скалярным произведением* $\langle x, y\rangle$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n, y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ называется 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 $W_f(y) = \sum\limits_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,y\rangle}$. 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 $\mathcal{B}_n$. Булева функция $\tilde{f}$ называется *дуальной* к бент-функции f, если $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ для каждого $x \in \mathbb{F}_2^n$. Бент-функция f называется *самодуальной* (*антисамодуальной*), если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). Множества самодуальных и антисамодуальных бент-функций от n переменных обозначаются через $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ соответственно. *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается $\mathrm{dist}(f, g)$. *Степенью* булевой функции называется максимальная из степеней мономов, входящих с ненулевыми коэффициентами в её алгебраическую нормальную форму (АНФ, полином Жегалкина).

Всюду далее предполагается, что n — чётное натуральное число.

В [2] исследованы ограничения бент-функций на подпространства коразмерности 2 и их сдвиги и установлена связь между максимальной нелинейностью получаемых подфункций и второй производной дуальной функции. На основании данного результата была предложена итеративная конструкция бент-функций от $n+2$ переменных из четырёх бент-функций f_0, f_1, f_2, f_3 от n переменных: $f(a, b, x) = f_{a+2b}(x)$, где $a, b \in \mathbb{F}_2$; $x \in \mathbb{F}_2^n$. Известно [3], что функция f является бент-функцией от $n+2$ переменных в том и только в том случае, когда $\widetilde{f_0}(x) \oplus \widetilde{f_1}(x) \oplus \widetilde{f_2}(x) \oplus \widetilde{f_3}(x) = 1$. Множество

[1]Исследование выполнено при финансовой поддержке РФФИ (проекты №18-07-01394, 18-31-00374).

бент-функций от $2k$ переменных, построенных с помощью данной конструкции, обозначается $\mathcal{BI}_{2k}$. Для множества самодуальных бент-функций из $\mathcal{BI}_{2k}$ используется обозначение $\mathrm{SB}^{+}_{\mathcal{BI}}(2k)$.

Открытой проблемой является полная характеризация и описание класса самодуальных бент-функций. Этому вопросу посвящены несколько работ за рубежом (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou, T. Feulner, L. Sok, A. Wassermann и др.). В частности, в [4] перечислены все самодуальные бент-функции от $2, 4, 6$ переменных и все квадратичные самодуальные бент-функции от 8 переменных. В [5] 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 [6]. В [7] найден спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

В данной работе найдены необходимые и достаточные условия самодуальности функций из класса $\mathcal{BI}$. На основании данного результата предложена итеративная конструкция самодуальных бент-функций и получена оценка на количество самодуальных бент-функций из класса $\mathcal{BI}$. Доказано, что существуют самодуальные бент-функции всех возможных для бент-функций степеней. Найдено минимальное расстояние Хэмминга между самодуальными бент-функциями. Доказано, что множества самодуальных и антисамодуальных бент-функций являются метрически регулярными.

Теорема 1. Пусть $f \in \mathcal{BI}_{n+2}$. Тогда f является самодуальной бент-функций в том и только в том случае, когда существует такая пара функций $g_1, g_2 \in \mathcal{B}_n$ и булева функция h от n переменных, что

$$
\begin{aligned}
f(00, x) &= (g_1 \oplus g_2)\, h(x) \oplus g_1(x) = \widetilde{g}_2(x),\\
f(01, x) &= (g_1 \oplus g_2)\, h(x) \oplus g_2(x) = \widetilde{g_1 \oplus h}(x),\\
f(10, x) &= (g_1 \oplus g_2)\, h(x) \oplus g_2(x) \oplus h(x) = \widetilde{g}_1(x),\\
f(11, x) &= (g_1 \oplus g_2)\, h(x) \oplus g_1(x) \oplus h(x) \oplus 1 = \widetilde{g_2 \oplus h}(x) \oplus 1.
\end{aligned}
$$

Можно показать, что функция h однозначно определяется парой функций g_1, g_2.

Следствие 1. Бент-функции

$$
\begin{gathered}
f_1(y_1, y_2, x) = (y_1 \oplus y_2)\left(f(x) \oplus \widetilde{f}(x)\right) \oplus f(x) \oplus y_1 y_2,\\
f_2(y_1, y_2, x) = (y_1 \oplus y_2)\,(\varphi(x) \oplus \omega(x)) \oplus \varphi(x) \oplus y_i \oplus y_1 y_2,\\
y_1, y_2 \in \mathbb{F}_2,\ x \in \mathbb{F}_2^n, = 1, 2,
\end{gathered}
$$

где $f \in \mathcal{B}_n$, $\varphi \in \mathrm{SB}^{+}(n)$, $\omega \in \mathrm{SB}^{-}(n)$, являются самодуальными бент-функциями от $n + 2$ переменных.

Заметим, что первая конструкция уже фигурировала в работе [4], но была получена другим способом — с помощью *непрямой суммы* бент-функций.

Следствие 2. Справедлива следующая оценка на количество итеративных самодуальных бент-функций:

$$
|\mathcal{B}_{n-2}| + \left|\mathrm{SB}^{+}(n-2)\right|^2 \leqslant \left|\mathrm{SB}^{+}_{\mathcal{BI}}(n)\right| \leqslant |\mathcal{B}_{n-2}|^2.
$$

Множество $\mathrm{SB}^{+}(2)$ содержит только две функции: $x_1 x_2$ и $x_1 x_2 \oplus 1$. В утверждениях $1, 2, 3$ предполагается, что $n \geqslant 4$.

Утверждение 1. Для каждого $d \in \{2, 3, \ldots, n/2\}$ существует самодуальная бент-функция от n переменных степени d.

Утверждение 2. Для любых различных $u, v \in \mathbb{F}_2^n$ найдётся пара самодуальных бент-функций $f, g \in \mathrm{SB}^+(n)$, такая, что $f(u) \oplus f(v) \oplus g(u) \oplus g(v) = 1$.

Известно [8], что минимальное расстояние Хэмминга между бент-функциями равно $2^{n/2}$. Данное расстояние достижимо на множестве самодуальных бент-функций.

Утверждение 3. Справедливо

$$\min_{f,g \in SB^+(n), f \neq g} \mathrm{dist}(f, g) = 2^{n/2}.$$

Пусть $A \subseteq \mathbb{F}_2^n$ — произвольное множество, $y \in \mathbb{F}_2^n$ — произвольный двоичный вектор. Расстояние от вектора y до множества A определяется как $\mathrm{dist}(y, A) = \min\limits_{x \in A} \mathrm{dist}(y, x)$. *Радиусом покрытия* множества A называется $d(A) = \max\limits_{y \in \mathbb{F}_2^n} \mathrm{dist}(y, A)$.

Множество двоичных векторов, находящихся на расстоянии $d(A)$ от множества $A \subseteq \mathbb{F}_2^n$, называется *метрическим дополнением* [9] множества A и обозначается $\widehat{A}$. Если $\widehat{\widehat{A}} = A$, то множество A называется *метрически регулярным*.

Следующая теорема описывает метрическое дополнение множества самодуальных бент-функций.

Теорема 2. Пусть $n \geqslant 4$. Тогда

— метрическим дополнением множества самодуальных бент-функций от n переменных является множество антисамодуальных бент-функций от n переменных;
— метрическим дополнением множества антисамодуальных бент-функций от n переменных является множество самодуальных бент-функций от n переменных.

Следствие 3. Множества самодуальных и антисамодуальных бент-функций являются метрически регулярными.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Canteaut A. and Charpin P.* Decomposing bent functions // IEEE Trans. Inf. Theory. 2003. V. 49. No. 8. P. 2004–2019.
3. *Tokareva N. N* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Commun. 2011. No. 4. P. 609–621.
4. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
5. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. P. 183—198.
6. *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. P. 395–406.
7. *Куценко А. В.* Спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана —МакФарланда // Дискретный анализ и исследование операций. 2018. Т. 25. № 1. С. 98–119.
8. *Коломеец Н. А., Павлов А. В.* Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4(6). С. 5–20.
9. *Облаухов А. К.* О метрическом дополнении подпространств булева куба // Дискретный анализ и исследование операций. 2016. Т. 23. № 3. С. 93–106.