ЛИТЕРАТУРА

1. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
2. *Tokareva N.* Algebraic Normal Form of a Bent Function: Properties and Restrictions. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/1160.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
4. *Langevin P.* Classification of Boolean Quartics Forms in Eight Variables. http://langevin.univ-tln.fr/project/quartics/quartics.html.

УДК 519.7 DOI 10.17223/2226308X/12/16

ИЗОМЕТРИЧНЫЕ ОТОБРАЖЕНИЯ МНОЖЕСТВА ВСЕХ БУЛЕВЫХ ФУНКЦИЙ В СЕБЯ, СОХРАНЯЮЩИЕ САМОДУАЛЬНОСТЬ И ОТНОШЕНИЕ РЭЛЕЯ[1]

А. В. Куценко

Изучаются изометричные отображения множества всех булевых функций от n переменных в себя. Получено полное описание изометричных отображений, сохраняющих самодуальность функций. Доказано, что каждое такое отображение сохраняет также антисамодуальность. Найдены все изометричные отображения, определяющие взаимно-однозначные соответствия между множествами самодуальных и антисамодуальных бент-функций. Получены все изометричные отображения, сохраняющие отношение Рэлея каждой булевой функции. Следствием данных результатов является полное описание всех изометричных отображений, сохраняющих максимальную нелинейность и расстояние Хэмминга между каждой бент-функцией и дуальной к ней.

Ключевые слова: *булева функция, изометричное отображение, самодуальная бент-функция, отношение Рэлея.*

Булевой функцией от n переменных 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 $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Весом Хэмминга* $\mathrm{wt}(x)$ вектора $x \in \mathbb{F}_2^n$ называется количество единиц в нём. *Расстояние Хэмминга* $\mathrm{dist}(f, g)$ между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения. Через $\mathcal{O}_n$ обознается ортогональная группа $\mathcal{O}_n = \left\{L \in GL(n, 2) : LL^T = I_n\right\}$, где L^T — операция транспонирования L; I_n — единичная матрица порядка n над полем $\mathbb{F}_2$ [1]. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y\rangle}$, $y \in \mathbb{F}_2^n$.

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

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

(*антисамодуальной*), если $f = \tilde{f}$ (соответственно $f = \widetilde{f} \oplus 1$). Множества самодуальных и антисамодуальных бент-функций от n переменных обозначаются через $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ соответственно [3].

Открытой проблемой является полная характеризация и описание класса самодуальных бент-функций. Этому и другим вопросам, связанным с самодуальными бент-функциями, посвящён ряд работ (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou, T. Feulner, L. Sok, A. Wassermann и др.). В частности, в работе [4] 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 [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 [5]. В [6] найден полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда.

Согласно [4, 7], *отношением Рэлея* (the Rayleigh quotient) S_f булевой функции f от n переменных называется число

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

Из соотношения

$$\mathrm{dist}\left(f, \widetilde{f}\right) = 2^{n-1} - \frac{1}{2^{n/2+1}} S_f$$

следует, что отношение Рэлея полностью характеризует расстояние Хэмминга между бент-функцией $f \in \mathcal{B}_n$ и дуальной к ней функцией $\widetilde{f} \in \mathcal{B}_n$. Известно [4], что абсолютное значение S_f не превосходит $2^{3n/2}$, при этом данная оценка достигается только на самодуальных бент-функциях $\left(+2^{3n/2}\right)$ и антисамодуальных бент-функциях $\left(-2^{3n/2}\right)$.

Отображение всех булевых функций от n переменных в себя называется *изометричным*, если оно сохраняет расстояние Хэмминга для каждой пары функций. Известно, что каждое такое отображение однозначно представляется в виде

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

где π — перестановка на множестве $\mathbb{F}_2^n$; g — булева функция от n переменных [8]. Единственным изометричным отображением множества всех булевых функций от n переменных в себя, оставляющим множество $\mathcal{B}_n$ на месте, является композиция аффинного преобразования координат и прибавления аффинной функции от n переменных [9].

Всюду далее предполагается, что n — чётное натуральное число.

В работе [5] (см. также [4]) доказано, что отображение всех булевых функций от n переменных в себя, имеющее вид

$$f(x) \longrightarrow f\left(L\left(x \oplus c\right)\right) \oplus \langle c, x \rangle \oplus d,$$

где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$, сохраняет самодуальность бент-функции. Нетрудно видеть, что все отображения данного вида являются изометричными.

В [7] приведены примеры отображений всех булевых функций от n переменных в себя, сохраняющих максимальную нелинейность и отношение Рэлея. Показано, что для каждой бент-функции $f \in \mathcal{B}_n$ и любых $L \in \mathcal{O}_n, c \in \mathbb{F}_2^n, d \in \mathbb{F}_2$ для бент-функций

$g, h \in \mathcal{B}_n$, определённых как $g(x) = f(Lx) \oplus d$ и $h(x) = f(x \oplus c) \oplus \langle c, x \rangle$, справедливо $S_g = S_f$ и $S_h = (-1)^{\langle c,c \rangle} S_f$.

В [3] отмечено, что отображение всех булевых функций от n переменных в себя, имеющее вид

$$f(x) \longrightarrow f(x \oplus c) \oplus \langle c, x \rangle,$$

где $c \in \mathbb{F}_2^n$, $\mathrm{wt}(c)$ — нечётное число, определяет биекцию между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$. Очевидно, что такое отображение сохраняет расстояние Хэмминга. Частный случай отображения данного вида — при $c = (1, 0, 0, \ldots, 0) \in \mathbb{F}_2^n$ — ранее был рассмотрен в работе [4], на основании чего был сделан вывод о том, что между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$ существует взаимно-однозначное соответствие.

В настоящей работе получено обобщение известных результатов в рамках класса изометричных отображений.

Пусть φ — изометричное отображение всех булевых функций от n переменных в себя, то есть

$$f(x) \longrightarrow f(\pi(x)) \oplus g(x),$$

где π — перестановка на множестве $\mathbb{F}_2^n$; g — булева функция от n переменных.

Теорема 1. Следующие условия эквивалентны:

- φ сохраняет самодуальность;
- φ сохраняет антисамодуальность;
- φ сохраняет отношение Рэлея каждой булевой функции от n переменных;
- $\pi(x) = L(x \oplus c)$ и $g(x) = \langle c, x \rangle \oplus d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

Следствие 1. Отображение φ сохраняет максимальную нелинейность и расстояние Хэмминга между каждой бент-функцией и дуальной к ней тогда и только тогда, когда $\pi(x) = L(x \oplus c)$ и $g(x) = \langle c, x \rangle \oplus d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — чётное число; $d \in \mathbb{F}_2$.

Теорема 2. Следующие условия эквивалентны:

- φ определяет взаимно-однозначное соответствие между множествами $\mathrm{SB}^+(n)$ и $\mathrm{SB}^-(n)$;
- φ меняет знак отношения Рэлея каждой булевой функции от n переменных;
- $\pi(x) = L(x \oplus c)$ и $g(x) = \langle c, x \rangle \oplus d$, где $L \in \mathcal{O}_n$; $c \in \mathbb{F}_2^n$; $\mathrm{wt}(c)$ — нечётное число; $d \in \mathbb{F}_2$.

Из полученных результатов следует, что более общего подхода к эквивалентности самодуальных бент-функций на основе изометричных отображений, чем предложенный в работах [4, 5], не существует.

ЛИТЕРАТУРА

1. *Janusz G. J.* Parametrization of self-dual codes by orthogonal matrices // Finite Fields Appl. 2007. No. 13 (3). P. 450–491.
2. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. No. 20 (3). P. 300–305).
3. *Hou X.-D.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. No. 63 (2). P. 183–198.
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. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. No. 68 (1). P. 395–406.

6. *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.
7. *Danielsen L. E., Parker M. G., and Solé P.* The Rayleigh quotient of bent functions // LNCS. 2009. V. 5921. P. 418–432.
8. *Марков А. А.* О преобразованиях, не распространяющих искажения // Избранные труды. Т. II. Теория алгорифмов и конструктивная математика, математическая логика, информатика и смежные вопросы. М.: МЦНМО, 2003. С. 70–93.
9. *Tokareva N. N.* The group of automorphisms of the set of bent functions // Discr. Math. Appl. 2010. No. 20 (5). P. 655–664.

УДК 519.7 DOI 10.17223/2226308X/12/17

О КЛАССАХ БУЛЕВЫХ ФУНКЦИЙ ОГРАНИЧЕННОЙ СЛОЖНОСТИ[1]

А. И. Метальникова, И. А. Панкратова

Рассматриваются классы булевых функций от n переменных, имеющих короткое (по сравнению с 2^n) представление. Подсчитаны мощности этих классов, приведены тесты на принадлежность функции классам и алгоритм доопределения частично заданной булевой функции до функции ограниченной степени.

Ключевые слова: *существенная зависимость функции от переменной, степень булевой функции, алгебраическая нормальная форма.*

Во многих шифрсистемах используются булевы функции. Если функция является ключом, как, например, в [1, 2], то она должна зависеть от большого числа переменных. Поскольку длина вектора значений булевой функции от n переменных равна 2^n и формула (в любом базисе) произвольной функции имеет ту же длину (порядка 2^n), представляют интерес классы функций, которые зависят от большого числа переменных, но имеют короткое задание. В связи с этим возникают следующие задачи: подсчёт количества функций в классе; разработка теста на принадлежность функции классу; разработка алгоритма доопределения частичной функции до функции из заданного класса.

Обозначим $P_2(n)$ множество всех булевых функций от n переменных; будем рассматривать следующие классы функций в $P_2(n)$ и называть их классами ограниченной сложности:

— $C_{n,k}$ — с заданным (равным k) числом существенных переменных;
— $C_{n,\leqslant k}$ — с ограниченным (не больше k) числом существенных переменных;
— $D_{n,k}$ — заданной степени ($\deg f = k$);
— $D_{n,\leqslant k}$ — ограниченной степени ($\deg f \leqslant k$);
— $L_{n,k}$ — с заданной (равной k) длиной алгебраической нормальной формы (АНФ);
— $L_{n,\leqslant k}$ — с ограниченной (не больше k) длиной АНФ;
— NR_n — имеющие бесповторную АНФ (каждая переменная входит в АНФ не более одного раза).

В таблице приведены мощности этих классов, здесь $\mathbb{S}_k$ — количество функций от k переменных, существенно зависящих от всех своих переменных (последовательность A000371 из [3]), $\mathbb{S}_k = \sum\limits_{i=0}^{k}(-1)^i\binom{k}{i}2^{2^{k-i}}$; $\mathbb{B}_k$ — число Белла, или количество всех

[1]Работа поддержана грантом РФФИ, проект № 17-01-00354.