Секция 2

ДИСКРЕТНЫЕ ФУНКЦИИ

УДК 519.7 DOI 10.17223/2226308X/13/4

О ПРОДОЛЖЕНИИ ДО БЕНТ-ФУНКЦИЙ И ОЦЕНКЕ СВЕРХУ ИХ ЧИСЛА

С. В. Агиевич

Булева бент-функция f от n переменных является продолжением булевой функции g от $k < n$ переменных, если g является сужением f на фиксированную аффинную плоскость размерности k. Доказывается, что продолжение всегда существует, если $k \leqslant n/2$. Получена оценка сверху для числа продолжений. Оценка усиливается для случая $k = n - 1$, когда g является почти-бент-функцией. В результате мы улучшаем известные оценки сверху для числа бент-функций.

Ключевые слова: *бент-функция, число бент-функций, почти-бент-функция, аффинная плоскость.*

Булева функция $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ от чётного числа переменных n называется *бент-функцией*, если $|\hat{f}(\mathbf{u})| = 2^{n/2}$ для всех $\mathbf{u} \in \mathbb{F}_2^n$. Здесь $\hat{f}$ — спектр Уолша — Адамара функции f:

$$\hat{f}(\mathbf{u}) = \sum_{x \in \mathbb{F}_2^n} \chi(f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}).$$

Символ χ под знаком суммы — это нетривиальный аддитивный характер $\mathbb{F}_2$: $\chi(a) = (-1)^a$, точка обозначает скалярное произведение векторов.

Пусть $\mathcal{B}_n$ — множество всех бент-функций от n переменных. Точное значение $|\mathcal{B}_n|$ неизвестно уже для $n = 10$, более того, адекватное оценивание $|\mathcal{B}_n|$ как сверху, так и снизу остаётся трудной задачей (см. обсуждение в [1]). В настоящей работе нас интересуют оценки сверху.

Обозначим $B(d, n) = 2^{\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{d}}$ и напомним, что булева функция f однозначно представляется многочленом фактор-кольца $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$. Пусть $\deg f$ — степень многочлена.

Наивная оценка сверху (так она названа в работе [2]) для $|\mathcal{B}_n|$ основана на том, что если $f \in \mathcal{B}_n$ и $n \geqslant 4$, то $\deg f \leqslant n/2$. Оценка имеет следующий вид:

$$|\mathcal{B}_n| \leqslant B(n/2, n) = 2^{2^{n-1}+\binom{n}{n/2}/2} \approx 2^{2^{n-1}+2^n/\sqrt{2\pi n}}.$$

Оценка может быть немного усилена: следует учесть условие $2 \leqslant \deg f$ и вычесть из правой части 2^{n+1} — число аффинных функций.

В [2] К. Карле и А. Клаппер нашли более серьёзное усиление:

$$|\mathcal{B}_n| \leqslant \frac{B(n/2, n)}{2^{2^{n/2}-n/2-1}}(1 + \varepsilon_n) + B(n/2 - 1, n), \quad \varepsilon_n = \frac{1}{2^{\binom{n-1}{n/2-1}-2}},$$

справедливое для $n \geqslant 6$. Эта оценка считается лучшей на сегодняшний день. В [2], кроме ограничения на $\deg f$, учитывается также спектральное строение бент-функций. Мы улучшаем оценку Карле — Клаппера.

Теорема 1. При чётном $n \geqslant 6$ справедлива оценка

$$|\mathcal{B}_n| \leqslant c_n\, 2^{2^{n-2}-n/2+5/2} \left(\frac{B(n/2, n-1) - B(n/2-1, n-1)}{2^{2^{n/2}-n/2-1}} + B(n/2-1, n-1) \right),$$

в которой $c_n = \exp(-1/2 + 23/(18 \cdot 2^{n-2}))/\sqrt{\pi}$, причём $c_n \leqslant c_6 \approx 0{,}3706$.

Различные оценки сверху для $|\mathcal{B}_n|$ при малых n сведены в табл. 1. Точные значения $|\mathcal{B}_6| = 5425430528$ и $|\mathcal{B}_8| = 99270589265934370305785861242880$ найдены в работах [3] и [4] соответственно.

Таблица 1

n	$\lvert\mathcal{B}_n\rvert$	Оценки сверху для $\lvert\mathcal{B}_n\rvert$		
		Наивная	[2]	Настоящая работа
2	8			
4	896	2032		
6	$\approx 2^{32,3}$	2^{42}	2^{38}	2^{36}
8	$\approx 2^{106,3}$	2^{163}	2^{152}	2^{149}
10	?	2^{638}	2^{612}	2^{608}
12	?	2^{2510}	2^{2453}	2^{2448}

Метод оценивания основан на подсчёте числа продолжений булевой функции g от $k < n$ переменных до бент-функций от n переменных. Функция $f \in \mathcal{B}_n$ является *продолжением* g, если

$$g(y_1, \ldots, y_k) = f(\underbrace{0, \ldots, 0}_{n-k}, y_1, \ldots, y_k).$$

Другими словами, f — продолжение g, если g является сужением f на аффинную плоскость $E = \{(0, \ldots, 0, y_1, \ldots, y_k)\}$. Выбор E здесь не имеет принципиального значения, можно зафиксировать любую другую плоскость размерности k.

Пусть $\mathcal{B}_n(g)$ — множество всех функций $f \in \mathcal{B}_n$, которые являются продолжениями g. При доказательстве теоремы 1 мы рассматривали функции g от $n-1$ переменных, для которых $\mathcal{B}_n(g) \neq \varnothing$. Если g является подходящей, то значения $\hat{g}$ принадлежат множеству $\{0, \pm 2^{n/2}\}$ (и тогда g называется *почти-бент-функцией*) и, кроме этого, выполняется условие $\deg g \leqslant n/2$. Для оценки числа подходящих функций g мы применили результаты работы [2].

Для оценки $|\mathcal{B}_n(g)|$ использована следующая лемма, доказанная с помощью техники работы [5].

Лемма 1. Пусть N — чётное, S_N — сумма N независимых случайных величин с равномерным распределением на $\{-1, 1\}$. Для $s = 0, \pm 2, \ldots, \pm N$ справедлива следующая оценка:

$$\mathsf{P}[S_N = s] = \binom{N}{(N+s)/2} 2^{-N} \leqslant \sqrt{\frac{2}{\pi N}} \exp\left(-\frac{s^2}{2N} + \frac{23}{18N} \right).$$

Лемма 1 имеет и самостоятельное значение. С её помощью можно оценивать (сверху) биномиальные коэффициенты, контролировать точность аппроксимации в локальной теореме Муавра — Лапласа. В нашем контексте лемма позволяет оценить вероятность того, что спектральный коэффициент случайной булевой функции принимает заданное значение.

Оценку леммы 1 можно несколько улучшить, это улучшение потребуется в теореме 2. Речь идёт об оценке вида

$$\mathsf{P}[S_N = s] \leqslant 2^{-\alpha_N s^2 - \beta_N},$$

где α_N и β_N настраиваются так, чтобы величина $\gamma_N = \alpha_N + \beta_N/N$ была максимальной.

При малых N оптимальные тройки $(\alpha_N, \beta_N, \gamma_N)$ можно определить, решая задачи линейного программирования. Решения представлены в табл. 2.

Таблица 2

N	α_N	β_N	γ_N
2	1/2	1	3/4
4	1/6	4/3	1/2
8	1/12	$14/3 - \log_2 7$	$2/3 - \frac{1}{8}\log_2 7 \approx 0{,}3157$

В общем случае из леммы 1 следует, что

$$\gamma_N \geqslant \frac{\log_2 e + \log_2 \pi + \log_2 N - 1}{2N} - \frac{23 \log_2 e}{18N^2}.$$

С точки зрения теории бент-прямоугольников [6] величина $|\mathcal{B}_n(g)|$ — это число прямоугольников размерности $(n-k) \times k$, у которых первая строка фиксирована — она заполнена значениями $\hat{g}$. Учитывая ограничения на строки и столбцы бент-прямоугольника (точнее, тождества Парсеваля для них), получаем следующий результат.

Теорема 2. Для булевой функции g от $k < n$ переменных справедлива оценка

$$\log_2 |\mathcal{B}_n(g)| \leqslant 2^n (1 - \gamma_{2^{n-k}}).$$

Отметим, что оценка теоремы 2 с $k = n-1$ несколько усиливается при доказательстве теоремы 1.

Начиная с $k = n/2 + 1$, появляются функции g, которые нельзя продолжить до бент-функций. В этом можно убедиться, анализируя ограничения на столбцы бент-прямоугольника. Впрочем, оказывается, что

Теорема 3. При чётном n любая булева функция от $k \leqslant n/2$ переменных может быть продолжена до бент-функции от n переменных.

Теорему достаточно доказать для $k = n/2$. В этом случае с помощью биаффинной конструкции, предложенной в [7], можно построить бент-квадрат размерности $k \times k$, все строки и столбцы которого являются аффинными перестановками значений $\hat{g}$. Легко добиться, чтобы первая строка квадрата в точности совпадала с $\hat{g}$.

ЛИТЕРАТУРА

1. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. London, UK; San Diego, CA, USA: Academic Press, 2015.
2. *Carlet C. and Klapper A.* Upper bounds on the numbers of resilient functions and of bent functions // Proc. 23rd Symp. Inform. Theory. Louvain-La-Neuve, Belgium. 2002. P. 307–314.
3. *Preneel B., Van Leekwijck W., Van Linden L., et al.* Propagation characteristics of Boolean functions // EUROCRYPT'90. LNCS. 1991. V. 473. P. 161–173.
4. *Langevin P. and Leander G.* Counting all bent functions in dimension eight 99270589265934370305785861242880 // Des. Codes Cryptogr. 2011. V. 59. P. 193–205.

5. *Szabados T.* A Simple Wide Range Approximation of Symmetric Binomial Distributions. Preprint arXiv:1612.01112 [math.PR]. 2016.
6. *Agievich S.* On the representation of bent functions by bent rectangles // Probabilistic Methods in Discrete Mathematics: Fifth Intern. Conf. (Petrozavodsk, Russia, June 1–6, 2000). Utrecht, Boston: VSP, 2002. P. 121–135.
7. *Agievich S.* Bent rectangles // Proc. NATO Advanced Study Institute on Boolean Functions in Cryptology and Information Security (Moscow, September 8–18, 2007). Amsterdam: IOS Press, 2008. P. 3–22.

УДК 519.7 DOI 10.17223/2226308X/13/5

О МЕТРИЧЕСКИХ СВОЙСТВАХ МНОЖЕСТВА САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Приводится обзор известных метрических свойств множества самодуальных бент-функций. Бент-функция называется самодуальной, если она совпадает со своей дуальной бент-функцией, и анти-самодуальной, если совпадает с отрицанием своей дуальной. Приводится полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда. Даются результаты, касающиеся характеризации булевых функций, находящихся на максимально возможном удалении от множества самодуальных бент-функций. Описаны группы автоморфизмов множеств самодуальных и анти-самодуальных бент-функций от n переменных, автоморфизмы множества булевых функций от n переменных, которые меняют местами множества самодуальных и анти-самодуальных бент-функций, изометричные отображения, сохраняющие неизменным отношение Рэлея каждой булевой функции от n переменных. Даётся характеризация всех изометричных отображений, сохраняющих максимальную нелинейность и расстояние Хэмминга между каждой бент-функций и дуальной к ней.

Ключевые слова: *булева функция, самодуальная бент-функция, расстояние Хэмминга, изометричное отображение, метрическая регулярность, группа автоморфизмов, 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 $\mathcal{F}_n$. Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначим скалярное произведение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Весом Хэмминга* $\mathrm{wt}(x)$ вектора $x \in \mathbb{F}_2^n$ называется число его ненулевых координат. *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается $\mathrm{dist}(f, g)$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством

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

[1]Работа выполнена в рамках государственного задания ИМ СО РАН (проект №0314-2019-0017) при поддержке РФФИ (проекты № 18-07-01394, 20-31-70043) и Лаборатории криптографии JetBrains Research.