2014 Теоретические основы прикладной дискретной математики № 4(26)

DOI 10.17223/20710410/26/6

УДК 519.7

О РАЗЛОЖЕНИИ ДУАЛЬНОЙ БЕНТ-ФУНКЦИИ В СУММУ ДВУХ БЕНТ-ФУНКЦИЙ[1]

Н. Н. Токарева

Институт математики им. С. Л. Соболева, г. Новосибирск, Россия

E-mail: tokareva@math.nsc.ru

Установлено, что бент-функции и функции, дуальные к ним, разложимы или не разложимы в сумму двух бент-функций одновременно.

Ключевые слова: *бент-функция, дуальная функция.*

Введение

Бент-функции — булевы функции с экстремальными нелинейными свойствами — интенсивно исследуются в связи с многими приложениями в криптографии, теории кодирования, дискретной математике [1]. Одним из нерешённых вопросов этой области остаётся вопрос об оценках числа таких функций.

В работе [2] предложен новый подход к этой проблеме и выдвинута гипотеза: *произвольная булева функция от n переменных степени $\leqslant n/2$ может быть представлена в виде суммы двух бент-функций от n переменных* (n *чётно,* $n \geqslant 2$). При малых $n = 2, 4, 6$ гипотеза проверена в [2], при $n = 8$ доказано [3], что каждая функция степени не выше трёх представима в виде суммы не более четырех бент-функций. Для произвольного n доказан [4] ослабленный вариант гипотезы. Авторы [5] доказали, что в виде суммы двух бент-функций может быть представлена любая квадратичная булева функция, любая бент-функция Мак-Фарланда, произвольная функция частичного расщепления. В работе [6] отмечается связь гипотезы с открытыми вопросами о метрических свойствах класса бент-функций.

В данной работе продолжено исследование разложимости произвольной булевой функции от чётного числа переменных в сумму двух бент-функций. Доказано, что бент-функции и функции, дуальные к ним, разложимы или не разложимы в сумму двух бент-функций одновременно.

1. Основные определения

Пусть $x = (x_1, \ldots, x_n)$ — двоичный вектор. Вектор x *предшествует* вектору y, если для всех $i = 1, \ldots, n$ выполняется $x_i \leqslant y_i$. Будем обозначать предшествование так: $x \preccurlyeq y$. Через $\mathrm{wt}(x)$ обозначим *вес* вектора x, т. е. число его ненулевых координат.

Напомним, что произвольная булева функция f от n переменных однозначно представляется с помощью *алгебраической нормальной формы* (АНФ):

$$f(x) = \sum_y f_y\, x_1^{y_1} \cdot \ldots \cdot x_n^{y_n}, \text{ где } f_y = \sum_{z \preccurlyeq y} f(z). \tag{1}$$

Здесь и далее под знаком суммы мы опускаем области значений векторов y, z, предполагая, что каждый вектор принимает все значения из множества $\mathbb{Z}_2^n$, возможно, с некоторыми ограничениями, как во втором случае: все такие z, что $z \preccurlyeq y$.

[1]Работа выполнена при финансовой поддержке РФФИ № 14-01-00507.

Степенью булевой функции называется число множителей в самом длинном слагаемом, присутствующем в её АНФ.

Преобразованием Уолша — Адамара булевой функции f от n переменных называется целочисленная функция W_f, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(y) = \sum_x (-1)^{\langle x,y\rangle \oplus f(x)},$$

где $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$.

Булева функция f от чётного числа переменных n называется *бент-функцией*, если $W_f(x) = \pm 2^{n/2}$ для любого вектора x. *Дуальной функцией* к бент-функции f называется булева функция $\widetilde{f}$ от n переменных, определяющая знаки коэффициентов Уолша — Адамара функции f, т. е. $\widetilde{f}$ для каждого x определяется равенством

$$W_f(x) = (-1)^{\widetilde{f}(x)}\, 2^{n/2}.$$

Несложно показать, что дуальная функция — всегда бент-функция, более того, $\widetilde{\widetilde{f}} = f$.

Согласно [1], выполняется

Утверждение 1. Степень бент-функции от $n \geqslant 4$ переменных не превышает $n/2$.

Известен следующий факт [7, лемма 5.17]:

Утверждение 2. Пусть f — бент-функция от n переменных, $n \geqslant 4$. Тогда

$$\sum_{x \preccurlyeq y} f(x) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} + 2^{\mathrm{wt}(y)-n/2} \sum_{x \preccurlyeq y \oplus 1} \widetilde{f}(x).$$

Бент-функции и функции, дуальные к ним, нередко исследуются вместе. Так, в работе [8] получен ряд результатов, направленных на характеризацию *самодуальных* бент-функций, т. е. таких, что $\widetilde{f} = f$. За исключением самодуальных функций, весь класс бент-функций разбивается на пары функций, связанных отношением дуальности. Интересно, что бент-функции из одной такой пары не обязательно имеют похожие свойства. Например, дуальные функции к бент-функциям Касами не являются мономиальными [9], а возможно (но пока это не доказано), и не эквивалентны им. Поэтому, если удаётся исследовать какое-либо свойство одновременно для бент-функций и функций, дуальных к ним, то «пространство исследования» сокращается в 2 раза (за исключением самодуальных функций). Далее покажем, что таким свойством как раз является разложимость функции в сумму двух бент-функций.

2. Разложение дуальных бент-функций

Теорема 1. Бент-функция от n переменных, $n \geqslant 4$, разложима в сумму двух бент-функций от n переменных тогда и только тогда, когда таким свойством обладает дуальная к ней бент-функция.

Доказательство. Пусть g — бент-функция от n переменных, такая, что $g = f \oplus h$, где f, h — бент-функции. Тогда для каждого ненулевого коэффициента g_y АНФ функции g справедливо представление $g_y = f_y \oplus h_y$, где y — произвольный вектор. Можем рассматривать лишь векторы веса не больше $n/2$, т. е. $\mathrm{wt}(y) \leqslant n/2$, поскольку в соответствии с утверждением 1 все коэффициенты g_y, f_y, h_y равны нулю, если $\mathrm{wt}(y) > n/2$. Согласно представлению (1), имеем

$$g_y = \sum_{x \preccurlyeq y} g(x) = \left(\sum_{x \preccurlyeq y} f(x)\right) \oplus \left(\sum_{x \preccurlyeq y} h(x)\right).$$

Используя равенство $a \oplus b = a + b - 2ab$, можем перейти в правой части к знакам обычного сложения и вычитания. По утверждению 2 выполняется равенство

$$\sum_{x \preccurlyeq y} g(x) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} + 2^{\mathrm{wt}(y)-n/2} \sum_{x \preccurlyeq y \oplus 1} \widetilde{g}(x).$$

Используя его и аналогичные равенства для функций f, h, получаем

$$2^{\mathrm{wt}(y)-n/2} \left(\sum_{x \preccurlyeq y} \widetilde{g}(x) - \sum_{x \preccurlyeq y} \widetilde{f}(x) - \sum_{x \preccurlyeq y} \widetilde{h}(x) \right) = 2^{\mathrm{wt}(y)-1} - 2^{n/2-1} - 2 f_y h_y.$$

Домножим равенство на $2^{n/2-\mathrm{wt}(y)}$. Тогда

$$\sum_{x \preccurlyeq y} \widetilde{g}(x) - \sum_{x \preccurlyeq y} \widetilde{f}(x) - \sum_{x \preccurlyeq y} \widetilde{h}(x) = 2^{n/2-1} - 2^{n-\mathrm{wt}(y)-1} - 2^{n/2-\mathrm{wt}(y)+1} f_y h_y.$$

Заметим, что выражение в правой части чётное, поскольку $\mathrm{wt}(y) \leqslant n/2$ и $n \geqslant 4$. Поэтому, рассматривая равенство по модулю два, получаем

$$\sum_{x \preccurlyeq y} \widetilde{g}(x) = \sum_{x \preccurlyeq y} \widetilde{f}(x) \oplus \sum_{x \preccurlyeq y} \widetilde{h}(x),$$

т. е. $\widetilde{g}_y = \widetilde{f}_y \oplus \widetilde{h}_y$ для произвольного вектора y веса $\leqslant n/2$. Напомним, что для векторов большего веса это равенство автоматически выполняется. Таким образом, $\widetilde{g} = \widetilde{f} \oplus \widetilde{h}$. Очевидно, что в обратную сторону теорема доказывается аналогично. ■

Следствие 1. Пусть g, f, h — бент-функции от n переменных, $n \geqslant 4$. Тогда если $g \oplus f \oplus h = 0$, то справедливо $\widetilde{g} \oplus \widetilde{f} \oplus \widetilde{h} = 0$.

Следствие 1 говорит о том, что, зная разложение бент-функции в сумму двух других, можно простым способом перейти к разложению дуальной бент-функции.

Следствие 2. Число различных разложений бент-функции g в сумму двух бент-функций равно числу аналогичных разложений дуальной бент-функции $\widetilde{g}$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N. N.* On the number of bent functions from iterative constructions: lower bounds and hypotheses // Adv. Math. Comm. 2011. V. 5. No. 4. P. 609–621.
3. *Tokareva N. N.* Every cubic Boolean function in 8 variables is the sum of not more than 4 bent functions // Прикладная дискретная математика. Приложение. 2014. № 7. С. 38–39.
4. *Токарева Н. Н.* О разложении булевой функции в сумму бент-функций // Прикладная дискретная математика. Приложение. 2012. № 5. С. 30.
5. *Qu L. and Li C.* When a Boolean function can be expressed as the sum of two bent functions // Cryptology ePrint Archive. 2014/048.
6. *Коломеец Н. А.* Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных // Прикладная дискретная математика. 2014. № 3. С. 28–39.
7. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. San Diego: Acad. Press, 2009. 245 p.
8. *Carlet C., Danielsen L.-E., Parker M. G., and Solé P.* Self-dual bent functions // Int. J. Inform. and Coding Theory. 2010. V. 1. No. 4. P. 384–399.
9. *Langevin Ph. and Leander G.* Monomial bent functions and Stickelberger's theorem // Finite Fields and Their Applications. 2008. V. 14. No. 3. P. 727–742.