

Следствие. Пусть n, d — натуральные числа, такие, что $n > 2$, $d < 2^n - 1$, $\|d\|_2 > n/2$. Тогда для любой функции $F \in \mathcal{F}_n$ выполняется неравенство

$$\max \{ |\Delta(F, \text{tr}_1^n(\alpha x^d) + \text{tr}_1^n(\beta x))| : \alpha, \beta \in \mathbb{F}_{2^n} \} > 2^{\frac{n}{2}}.$$

З а м е ч а н и е. Зафиксируем натуральное n . В качестве примера показателя d , удовлетворяющего условию следствия, можно привести число $2^t - 1$, где $t > n/2$. Если требуется, чтобы моном x^d задавал подстановку на $\mathbb{F}_{2^n}$, то t необходимо выбрать взаимно простым с n . Таким условиям при $n > 2$ удовлетворяет t , равное $n - 1$.

Теоретический и практический интерес представляют задачи количественной оценки для натурального n , $d \in \overline{1, 2^n - 1}$ и функции $F \in \mathcal{F}_n$ величины

$$\max \{ |\Delta(F, \text{tr}_1^n(\alpha x^d) + \text{tr}_1^n(\beta x))| : \alpha, \beta \in \mathbb{F}_{2^n} \}$$

как для всех функций из $\mathcal{F}_n$, так и для отдельных классов таких функций, например бент-функций [4]. Рассмотрим способ построения бент-функций с помощью координатных функций степенных преобразований поля $\mathbb{F}_{2^n}$ и продемонстрируем эффективность аппроксимации построенных функций приближениями из рассмотренных классов.

Теорема 2. Пусть натуральные числа n и s четны, $n/2$ нечетно и $(n, s) = 2$. Положим $d = 1 + 2^s$ и выберем натуральное число σ таким, что $\sigma d \equiv 1 \pmod{2^n - 1}$. Пусть значения функции $F_{a,b} \in \mathcal{F}_n$ для любого элемента $x \in \mathbb{F}_{2^n}$ определены равенством $F_{a,b}(x) = \text{tr}_1^n(b^\sigma x) \text{tr}_1^n(ax) + \text{tr}_1^n(bx^d)$, а элементы $a, b \in \mathbb{F}_{2^n} \setminus \{0\}$ таковы, что $\text{tr}_1^n(ab^{-\sigma}) = e$. Тогда:

а) $F_{a,b}$ является бент-функцией;

б) $\max \{ |\Delta(F_{a,b}(x), \text{tr}_1^n(c_1 x^{d'}) + \text{tr}_1^n(c_2 x))| : c_1, c_2 \in \mathbb{F}_{2^n}, d' \in \overline{1, 2^n - 2} \} \geq 2^{n-1}$.

ЛИТЕРАТУРА

1. Иванов А. В. Использование приведенного представления булевых функций при построении их нелинейных аппроксимаций // Вестник Томского государственного университета. Приложение. 2007. № 23. С. 31–35.
2. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18. № 1. С. 9–29.
3. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МНЦМО, 2004. 470 с.
4. Rothaus O. S. On “bent” functions // J. Comb. Theory. 1976. Ser. A. V. 20. P. 300–305.
5. Лидл Р., Нидеррайтер Г. Конечные поля. Т. 1, 2. М.: Мир, 1988. 818 с.

УДК 519.7

СВЯЗЬ ПОДПРОСТРАНСТВ, НА КОТОРЫХ АФФИННЫ БЕНТ-ФУНКЦИЯ И ДУАЛЬНАЯ К НЕЙ¹

Н. А. Коломеец

Настоящая работа является продолжением исследований, начатых в [1]. Ранее было установлено, что минимальное расстояние Хэмминга между бент-функциями от n переменных равно $2^{n/2}$ и бент-функции находятся на этом расстоянии тогда и только тогда, когда их значения отличаются на аффинном подпространстве и обе функции

¹Работа выполнена при финансовой поддержке гранта Президента РФ для молодых российских ученых (грант МК № 1250.2009.1).

на нем аффинны. В данной работе для бент-функции и дуальной к ней устанавливается соответствие между подпространствами, на которых каждая из них аффинна.

Бент-функция — это булева функция от четного числа переменных, максимально удаленная от класса аффинных функций (функций вида $a_1x_1 \oplus a_2x_2 \oplus \dots \oplus a_nx_n \oplus a_{n+1}$). С бент-функцией f часто связывают дуальную функцию $\tilde{f}$, которая определяется из равенства

$$W_f(w) = 2^{n/2}(-1)^{\tilde{f}(w)},$$

где $W_f(w) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle w, x \rangle}$ — коэффициенты Уолша — Адамара.

(По альтернативному определению бент-функция — это такая функция, для которой все коэффициенты Уолша — Адамара по модулю равны $2^{n/2}$.)

Теорема 1. Не для всех бент-функций от n переменных, $n \geq 14$, существуют бент-функции на минимальном расстоянии $2^{n/2}$.

Эта теорема следует из результатов, полученных в [1, 2]. В работе А. Canteaut и др. рассматриваются *нормальные* и *ненормальные* бент-функции. Бент-функция от n переменных называется нормальной (слабо нормальной), если существует аффинное подпространство размерности $n/2$, на котором она постоянна (аффинна). В [2] доказывается существование не слабо нормальных бент-функций.

Пусть f — бент-функция от n переменных. Множество $L_{\text{all}}(f)$ — множество всех аффинных подпространств размерности $n/2$, на которых функция f аффинна.

Чтобы понять, есть ли в распределении функций на минимальном расстоянии регулярные свойства, рассмотрим задачу построения бент-функций на минимальном расстоянии от f с условием, что получившиеся бент-функции обязательно должны отличаться от f в заданной точке x_0 . Определим множество $L_{\text{all}}^{x_0}(f) = \{L \in L_{\text{all}}(f) \mid x_0 \in L\}$. Тогда все функции с нужным свойством будут строиться с помощью множества $L_{\text{all}}^{x_0}(f)$. Чтобы рассмотреть это множество с другой стороны, сделаем следующее.

Определим функцию $F_f : L_{\text{all}}(f) \rightarrow L_{\text{all}}(\tilde{f})$ следующим образом: если $f|_{x_0 \oplus L}(x) = \langle w_0, x \rangle \oplus c$ для некоторых векторов w_0, x_0 , константы c и подпространства L , то справедливо $F_f(x_0 \oplus L) = w_0 \oplus L^\perp$.

Лемма 1. Функция F_f задана корректно.

Теорема 2. Функция F_f взаимнооднозначна, причем $(F_f)^{-1} = F_{\tilde{f}}$.

Таким образом, мы получаем, что множество $L_{\text{all}}^{x_0}(f)$ состоит из элементов вида $x_0 \oplus L$, таких, что функция $\tilde{f}(x) \oplus \langle x_0, x \rangle$ на некотором сдвиге $L^\perp$ постоянна.

Но так как дуальная функция является бент-функцией, а бент-функции равноудалены ровно от половины аффинных функций, то встает вопрос: равны ли мощности $L_{\text{all}}^{x_0}(f)$ для различных x_0 ? Как выяснилось, в общем случае это не так, хотя и существуют функции с одинаковыми мощностями $L_{\text{all}}^{x_0}(f)$. Например, все бент-функции от шести переменных обладают такой регулярностью.

ЛИТЕРАТУРА

1. Коломеец Н. А., Павлов А. В. Свойства бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–21.
2. Canteaut A., Daum M., Dobbertin H., Leander G. Finding nonnormal bent functions // Discr. Appl. Math. 2006. V. 154. P. 202–218.
3. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.