УДК 519.7 DOI 10.17223/2226308X/10/16

КОНСТРУКЦИЯ БЕНТ-ФУНКЦИЙ ПО БЕНТ-ФУНКЦИИ, АФФИННОЙ НА НЕСКОЛЬКИХ СДВИГАХ ПОДПРОСТРАНСТВА[1]

Н. А. Коломеец

Предлагается конструкция бент-функций по имеющейся бент-функции, аффинной на нескольких смежных классах некоторого линейного подпространства размерности t. Конструкция обобщает метод построения бент-функций на минимальном возможном расстоянии от заданной бент-функции. Для $t = 2$ и для квадратичной бент-функции приведён упрощённый вид конструкции. Получена точная верхняя оценка числа порождаемых функций и доказано, что при любом $t \geqslant 2$ оценка достигается только для квадратичных бент-функций.

Ключевые слова: *булевы функции, бент-функции, минимальное расстояние, аффинность.*

Отображение вида $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от n переменных, функция $D_a f(x) = f(x) \oplus f(x \oplus a)$ — её производная по направлению $a \in \mathbb{F}_2^n$. *Носитель* функции f определяется как $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. Пусть $\langle w, x\rangle = w_1x_1 \oplus \ldots \oplus w_nx_n$, где $w, x \in \mathbb{F}_2^n$. Обозначим через Ind_S характеристическую булеву функцию множества $S \subseteq \mathbb{F}_2^n$. *Бент-функцией* называется булева функция, производные которой по всем ненулевым направлениям уравновешены (принимают значения 0 и 1 на одинаковом числе аргументов), это возможно только при чётном числе переменных. Бент-функции предложены О. Ротхаусом [1]. Они имеют приложения в алгебре, комбинаторике, теории кодирования, криптографии [2, 3]. Обозначим через $\mathcal{B}_{2k}$ множество всех бент-функций от $2k$ переменных.

В работе исследуются свойства приведённой в следующей теореме конструкции, порождающей бент-функции путём изменения некоторой имеющейся бент-функции.

Теорема 1. Пусть $f \in \mathcal{B}_{2k}$ и для некоторого $w \in \mathbb{F}_2^{2k}$ бент-функция $f(x) \oplus \langle w, x\rangle$ постоянна на каждом из 2^{2k-2t} различных смежных классов $a_1 \oplus L, \ldots, a_{2^{2k-2t}} \oplus L$ некоторого линейного подпространства $L \subseteq \mathbb{F}_2^{2k}$ размерности t, где $0 \leqslant t \leqslant k$. Тогда функция

$$f \oplus \mathrm{Ind}_{(a_1 \oplus L) \cup \ldots \cup (a_{2^{2k-2t}} \oplus L)} \tag{1}$$

также является бент-функцией.

Замечание 1. Конструкция (1) при $t = k$ становится конструкцией, предложенной К. Карле [4] и порождающей все бент-функции на расстоянии 2^k от f (это минимальное возможное расстояние Хэмминга между двумя бент-функциями) [5].

Замечание 2. В случае $t \in \{0, 1\}$ конструкция (1) тривиальна и даёт сходный результат для любой бент-функции f: при $t = 0$ можно получить только функцию $f \oplus 1$, а при $t = 1$ порождается в точности семейство функций

$$\{f(x \oplus a) \oplus c : a \in \mathbb{F}_2^{2k} \backslash \{0\}, c \in \mathbb{F}_2\}.$$

Замечание 3. Требуемый для конструкции (1) набор смежных классов размерности t всегда найдётся, если бент-функция представлена в виде линейного разветвления с индексом линейности не меньше t [6] или принадлежит классу Мэйорана — МакФарланда [7]. Заметим также, что при разных t конструкция порождает различные бент-функции.

[1]Работа поддержана грантом РФФИ, проект № 15-07-01328.

При $t = 2$ теорему 1 можно переформулировать следующим образом.

Следствие 1. Пусть $f \in \mathcal{B}_{2k}$ и для произвольных $u, v \in \mathbb{F}_2^{2k}$, $u \neq v$, и $c, d \in \mathbb{F}_2$

$$U = \operatorname{supp}(c \oplus D_u f) \cap \operatorname{supp}(d \oplus D_v f).$$

Тогда при $U \subseteq \operatorname{supp}(1 \oplus D_u D_v f)$ функция $f \oplus \operatorname{Ind}_U$ является бент-функцией.

Для квадратичной бент-функции f множество $U = (a_1 \oplus L) \cup \ldots \cup (a_{2^{2k-2t}} \oplus L)$ всегда является аффинным подпространством. Заметим, что общий подход к получению бент-функций инверсией значений исходной бент-функции на аффинном подпространстве можно найти в [4]. Опишем функции, порождаемые конструкцией (1) из квадратичной бент-функции.

Теорема 2. Пусть квадратичная бент-функция $f \in \mathcal{B}_{2k}$ постоянна на некотором смежном классе линейного подпространства $L \subseteq \mathbb{F}_2^{2k}$ с базисом $b_1, \ldots, b_t \in \mathbb{F}_2^{2k}$. Тогда для $U = \bigcap\limits_{i=1}^{t} \operatorname{supp}(D_{b_i} f \oplus c_i)$ при произвольных $c_1, \ldots, c_t \in \mathbb{F}_2$ функция $f \oplus \operatorname{Ind}_U$ является бент-функцией, а U — аффинным подпространством $\mathbb{F}_2^{2k}$ размерности $2k - t$.

В силу замечания 1 конструкция (1) является обобщением конструкции бент-функций на расстоянии 2^k от заданной бент-функции. Обобщим также некоторые результаты, касающиеся бент-функций, располагающихся на минимально возможном расстоянии друг от друга.

Теорема 3. Для произвольной $f \in \mathcal{B}_{2k}$ конструкция (1) порождает не более чем

$$2^t \prod_{i=0}^{t-1} \frac{2^{2k-2i} - 1}{2^{t-i} - 1}$$

бент-функций (для фиксированного t). При $t \geqslant 2$ оценка достигается, если и только если f является квадратичной бент-функцией.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
3. *Tokareva N. N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
4. *Carlet C.* Two new classes of bent functions // LNCS. 1994. V. 765. P. 77–101.
5. *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.
6. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Проблемы передачи информации. 1997. Т. 33. № 1. С. 75–86.
7. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.