

Теорема 1.

1) Для любой бент-функции от 4 переменных существуют базисы $(\varepsilon_0^{(1)}, \varepsilon_1^{(1)}, \varepsilon_2^{(1)}, \varepsilon_3^{(1)})$ и $(\varepsilon_0^{(2)}, \varepsilon_1^{(2)}, \varepsilon_2^{(2)}, \varepsilon_3^{(2)})$ векторного пространства $(\mathbb{F}_{2^4})_{\mathbb{F}_2}$, такие, что приведенное представление данной функции в первом базисе является, а во втором не является гипербент-функцией.

2) Для любого четного $n > 4$ существуют функции от n переменных, для каждой из которых можно найти два базиса векторного пространства $(\mathbb{F}_{2^n})_{\mathbb{F}_2}$, таких, что приведенное представление функции в первом базисе является, а во втором не является гипербент-функцией.

ЛИТЕРАТУРА

1. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишков А. Б. Приближение булевых функций мономияльными // Дискретная математика. 2006. Т. 18. № 1. С. 9–29.
2. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МНЦМО, 2004. 470 с.
3. Youssef A. M., Gong G. Hyper-bent functions // Proceedings of Advances in Cryptology, EUROCRYPT'2001. Lect. Notes in Comp. Sci. New York: Springer Verlag, 2001. V. 2045. P. 406–419.

УДК 519.7

СВОЙСТВА БЕНТ-ФУНКЦИЙ, НАХОДЯЩИХСЯ НА МИНИМАЛЬНОМ РАССТОЯНИИ ДРУГ ОТ ДРУГА

Н. А. Коломеец, А. В. Павлов, А. А. Левин

Здесь и далее пусть n — четное натуральное число. Обозначим:

- E^n — множество двоичных векторов длины n ;
- $\mathcal{F}_n$ — множество всех булевых функций от n переменных;
- нелинейность — расстояние Хэмминга до класса аффинных функций;
- бент-функции — булевы функции от четного числа переменных, обладающие максимальной нелинейностью;
- $\mathfrak{B}_n$ — множество всех бент-функций от n переменных;
- $D(f, g) = \{x \in E^n \mid f(x) \neq g(x)\}$, где $f, g \in \mathcal{F}_n$;
- f аффинна на D , если для некоторых $w_0 \in E^n, c \in E$ и для любого $x \in D$ выполняется $f(x) = w_0 \cdot x \oplus c$, где $f \in \mathcal{F}_n, D \subseteq E^n$;
- $d(A)$ — минимальное расстояние между двумя функциями в классе $A \subseteq \mathcal{F}_n$;
- U — многообразие в E^n , т. е. $U = x_0 \oplus L$, где L — подпространство в $E^n, x_0 \in E^n$.

Имеет место нижняя оценка на расстояние между бент-функциями.

Теорема 1. Справедливо $d(\mathfrak{B}_n) \geq 2^{n/2}$.

Следующая теорема дает критерий расположения функций на расстоянии $2^{n/2}$.

Теорема 2. Пусть $f, g \in \mathcal{F}_n$, f — бент-функция, $|D(f, g)| = 2^{n/2}$. Тогда g — бент-функция тогда и только тогда, когда множество $D(f, g)$ — линейное многообразие размерности $n/2$ и f на нем аффинна.

Следствие 1. Минимальное расстояние в классе бент-функций равно $2^{n/2}$.

Определим следующие множества.

- $L_{all}(f)$ — множество всевозможных подпространств в E^n размерности $n/2$, на которых f аффинна;
- $U_{all}(f)$ — множество всевозможных многообразий в E^n размерности $n/2$, на которых f аффинна.

По предыдущей теореме все бент-функции на минимальном расстоянии от заданной бент-функции описываются следующим образом.

Следствие 2. Пусть $f \in \mathfrak{B}_n$. Тогда функция $g \in \mathfrak{B}_n$ находится на минимальном расстоянии от f тогда и только тогда, когда g представляется в следующем виде:

$$g(x) = f(x) \oplus I_U(x), \text{ для некоторого } U \in U_{all}(f),$$

где $I_U(x)$ — индикатор множества U .

В связи с предложенным описанием бент-функций на минимальном расстоянии от заданной бент-функции рассмотрим индикаторы линейных многообразий:

Лемма 1. Пусть U — многообразие в E^n размерности $n/2$. Тогда индикатор U можно представить в следующем виде:

$$I_U(x) = (a_1 \cdot x \oplus c_1) \cdot \dots \cdot (a_{n/2} \cdot x \oplus c_{n/2})$$

для некоторых $a_i \in E^n$ и $c_i \in \{0, 1\}$.

Утверждение 1. Любая функция из $\mathfrak{B}_6$ имеет непустое L_{all} .

Утверждение 2. Любая функция из $\mathfrak{B}_8$ степени не больше 3 имеет непустое L_{all} .

Для доказательства этих утверждений использовались аффинно неэквивалентные бент-функции, приведенные в [2].

Утверждение 3. Любая функция из $\mathfrak{B}_n$, аффинно эквивалентная функции в виде линейного разветвления с индексом линейности $n/2$, имеет непустое L_{all} . В частности, любая функция из класса Мэйорана — Мак-Фарланда имеет непустое L_{all} .

Описание класса $\mathfrak{B}_n$ в виде линейного разветвления можно найти в [1], класс Мэйорана — Мак-Фарланда в [3].

Утверждение 4. Существуют бент-функции от 8 переменных, имеющие непустое L_{all} , которые не являются аффинно эквивалентными функциям в виде линейного разветвления с индексом линейности 4.

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
2. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. Т. 3. № 1. С. 15–37.
3. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.