УДК 519.7 DOI 10.17223/2226308X/8/12

О СВЯЗНОСТИ ГРАФА МИНИМАЛЬНЫХ РАССТОЯНИЙ МНОЖЕСТВА БЕНТ-ФУНКЦИЙ[1]

Н. А. Коломеец

Рассматривается связность графа GB_{2k} минимальных расстояний множества бент-функций. Вершинами данного графа являются все бент-функции от $2k$ переменных, две вершины-функции соединены ребром, если они находятся на расстоянии 2^k друг от друга. Доказано, что подграф GB_{2k}, порождённый множеством бент-функций, аффинно эквивалентных бент-функциям из класса Мэйорана — МакФарланда, является связным. Доказана связность графов GB_2, GB_4 и GB_6.

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

Отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от n переменных. *Аффинной* булевой функцией называется функция вида $\langle a, x\rangle \oplus c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$ и $\langle a, x\rangle = a_1x_1 \oplus a_2x_2 \oplus \ldots \oplus a_nx_n$. *Расстоянием Хэмминга* $\mathrm{dist}(f, g)$ между двумя булевыми функциями f и g от n переменных называется количество $x \in \mathbb{F}_2^n$, таких, что $f(x) \neq g(x)$. *Бент-функцией* называется булева функция от чётного числа переменных, находящаяся на максимально возможном расстоянии от множества всех аффинных функций. Обозначим через $\mathcal{B}_{2k}$ множество всех бент-функций от $2k$ переменных. Бент-функции предложены О. Ротхаусом [1]. Они имеют большое число приложений в алгебре, комбинаторике, теории кодирования, криптографии [2].

Граф $GB_{2k} = (V, E)$ называется *графом минимальных расстояний множества бент-функций*, если $V = \mathcal{B}_{2k}$ и $(f, g) \in E$ тогда и только тогда, когда $\mathrm{dist}(f, g) = 2^k$. Заметим, что 2^k является минимально возможным расстоянием между двумя бент-функциями от $2k$ переменных.

Напомним, что функции следующего вида являются бент-функциями и образуют класс Мэйорана — МакФарланда M_{2k} [3]:

$$f(x, y) = \langle x, \pi(y)\rangle \oplus \varphi(y),$$

где $x, y \in \mathbb{F}_2^k$; π — подстановка на множестве $\mathbb{F}_2^k$; φ — произвольная булева функция от k переменных.

Пусть множество $\widetilde{M}_{2k}$ содержит все функции вида $f(Ax \oplus b)$, где $f \in M_{2k}$; A — обратимая двоичная матрица размера $2k \times 2k$ и $b \in \mathbb{F}_2^{2k}$. Другими словами, любая функция из $\widetilde{M}_{2k}$ является бент-функцией, *аффинно эквивалентной* некоторой бент-функции из класса Мэйорана — МакФарланда. Заметим, что $f \oplus \ell$ лежит в $\widetilde{M}_{2k}$ для любой $f \in \widetilde{M}_{2k}$ и любой аффинной функции ℓ от $2k$ переменных.

Обозначим через GM_{2k} подграф графа GB_{2k}, порождённый множеством вершин $\widetilde{M}_{2k}$. Известно [4], что максимальная степень вершины в графах GB_{2k} и GM_{2k} равна $2^k(2^1 + 1)(2^2 + 1)\ldots(2^k + 1)$, причём любая вершина максимальной степени является квадратичной бент-функцией.

В данной работе рассматривается связность графов GB_{2k} и GM_{2k}.

Утверждение 1. Степень любой вершины графа GM_{2k} не меньше, чем $2^{2k+1} - 2^k$.

Теорема 1. Граф GM_{2k} является связным для любого $k \geqslant 1$.

Следствие 1. Граф GM_{2k} является рёберно 3-связным.

[1]Работа поддержана грантом РФФИ, проект № 15–31–20635.

Следствие 2. Графы GB_2, GB_4 и GB_6 являются связными.

Отметим, что в общем случае граф GB_{2k} не является связным, поскольку он может содержать изолированные вершины. В частности, это справедливо при $2k \geqslant 14$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Tokareva N. N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
3. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.
4. *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.

УДК 519.7 DOI 10.17223/2226308X/8/13

О САМОДУАЛЬНЫХ БУЛЕВЫХ БЕНТ-ФУНКЦИЯХ[1]

А. В. Куценко

Получен критерий самодуальности (анти-самодуальности) булевой бент-функции, а именно доказано, что булева бент-функция f от чётного числа переменных является самодуальной (анти-самодуальной) тогда и только тогда, когда при каждом фиксированном $y \in \mathbb{F}_2^n$ для булевой функции $F_y(x) = f(x) \oplus f(y) \oplus x \cdot y$ справедливо $\mathrm{wt}(F_y) = 2^{n-1} - 2^{n/2-1}$ (соответственно $\mathrm{wt}(F_y) = 2^{n-1} + 2^{n/2-1}$).

Ключевые слова: *булева функция, бент-функция, самодуальная бент-функция.*

Булевой функцией f называется любое отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Скалярным произведением* $x \cdot y$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ называется $x \cdot y = \bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша – Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x \cdot y}$. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. Булева функция $\tilde{f}$ называется *дуальной* к бент-функции f, если $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ для каждого $x \in \mathbb{F}_2^n$. Бент-функция f называется *самодуальной (анти-самодуальной)*, если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). *Носителем* булевой функции f от n переменных называется множество $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. *Весом* вектора $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ называется число $\mathrm{wt}(x) = \sum\limits_{i=1}^{n} x_i$. *Весом Хэмминга* булевой функции f называется вес её вектора значений $\mathrm{wt}(f) = |\mathrm{supp}(f)|$. Сложной задачей является полная характеризация и описание класса самодуальных бент-функций. Этому вопросу посвящены несколько работ за рубежом (C. Carlet, L. E. Danielson, M. G. Parker, P. Solé, X. Hou и др.). В частности, в работе [1] перечислены все самодуальные бент-функции от 2, 4 и 6 переменных и все квадратичные самодуальные бент-функции от 8 переменных; в [2] приведена классификация всех квадратичных самодуальных бент-функций.

[1]Исследование выполнено при финансовой поддержке РФФИ (проект №15-31-20635).