**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).

**Теорема 1.** Булева бент-функция $f$ от чётного числа переменных $n$ 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 $2^{n-1} + 2^{n/2-1}$).

ЛИТЕРАТУРА

1. *Carlet C., Danielson L. E., Parker M. G., Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
2. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. Iss. 2. P. 183–198.

УДК 519.7 DOI 10.17223/2226308X/8/14

# ОБ ОБРАТИМОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ

И. А. Панкратова

Рассматривается класс $\mathcal{F}_{n,m,k}$ обратимых векторных булевых функций из $\mathbb{F}_2^n$ в $\mathbb{F}_2^m$, координатные функции которых существенно зависят от заданного числа $k$ переменных. Доказано: 1) таких функций не существует при любом $n = m$ и $k = 2$; 2) функции класса $\mathcal{F}_{n,n,n-1}$ могут (не могут) быть построены из аффинных координатных функций при чётном (нечётном) $n$; 3) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то и $\mathcal{F}_{n+1,m+1,k} \neq \varnothing$.

**Ключевые слова:** *векторная булева функция, обратимые функции.*

Задача построения обратимых векторных булевых функций возникает при создании многих криптосистем; в частности, такие функции используются в многораундовых симметричных блочных шифрах класса SIBCipher [1]. Для того чтобы значения функции можно было эффективно вычислять, часто вводится ограничение на количество существенных переменных у каждой координатной функции векторной функции.

Для $n, m, k \in \mathbb{Z}$ обозначим через $\mathcal{F}_{n,m,k}$ класс функций $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, где $F = (f_1 \dots f_m)$, таких, что координатные функции $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \dots, m$, существенно зависят ровно от $k$ переменных и функция $F$ — инъекция (т. е. обратима).

В случае $n = m$ (практически важном для построения многораундовых шифров) будем обозначать $\mathcal{F}_{n,k} = \mathcal{F}_{n,n,k}$.

Непосредственно проверяются следующие свойства:

1) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $m \geqslant n$;
2) если $F \in \mathcal{F}_{n,k}$, то $F$ есть подстановка на $\mathbb{F}_2^n$ и все её координатные функции уравновешены;
3) если $F = (f_1 \dots f_m) \in \mathcal{F}_{n,m,k}$, то и $F' = (f_1 \dots \bar{f}_i \dots f_m) \in \mathcal{F}_{n,m,k}$, $i \in \{1, \dots, m\}$;
4) если $\mathcal{F}_{n,m,k} \neq \varnothing$, то $\mathcal{F}_{n,t,k} \neq \varnothing$ для любого $t > m$;
5) если $\mathcal{F}_{k,k} \neq \varnothing$, то $\mathcal{F}_{ks,k} \neq \varnothing$ для любого $s > 1$.

Последнее свойство используется при построении шифров SIBCiphers семейства Люцифер [1]: $ks$ переменных разбиваются на блоки по $k$ переменных в каждом и «большая» раундовая функция набирается из $s$ «маленьких» функций — подстановок на $\mathbb{F}_2^k$.

**Пример 1.** Функция $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ с вектором значений (0 6 7 2 4 3 1 5) принадлежит множеству $\mathcal{F}_{3,3}$; её координатные функции $f_1 = x_1 \oplus x_2 \oplus x_3$, $f_2 = x_1x_2 \oplus \oplus x_2x_3 \oplus x_2 \oplus x_3$, $f_3 = x_1x_3 \oplus x_2x_3 \oplus x_2$.