УДК 519.7 DOI 10.17223/2226308X/10/17

О НЕКОТОРЫХ СВОЙСТВАХ ИЗВЕСТНЫХ ИЗОМЕТРИЧНЫХ ОТОБРАЖЕНИЙ МНОЖЕСТВА БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Рассматриваются свойства некоторых известных отображений булевых функций, отображающих множество бент-функций в себя и сохраняющих расстояние Хэмминга. Доказано, что не существует изометричного отображения множества всех булевых функций в себя, которое каждой бент-функции ставило бы в соответствие дуальную к ней. Для бент-функций от малого числа переменных получено утверждение, характеризующее аффинную эквивалентность бент-функции и функции, дуальной к ней.

Ключевые слова: *булева функция, бент-функция, изометричное отображение булевых функций, дуальная бент-функция.*

Булевы функции от одного числа переменных называются *аффинно эквивалентными*, если они равны с точностью до аффинной замены координат и сдвига на аффинную функцию от того же числа переменных. *Скалярное произведение* $x \cdot y$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ равно $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot y}$. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [1]. Булева функция $\tilde{f}$ называется *дуальной* к бент-функции f, если $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ для каждого $x \in \mathbb{F}_2^n$ [2]. Дуальная функция является бент-функцией и определяется однозначно. *Расстояние Хэмминга* $\mathrm{dist}(f, g)$ между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения. Отображение φ множества всех булевых функций от n переменных в себя называется *изометричным*, если оно сохраняет расстояние Хэмминга между булевыми функциями, т. е. $\mathrm{dist}(\varphi(f), \varphi(g)) = \mathrm{dist}(f, g)$, где f, g — произвольные булевы функции от n переменных.

Известно, что отображение, определённое на множестве бент-функций и сопоставляющее каждой бент-функции дуальную к ней, сохраняет расстояние Хэмминга [3]. В [4] доказано, что единственным изометричным отображением множества всех булевых функций в себя, сохраняющим множество бент-функций на месте, является композиция аффинного преобразования координат и аффинный сдвиг.

В данной работе получены некоторые свойства известных отображений, оставляющих множество бент-функций на месте и сохраняющих расстояние Хэмминга.

Утверждение 1. Отображение, определённое на множестве бент-функций от чётного числа переменных n, действующее по правилу $f(x) \to \tilde{f}(x)$, не может быть расширено до изометричного отображения множества всех булевых функций от n переменных.

Утверждение 2. Пусть $n \leqslant 6$ — чётное число, тогда каждая бент-функция от n переменных аффинно эквивалентна своей дуальной бент-функции.

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.

Утверждение 3. При каждом чётном $n \geqslant 6$ существуют различные бент-функции от n переменных, не совпадающие со своими дуальными функциями и их отрицаниями, которые не могут быть получены друг из друга с помощью отображения, представляющего собой композицию аффинного преобразования координат, аффинного сдвига и постановки в соответствие дуальной бент-функции.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Carlet C., Danielson L. E., Parker M. G., and Solé P.* Self dual bent functions // Int. J. Inform. Coding Theory. 2010. No. 1. P. 384–399.
3. *Carlet C.* Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. N. Y.: Cambridge Univ. Press, 2010. P. 257–397.
4. *Токарева Н. Н.* Группа автоморфизмов множества бент-функций // Дискретная математика. 2010. Т. 22. № 4. С. 34–42.

УДК 519.7 DOI 10.17223/2226308X/10/18

ВЗАИМНО ОДНОЗНАЧНЫЕ БИНОМИАЛЬНЫЕ ВЕКТОРНЫЕ БУЛЕВЫ ФУНКЦИИ В ПОЛИНОМИАЛЬНОМ ПРЕДСТАВЛЕНИИ. УСЛОВИЯ СУЩЕСТВОВАНИЯ[1]

А. В. Милосердов

Сформулировано и доказано необходимое условие взаимной однозначности биномиальной векторной булевой функции. Исследован вопрос существования взаимно однозначных биномиальных функций при различном числе переменных.

Ключевые слова: *полиномиальное представление, взаимно однозначные функции, биномиальные функции.*

Компонентами многих шифров являются S-блоки — векторные булевы функции. В большинстве случаев S-блоки являются перестановками, то есть взаимно однозначными функциями. Для программной и аппаратной реализации S-блока на вычислительных системах хорошо подходит его полиномиальное представление. Например, полиномиальное представление S-блоков используется в AES — современном стандарте симметричного шифрования США.

В работе исследуются взаимосвязи между комбинаторным и алгебраическим представлениями взаимно однозначных векторных булевых функций [1]. Рассматриваются взаимно однозначные функции $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(x) = \alpha^k x^i + x^j$, где α — примитивный элемент поля; $0 \leqslant k \leqslant 2^n - 1$ и $1 \neq j < i \leqslant 2^n - 1$.

Теорема 1. Пусть $1 \leqslant j < i \leqslant 2^n - 1$, $1 \leqslant k \leqslant 2^n - 1$, α — примитивный элемент поля $\mathbb{F}_{2^n}$. Если функция $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(y) = \alpha^k y^i + y^j$ взаимно однозначна, то $(i - j, 2^n - 1)$ не делит $(k, 2^n - 1)$.

Теорема 2. Пусть $1 \leqslant j < i \leqslant 2^n - 1$, $1 \leqslant k \leqslant 2^n - 1$, α — примитивный элемент поля $\mathbb{F}_{2^n}$. Если $2^n - 1$ — простое, то взаимно однозначных функций $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(x) = \alpha^k x^i + x^j$ не существует.

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.