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.

Теорема 3. 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 n — составное число, то существует взаимно однозначная функция $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(x) = \alpha^k x^i + x^j$.

Опираясь на результаты [2], доказана

Теорема 4. Если $2^n - 1$ имеет делитель $d < \dfrac{n}{2\log_2(n)} - 1$, то существует взаимно однозначная функция $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(y) = ay^i + y^j$ для некоторого $a \in \mathbb{F}^*_{2^n}$, $0 < j < i < 2^n - 1$.

Остался не исследованным вопрос существования взаимно однозначной векторной булевой функции при простом числе n и составном числе $2^n - 1$, если у него нет делителя $d < \dfrac{n}{2\log_2(n)} - 1$.

С использованием полученных результатов найдены все взаимно однозначные функции данного вида для всех $n \leqslant 8$. При этих же значениях n найдены все взаимно однозначные биномиальные дифференциально 4-равномерные векторные булевы функции. Посчитано количество взаимно однозначных биномиальных функций с максимальной компонентной алгебраической иммунностью при $n = 4, 6$. При $n = 4$ таких функций 10, а при $n = 6$ — 319 [3].

ЛИТЕРАТУРА

1. *Shallue C. J.* Permutation Polynomials of Finite Fields. Honours Thesis. Monash University, 2012.
2. *Masuda A. M. and Zieve M. E.* Permutation binomials over finite Ffeld // Trans. AMS. 2009. V. 361. No. 8. P. 4169–4180.
3. *Милосердов А. В.* Комбинаторные свойства полиномиального представления булевой функции. Выпускная квалификационная работа бакалавра. Новосибирск: НГУ, 2017.

УДК 519.7 DOI 10.17223/2226308X/10/19

НИЖНИЕ ОЦЕНКИ РАЗМЕРНОСТИ ЛИНЕЙНЫХ КОДОВ ДЛЯ ТЕХНОЛОГИИ СОТОВОЙ СВЯЗИ CDMA[1]

Н. С. Одинокиx

Линейный код называется *кодом, сохраняющим свойство бент* (*SPB-кодом*) для функции f, если сдвиг на любой элемент кода оставляет функцию f в классе бент-функций. В работе построены линейные SPB-коды для функций из класса Мэйорана — МакФарланда, получены нижние оценки максимальной размерности SPB-кодов для произвольной бент-функции.

Ключевые слова: *линейные коды, бент-функции, коды постоянной амплитуды.*

Code Division Multiple Access (CDMA) — это технология мобильной связи, основанная на кодовом разделении канала. Для оценки качества сигнала в CDMA вводится понятие коэффициента отношения пиковой и средней мощностей сигнала (Peak-to-Average Power Ratio). Многие задачи, связанные с CDMA, направлены на снижение коэффициента PAPR, так как высокие значения коэффициента ведут к необходимости использования дорогих усилителей. Векторами, на которых достигается минимальное

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