УДК 519.7 DOI 10.17223/2226308X/9/11

О МНОЖЕСТВЕ РАССТОЯНИЙ ХЭММИНГА МЕЖДУ САМОДУАЛЬНЫМИ БЕНТ-ФУНКЦИЯМИ[1]

А. В. Куценко

Получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда со следующим ограничением: перестановка, фигурирующая в данной конструкции, должна быть элементом полной линейной группы соответствующего порядка. На основании этого результата сделан вывод о минимальном расстоянии Хэмминга между рассмотренными функциями.

Ключевые слова: *булева функция, бент-функция, преобразование Уолша — Адамара, самодуальная бент-функция, конструкция Мэйорана — МакФарланда.*

Булевой функцией f называется любое отображение $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$. *Скалярным произведением* $\langle x, y\rangle$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_2^n$ называется число $\bigoplus\limits_{i=1}^{n} x_i y_i$, где операция $\oplus$ есть сложение по модулю 2. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{Z}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y\rangle}$. Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{Z}_2^n$ [1]. Булева функция $\tilde{f}$ называется *дуальной* к бент-функции f, если $W_f(x) = (-1)^{\tilde{f}(x)} 2^{n/2}$ для каждого $x \in \mathbb{Z}_2^n$. Бент-функция f называется *самодуальной* (*анти-самодуальной*), если $f = \tilde{f}$ (соответственно $f = \tilde{f} \oplus 1$). *Расстояние Хэмминга* между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения, обозначается как $\mathrm{dist}(f, g)$.

Известна следующая конструкция бент-функций: *конструкция Мэйорана — МакФарланда* (1973): пусть π — любая перестановка на $\mathbb{Z}_2^{n/2}$, а h — произвольная булева функция от $n/2$ переменных. Тогда функция $f(x, y) = \langle x, \pi(y)\rangle \oplus h(y)$ является бент-функцией от n переменных [2]. Эта конструкция является достаточно богатой. В работе [3] найдены необходимые и достаточные условия самодуальности бент-функции, построенной с помощью конструкции Мэйорана — МакФарланда, в случае $\pi \in \mathrm{GL}(n/2, \mathbb{Z}_2)$.

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, T. Feulner, L. Sok, A. Wassermann и др.). В частности, в работе [3] перечислены все самодуальные бент-функции от 2, 4, 6 переменных и все квадратичные самодуальные бент-функции от 8 переменных. В [4] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных можно найти в [5].

В данной работе получен полный спектр расстояний Хэмминга между самодуальными бент-функциями из класса Мэйорана — МакФарланда со следующим ограничением: перестановка, фигурирующая в конструкции, должна быть элементом полной линейной группы соответствующего порядка.

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

Теорема 1. Пусть f, g — различные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана — МакФарланда при условии, что перестановка, фигурирующая в данной конструкции, является элементом $\mathrm{GL}(n/2, \mathbb{Z}_2)$. Если бент-функции f, g самодуальные, то

$$\mathrm{dist}(f,g) \in \{2^{n-1}, 2^{n-1}(1 \pm 1/2), 2^{n-1}\left(1 \pm 1/2^2\right), \ldots, 2^{n-1}\left(1 \pm 1/2^{n/2-1}\right), 2^n\}.$$

Следствие 1. Пусть f, g — различные самодуальные бент-функции от чётного числа переменных $n \geqslant 4$, построенные с помощью конструкции Мэйорана — МакФарланда при условии, что перестановка, фигурирующая в данной конструкции, является элементом $\mathrm{GL}(n/2, \mathbb{Z}_2)$. Тогда

$$\mathrm{dist}(f,g) \geqslant 2^{n-2}.$$

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *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.
3. *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.
4. *Hou X.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. P. 183–198.
5. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. P. 395–406.

УДК 519.7 DOI 10.17223/2226308X/9/12

УСЛОВИЯ СУЩЕСТВОВАНИЯ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ С МАКСИМАЛЬНОЙ КОМПОНЕНТНОЙ АЛГЕБРАИЧЕСКОЙ ИММУННОСТЬЮ[1]

Д. П. Покрасенко

Исследуется максимальная компонентная алгебраическая иммунность и её связь с матрицами специального вида. Получены ограничения на значения n, m, при которых возможно существование векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ с максимальной компонентной алгебраической иммунностью.

Ключевые слова: *векторная булева функция, компонентная алгебраическая иммунность.*

Важным криптографическим свойством булевых функций является алгебраическая иммунность, она была введена в работе [1]. *Алгебраической иммунностью* $\mathrm{AI}(f)$ булевой функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется минимальное число d, такое, что существует булева функция g степени d, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$.

Данное понятие различными способами было обобщено на векторный случай. Одним из наиболее естественных обобщений является понятие компонентной алгебраической иммунности, введённое в [2]. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $b \cdot F$ ($b \in \mathbb{Z}_2^m$, $b \neq 0$), т. е. $\mathrm{AI}_{\mathrm{comp}}(F) = \min\{\mathrm{AI}(b \cdot F) : b \in \mathbb{Z}_2^m, b \neq 0\}$, где $b \cdot F = b_1 f_1 \oplus \ldots \oplus b_m f_m$.

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