ЛИТЕРАТУРА

1. *Солодовников В. И.* Регистры сдвига и криптоалгоритмы на их основе. LAP LAMBERT Academic Publishing, 2017.
2. *Солодовников В. И.* Гомоморфизмы регистров сдвига в линейные автоматы // Дискретная математика. 2008. № 4. С. 87–101.
3. *Лидл Р., Нидеррайтер Г.* Конечные поля. М.: Мир, 1988.
4. *Солодовников В. И.* Гомоморфизмы двоичных регистров сдвига // Дискретная математика. 2005. № 1. С. 73–88.
5. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. № 10. С. 97–122.
6. *Черемушкин А. В.* Аддитивный подход к определению степени нелинейности дискретной функции // Прикладная дискретная математика. 2010. № 2. С. 22–33.

УДК 519.7 DOI 10.17223/2226308X/12/22

# О ВЗАИМОСВЯЗИ МЕЖДУ КВАТЕРНАРНЫМИ И БУЛЕВЫМИ БЕНТ-ФУНКЦИЯМИ[1]

А. С. Шапоренко

Исследуются кватернарные бент-функции вида $f : \mathbb{Z}_4^n \to \mathbb{Z}_4$. Показано представление коэффициентов Уолша — Адамара кватернарной функции через коэффициенты двух булевых функций. Получено, что любая кватернарная бент-функция является регулярной. Изучается связь кватернарных бент-функций от одной и двух переменных с булевыми бент-функциями от двух и четырёх переменных соответственно.

**Ключевые слова:** *кватернарные функции, булевы функции, регулярные бент-функции.*

Пусть $\langle x, y\rangle$ — скалярное произведение векторов, где суммирование производится по модулю 2, а $x.y$ — скалярное произведение векторов с суммированием по модулю 4.

*Преобразованием Уолша — Адамара булевой функции* $f$ от $n$ переменных называется целочисленная функция $W_f(x)$, заданная на множестве $\mathbb{Z}_2^n$ равенством

$$W_f(x) = \sum_{y \in \mathbb{Z}_2^n} (-1)^{\langle x,y\rangle \oplus f(y)}.$$

Булева функция $f$ от $n$ ($n$ — чётное) переменных называется *бент-функцией*, если $|W_f(x)| = 2^{n/2}$ для любого $x \in \mathbb{Z}_2^n$.

Функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется *кватернарной функцией* от $n$ переменных [1]. *Преобразование Уолша — Адамара кватернарной функции* $g$ определяется следующим образом:

$$W_g(x) = \sum_{y \in \mathbb{Z}_4^n} i^{x.y+g(y)}.$$

Здесь «+» означает сложение по модулю 4.

Кватернарная функция $g$ от $n$ переменных называется *бент-функцией*, если $|W_g(x)| = 4^{n/2}$ для любого $x \in \mathbb{Z}_4^n$.

[1]Работа выполнена при финансовой поддержке РФФИ (проект № 18-07-01394), Министерства образования и науки (Задание № 1.13559.2019/13.1 и Программа 5-100).

Пусть кватернарная функция $g$ от $n$ переменных задается для любых $x, y \in \mathbb{Z}_2^n$ следующим образом:

$$g(x + 2y) = a(x, y) + 2b(x, y),$$

где сложение производится по модулю 4; $a$ и $b$ — булевы функции от $2n$ переменных.

**Лемма 1.** Справедлива следующая связь коэффициентов Уолша — Адамара функций $g, b$ и $a \oplus b$:

$$W_g(x + 2y) = \frac{1}{2}(W_b(x \oplus y, y) + W_{a\oplus b}(y, x) - 2c_1 - 2d_1) +$$
$$+\frac{i}{2}(W_b(y, x) - W_{a\oplus b}(x \oplus y, x) - 2c_2 + 2d_2),$$

где

$$c_1 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle},\ c_2 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle},$$
$$d_1 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle},\ d_2 = \sum_{x'\in X_1, y'\in\mathbb{Z}_2^n} (-1)^{b(x',y')\oplus a(x',y')\oplus\langle x,y'\rangle\oplus\langle y,x'\rangle\oplus\langle x,x'\rangle}.$$

Множество $X_1$ состоит из всех таких $x' \in \mathbb{Z}_2^n$, для которых равенство $\langle x, x'\rangle = x.x'$ не выполняется.

Кватернарная бент-функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ называется *регулярной* [2], если каждый коэффициент Уолша — Адамара этой функции может быть представлен в виде $W_g(x) = 4^{n/2} i^{h(x)}$, где $h(x)$ — некоторая кватернарная функция.

**Теорема 1.** Кватернарная бент-функция $g : \mathbb{Z}_4^n \to \mathbb{Z}_4$ является регулярной при любом $n$.

Из леммы 1 следует, что для $n = 1$

$$W_g(x + 2y) = \frac{1}{2}(W_b(x \oplus y, y) + W_{a\oplus b}(y, x)) + \frac{i}{2}(W_b(y, x) - W_{a\oplus b}(x \oplus y, x)),$$

так как множество $X_1$ пусто для любого $x$.

**Утверждение 1.** Пусть функция $g(x + 2y) = a(x, y) + 2b(x, y)$, где $x, y \in \mathbb{Z}_2$; $a$ и $b$ — булевы функции от двух переменных, является бент-функцией. Тогда $b$ и $a \oplus b$ — бент-функции. Обратное, вообще говоря, не верно.

Так, функция $g(x_1+2x_2) = x_2+2x_1x_2$ не является бент-функцией, но $b(x_1, x_2) = x_1x_2$ и $a(x_1, x_2) \oplus b(x_1, x_2) = x_1x_2 \oplus x_2$ — бент-функции.

Компьютерные вычисления показали, что количество кватернарных бент-функций от одной переменной равно 32. Чтобы получить каждую из них, достаточно взять в качестве функции $b(x_1, x_2)$ любую из восьми булевых бент-функций от двух переменных и использовать одну из четырёх функций $0, 1, x_1$ или $x_1 \oplus 1$ в качестве функции $a(x_1, x_2)$.

Количество кватернарных бент-функций при $n = 2$ равно 200704. Среди них 98304 — таких, что ни одна из булевых функций $a, b$ и $a \oplus b$ не является бент-функцией, но при этом для 3072 из них $a$ линейная. Существуют 36864 функции, таких, что $b$ и $a \oplus b$ — бент-функции, при этом для 33792 из них функция $a$ нелинейная, а для 2304 и 768 является линейной функцией и константой соответственно. Количество кватернарных функций, для которых каждая из функций $a, b$ и $a \oplus b$ — бент-функция, равно 16384. Для оставшихся 49152 функций $a$ является бент-функцией, а $b$ и $a \oplus b$ — нелинейные булевы функции. Интересно, что среди всех кватернарных бент-функций нет ни одной, для которой $b$ или $a \oplus b$ были бы линейными или константами.

ЛИТЕРАТУРА

1. *Kumar P. V., Scholtz R. A., and Welch L. R.* Generalized bent functions and their properties // J. Combin. Theory. Ser. A40. 1985. P. 90–107.
2. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press, 2015.

УДК 621.391:519.7 DOI 10.17223/2226308X/12/23

# КЛАСС БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ДВОИЧНЫХ РАЗРЯДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦОМ $\mathbb{Z}_{2^n}$

Д. У. Эрнандес Пилото

Рассматривается класс булевых функций, построенных на основе двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ с отмеченным характеристическим многочленом максимального периода. Для этого класса изучаются веса функций, степень нелинейности функций, расстояние между функциями. Кроме того, рассматривается расстояние между функциями из разных классов.

**Ключевые слова:** *булевы функции, линейные рекуррентные последовательности, двоичные разрядные последовательности.*

## Введение

Пусть $R = \mathbb{Z}_{2^n}$ — кольцо вычетов по модулю $2^n$, $F(x)$ — отмеченный многочлен степени $m$ максимального периода $T(F) = 2^m - 1$ над кольцом $R$ [1]. Введём обозначения: $P = \mathbb{Z}_2$; $\bar{F}(x)$ — многочлен, полученный из $F(x)$ приведением всех его коэффициентов по модулю 2. Тогда $T(\bar{F}) = 2^m - 1$ и $\bar{F}(x)$ является примитивным многочленом над полем $P$. Пусть $\omega_1, \ldots, \omega_m$ — линейно независимая система линейных рекуррентных последовательностей (ЛРП) над полем $P$ с характеристическим многочленом $\bar{F}(x)$. Обозначим через $L_R(F)^*$ множество всех ЛРП $u$ над кольцом $R$, у которых среди элементов $u(0), \ldots, u(m-1)$ есть хотя бы один обратимый элемент кольца $R$. Рассмотрим функцию $\psi : R \longrightarrow P$, действующую на каждый элемент $a \in R$ с двоичным представлением

$$a = a_0 + 2a_1 + 2^2a_2 + \ldots + 2^{n-1}a_{n-1}, \quad a_0, a_1, \ldots a_{n-1} \in P$$

по правилу

$$\psi(a) = a_{n-1} \oplus a_{n-2}a_{n-3} \ldots a_{n-k}, \tag{1}$$

где $n \geqslant 3$; $k \in \{3, \ldots, n\}$. Для каждой ЛРП $u \in L_R(F)^*$ рассмотрим булеву функцию $f(x_1, \ldots, x_m) = f_{u,\psi}(x_1, \ldots, x_m)$, определённую по следующему правилу: $f(0, \ldots, 0) = \psi(0)$ и для всех $i \in \{0, \ldots, 2^m - 2\}$

$$f(\omega_1(i), \ldots, \omega_m(i)) = \psi(u(i)). \tag{2}$$

Пусть $\chi : R \longrightarrow \mathbb{C}^*$ — аддитивный характер кольца $R$, определённый равенством

$$\chi(x) = e^{2\pi i x/2^n}, \ x \in R.$$

Группа всех аддитивных характеров кольца $R$ имеет вид $\{\chi(ax) : a \in R\}$. Множество всех отображений из $R$ в $\mathbb{C}^*$ образует унитарное пространство со скалярным произведением, определённым для отображений $g$ и $h$ по правилу

$$\langle g, h \rangle = \sum_{x \in R} g(x)\bar{h}(x).$$