Math-Net.Ru

Общероссийский математический портал

О. В. Камловский, Суммы модулей коэффициентов Уолша–Адамара некоторых сбалансированных булевых функций, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 4, 75–98

DOI: <https://doi.org/10.4213/mvk240>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.149

26 апреля 2023 г., 13:26:36

Суммы модулей коэффициентов Уолша – Адамара некоторых сбалансированных булевых функций

О. В. Камловский

ООО «Центр сертификационных исследований», Москва

Получено 11.V.2017

Аннотация. Рассматриваются следующие сбалансированные булевы функции от n переменных: а) построенные из нормальных бент-функций методом Доббертина, б) мажоритарная, в) функции, у которых в столбце значений единичные значения располагаются подряд, начиная с любого места. Для них вычисляются точные значения сумм модулей коэффициентов Уолша – Адамара и приводятся их оценки.

Ключевые слова: булевы функции, коэффициенты Уолша – Адамара, фильтрующие генераторы, комбинирующие генераторы

The sum of modules of Walsh coefficients for some balanced Boolean functions

O. V. Kamlovskii

Certification Research Center, LLC, Moscow

Abstract. We consider the following balanced Boolean functions: a) constructed from normal bent-function by the Dobbertin method, b) majority function, c) functions whose units values are located consequentially in the truth table. Exact formulas and bounds for sums of modules of Walsh coefficients are obtained.

Keywords: Boolean functions, Walsh coefficients, filtering generators, combining generators

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 4, pp. 75–98 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

Введение

Пусть n — натуральное число, f — булева функция от n переменных. Коэффициент $W_f(\vec{a})$ Уолша–Адамара булевой функции f определяется для каждого вектора $\vec{a} = (a_1, a_2, \dots, a_n) \in \{0, 1\}^n$ равенством (см., например, [1])

$$W_f(\vec{a}) = \sum_{\vec{b}=(b_1, b_2, \dots, b_n) \in \{0, 1\}^n} (-1)^{f(\vec{b}) \oplus a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_n b_n}.$$

Введем обозначение

$$\sigma(f) = \sum_{\vec{a} \in \{0, 1\}^n} |W_f(\vec{a})|.$$

В работах [2, 3] величина $\sigma(f)$ была использована для оценивания частот появлений элементов на отрезках выходных последовательностей фильтрующих и комбинирующих генераторов с функцией усложнения f . Чем меньше значение $\sigma(f)$, тем более точные оценки рассматриваемых частот удастся получить.

Отдельному исследованию величины $\sigma(f)$ посвящена работа [4], где были получены следующие оценки:

$$2^n \leq \sigma(f) \leq 2^{3n/2},$$

справедливые для каждой булевой функции f от n переменных. Указанная нижняя оценка обращается в равенство тогда и только тогда, когда f — аффинная булева функция. Верхняя оценка обращается в равенство тогда и только тогда, когда f — бент-функция. Кроме того, было показано, что среднее значение параметра $\sigma(f)$ в классе всех булевых функций от n переменных и в его подклассе из всех сбалансированных булевых функций эквивалентно при $n \rightarrow \infty$ величине

$$\sqrt{\frac{2}{\pi}} 2^{3n/2}.$$

В данной работе приводятся точные значения величин $\sigma(f)$ в случае, когда f — произвольная сбалансированная функция, полученная из нормальной бент-функции методом Г. Доббертина [5]. Доказывается, что для этих функций при $n \rightarrow \infty$

$$\sigma(f) \sim 2^{3n/2}.$$

Ранее в [4] этот результат был получен для частного случая, когда f — бент-функция из класса Мэйорана–Мак-Фарланда (см., например, [6, 7]). Изучается величина $\sigma(f)$ для мажоритарной булевой функции f от нечетного числа переменных. В этом случае получены оценки снизу и сверху исследуемой величины, из которых следует, что

$$\sigma(f) \sim \frac{2}{\sqrt{\pi n}} 2^{3n/2} \quad \text{при } n \rightarrow \infty.$$

Кроме того, рассматривается класс функций f , у которых столбец значений (при лексикографическом порядке) получен всевозможными циклическими сдвигами столбца значений функции $f(x_{n-1}, x_{n-2}, \dots, x_0) = x_{n-1}$. В этом случае вычисляются точные значения величин $\sigma(f)$ и показано, что

$$\sigma(f) \leq \frac{n 2^{n+1}}{3}.$$

1. Функции, построенные с использованием конструкции Г. Доббертина

Пусть $n = 2k$, где k — произвольное натуральное число, $h(\vec{x}, \vec{y})$ — булева функция от n переменных, где $\vec{x} = (x_1, x_2, \dots, x_k)$, $\vec{y} = (y_1, y_2, \dots, y_k)$. Бент-функция h называется нормальной (см. [5]), если существует такое многообразие $M = \vec{\alpha} + L$, порожденное линейным пространством L размерности $\dim L = k$ и вектором $\vec{\alpha}$, что ограничение h на M является константой. Отметим, что не каждая бент-функция h является нормальной (см. [8]), однако практически все известные классы бент-функций состоят только из нормальных бент-функций.

Пусть $M = \vec{\alpha} \oplus L$, где $\vec{\alpha} \in \{0, 1\}^n$, а L — линейное пространство двоичных векторов-строк длины n , $\dim L = k$. Рассмотрим линейное пространство $L_0 = \{(\vec{0}, \vec{y}) : \vec{y} \in \{0, 1\}^k\}$. Покажем, что функция h аффинно-эквивалентна (см., например, [1]) бент-функции $\varphi(\vec{x}, \vec{y})$, которая является константой на многообразии $\{(\vec{x}_0, \vec{y}) : \vec{y} \in \{0, 1\}^k\} = (\vec{x}_0, \vec{0}) \oplus L_0$. Действительно, если τ — такое обратимое линейное преобразование линейного пространства $\{0, 1\}^n$, что $\tau(L) = L_0$, то для бент-функции $\varphi(\vec{x}, \vec{y}) = h(\tau^{-1}(\vec{x}, \vec{y}))$ имеем

$$\varphi|_{\tau(\vec{\alpha}) \oplus L_0} = \text{const} = c,$$

и если $\tau(\vec{\alpha}) = (\vec{x}_0, \vec{y}_0)$, то

$$\tau(\vec{\alpha}) \oplus L_0 = (\vec{x}_0, \vec{0}) \oplus L_0.$$

Выберем произвольную булеву функцию $g(\vec{y})$ от k переменных и построим функцию $f(\vec{x}, \vec{y})$ по правилу

$$f(\vec{x}, \vec{y}) = \begin{cases} g(\vec{y}), & \text{если } \vec{x} = \vec{x}_0, \\ \varphi(\vec{x}, \vec{y}), & \text{если } \vec{x} \neq \vec{x}_0. \end{cases} \quad (1)$$

Данная конструкция была предложена Г. Доббертином в работе [5], где она рассматривалась в случае $\vec{x}_0 = \vec{0}$, $c = 0$. Для построенных функций удастся вычислить величину $\sigma(f)$.

Теорема 1. Пусть f — булева функция, определенная равенством (1). Тогда

$$\sigma(f) = 2^{3n/2} - 2^n + 2^{n/2} |W_g(\vec{0})|.$$

Доказательство. Вычислим коэффициенты Уолша – Адамара $W_f(\vec{a}, \vec{b})$ функции f , где $\vec{a}, \vec{b} \in \{0, 1\}^k$. Имеем:

$$\begin{aligned} W_f(\vec{a}, \vec{b}) &= \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n} (-1)^{f(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{b} \rangle, \langle \vec{x}, \vec{y} \rangle} = \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n} (-1)^{f(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{x} \rangle \oplus \langle \vec{b}, \vec{y} \rangle} = \\ &= \sum_{\vec{y} \in \{0, 1\}^k} (-1)^{g(\vec{y}) \oplus \langle \vec{a}, \vec{x}_0 \rangle \oplus \langle \vec{b}, \vec{y} \rangle} + \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n, \vec{x} \neq \vec{x}_0} (-1)^{\varphi(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{x} \rangle \oplus \langle \vec{b}, \vec{y} \rangle} = \\ &= (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} W_g(\vec{b}) + S(\vec{a}, \vec{b}), \end{aligned}$$

где

$$S(\vec{a}, \vec{b}) = \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n, \vec{x} \neq \vec{x}_0} (-1)^{\varphi(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{x} \rangle \oplus \langle \vec{b}, \vec{y} \rangle}.$$

Пусть $\tilde{\varphi}$ — бент-функция, дуальная к функции φ (см. [1]). Тогда

$$W_{\varphi}(\vec{a}, \vec{b}) = \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n} (-1)^{\varphi(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{x} \rangle \oplus \langle \vec{b}, \vec{y} \rangle} = (-1)^{\tilde{\varphi}(\vec{a}, \vec{b})} 2^k,$$

кроме того,

$$\begin{aligned} \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n, \vec{x} = \vec{x}_0} (-1)^{\varphi(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{x} \rangle \oplus \langle \vec{b}, \vec{y} \rangle} &= (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} \sum_{\vec{y} \in \{0, 1\}^k} (-1)^{\varphi(\vec{x}_0, \vec{y}) \oplus \langle \vec{b}, \vec{y} \rangle} = \\ &= (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} \sum_{\vec{y} \in \{0, 1\}^k} (-1)^{c \oplus \langle \vec{b}, \vec{y} \rangle} = (-1)^{\langle \vec{a}, \vec{x}_0 \rangle \oplus c} 2^k \delta_{\vec{b}, \vec{0}}, \end{aligned}$$

где $\delta_{\vec{b}, \vec{0}} = 0$, если $\vec{b} \neq \vec{0}$, и $\delta_{\vec{b}, \vec{0}} = 1$, если $\vec{b} = \vec{0}$.

Значит,

$$S(\vec{a}, \vec{b}) = \left((-1)^{\tilde{\varphi}(\vec{a}, \vec{b})} - (-1)^{\langle \vec{a}, \vec{x}_0 \rangle \oplus c} \delta_{\vec{b}, \vec{0}} \right) 2^k.$$

Таким образом, получаем формулу

$$W_f(\vec{a}, \vec{b}) = \begin{cases} (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} W_g(\vec{b}) + 2^k (-1)^{\tilde{\varphi}(\vec{a}, \vec{b})} & \text{при } \vec{b} \neq \vec{0}, \\ (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} W_g(\vec{0}) + 2^k \left((-1)^{\tilde{\varphi}(\vec{a}, \vec{0})} - (-1)^{\langle \vec{a}, \vec{x}_0 \rangle \oplus c} \right) & \text{при } \vec{b} = \vec{0}. \end{cases} \quad (2)$$

Рассмотрим величину

$$\sum_{\vec{a} \in \{0,1\}^k} W_{\varphi}(\vec{a}, \vec{b}) (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} = \sum_{\vec{a} \in \{0,1\}^k} 2^k (-1)^{\tilde{\varphi}(\vec{a}, \vec{b}) \oplus \langle \vec{a}, \vec{x}_0 \rangle}.$$

Она равна

$$\begin{aligned} & \sum_{\vec{a} \in \{0,1\}^k} \sum_{\vec{x}, \vec{y} \in \{0,1\}^k} (-1)^{\varphi(\vec{x}, \vec{y}) \oplus \langle \vec{a}, \vec{x} \rangle \oplus \langle \vec{b}, \vec{y} \rangle \oplus \langle \vec{a}, \vec{x}_0 \rangle} = \\ &= \sum_{\vec{x}, \vec{y} \in \{0,1\}^k} (-1)^{\varphi(\vec{x}, \vec{y}) \oplus \langle \vec{b}, \vec{y} \rangle} \sum_{\vec{a} \in \{0,1\}^k} (-1)^{\langle \vec{a}, \vec{x} \oplus \vec{x}_0 \rangle} = \\ &= 2^k \sum_{\vec{y} \in \{0,1\}^k} (-1)^{\varphi(\vec{x}_0, \vec{y}) \oplus \langle \vec{b}, \vec{y} \rangle} = 2^k \sum_{\vec{y} \in \{0,1\}^k} (-1)^{c \oplus \langle \vec{b}, \vec{y} \rangle} = 2^{2k} (-1)^c \delta_{\vec{b}, \vec{0}}. \end{aligned}$$

Поэтому

$$\sum_{\vec{a} \in \{0,1\}^k} (-1)^{\tilde{\varphi}(\vec{a}, \vec{b}) \oplus \langle \vec{a}, \vec{x}_0 \rangle} = \begin{cases} 0, & \text{если } \vec{b} \neq \vec{0}, \\ 2^k (-1)^c, & \text{если } \vec{b} = \vec{0}. \end{cases} \quad (3)$$

В частности, получим тождество $\tilde{\varphi}(\vec{a}, \vec{0}) = \langle \vec{a}, \vec{x}_0 \rangle \oplus c$, из которого согласно равенствам (2)

$$W_f(\vec{a}, \vec{b}) = \begin{cases} (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} W_g(\vec{b}) + 2^k (-1)^{\tilde{\varphi}(\vec{a}, \vec{b})}, & \text{если } \vec{b} \neq \vec{0}, \\ (-1)^{\langle \vec{a}, \vec{x}_0 \rangle} W_g(\vec{0}), & \text{если } \vec{b} = \vec{0}. \end{cases} \quad (4)$$

Для модулей коэффициентов Уолша – Адамара, учитывая неравенства $|W_g(\vec{b})| \leq 2^k$ ($\vec{b} \in \{0,1\}^k$), имеем

$$|W_f(\vec{a}, \vec{b})| = \begin{cases} |W_g(\vec{0})|, & \text{если } \vec{b} = \vec{0}, \\ 2^k - W_g(\vec{b}), & \text{если } \tilde{\varphi}(\vec{a}, \vec{b}) \neq \langle \vec{a}, \vec{x}_0 \rangle, \\ 2^k + W_g(\vec{b}), & \text{если } \tilde{\varphi}(\vec{a}, \vec{b}) = \langle \vec{a}, \vec{x}_0 \rangle. \end{cases}$$

Значит, для суммы всех модулей рассматриваемых коэффициентов справедливо равенство

$$\begin{aligned}\sigma(f) &= \sum_{\vec{a} \in \{0,1\}^k, \vec{b} = \vec{0}} |W_g(\vec{0})| + \sum_{\vec{b} \neq \vec{0}} \sum_{\vec{a}: \tilde{\varphi}(\vec{a}, \vec{b}) = \langle \vec{a}, \vec{x_0} \rangle} (2^k + W_g(\vec{b})) + \\ &+ \sum_{\vec{b} \neq \vec{0}} \sum_{\vec{a}: \tilde{\varphi}(\vec{a}, \vec{b}) \neq \langle \vec{a}, \vec{x_0} \rangle} (2^k - W_g(\vec{b})).\end{aligned}$$

Из соотношения (3) следует, что при каждом фиксированном $\vec{b} \neq \vec{0}$ равенство $\tilde{\varphi}(\vec{a}, \vec{b}) = \langle \vec{a}, \vec{x_0} \rangle$ выполняется ровно для половины всех векторов $\vec{a}$, поэтому

$$\begin{aligned}\sigma(f) &= 2^k |W_g(\vec{0})| + \sum_{\vec{b} \neq \vec{0}} \sum_{\vec{a}: \tilde{\varphi}(\vec{a}, \vec{b}) = \langle \vec{a}, \vec{x_0} \rangle} (2^k + W_g(\vec{b}) + 2^k - W_g(\vec{b})) = \\ &= 2^k |W_g(\vec{0})| + (2^k - 1) 2^{2k} = 2^{3n/2} - 2^n + 2^{n/2} |W_g(\vec{0})|. \quad \square\end{aligned}$$

Функции f , рассмотренные в теореме 1, являются сбалансированными тогда и только тогда, когда $W_f(\vec{0}, \vec{0}) = 0$, что согласно равенству (4) равносильно условию $W_g(\vec{0}) = 0$, т. е. условию сбалансированности функции g .

Пусть $\vec{x_0} = (c_1, c_2, \dots, c_k)$, тогда из равенства

$$f(\vec{x}, \vec{y}) = (x_1 \oplus \bar{c}_1)(x_2 \oplus \bar{c}_2) \cdots (x_k \oplus \bar{c}_k)(g(\vec{y}) \oplus c) \oplus \varphi(\vec{x}, \vec{y})$$

и соотношения $\deg \varphi(\vec{x}, \vec{y}) \leq k$ (см., например, [1]) следует, что при условии $g(\vec{y}) \neq \text{const}$ для алгебраической степени функции f имеет место равенство

$$\deg f = \frac{n}{2} + \deg g.$$

Из доказательства теоремы 1 получаем

$$\max_{\vec{a}, \vec{b}} |W_f(\vec{a}, \vec{b})| = \max_{\vec{b}} |W_g(\vec{b})| + 2^k, \quad \text{nl}(f) = 2^{n-1} - 2^{n/2} + \text{nl}(g),$$

где $\text{nl}(f)$ — нелинейность функции f (расстояние Хэмминга от f до класса всех аффинных булевых функций от n переменных), которая вычисляется по формуле (см., например, [1])

$$\text{nl}(f) = 2^{n-1} - \frac{1}{2} \max_{\vec{a} \in \{0,1\}^n} |W_f(\vec{a})|.$$

Пусть $\varphi(\vec{x}, \vec{y}) = \langle \pi(\vec{x}), \vec{y} \rangle \oplus h(\vec{x})$ — бент-функция из класса Мэйорана – Мак-Фарланда, где π — подстановка на множестве $\{0, 1\}^k$, а h — произвольная булева функция от k переменных. Тогда если $\pi(\vec{x}_0) = \vec{0}$, то на многообразии $M = \{(\vec{x}_0, \vec{y}) : \vec{y} \in \{0, 1\}^k\}$ выполнено равенство $\varphi(\vec{x}, \vec{y}) = h(\vec{x}_0) = c$ и булева функция

$$f(\vec{x}, \vec{y}) = \begin{cases} g(\vec{y}), & \text{если } \vec{x} = \pi^{-1}(\vec{0}), \\ \langle \pi(\vec{x}), \vec{y} \rangle \oplus h(\vec{x}), & \text{если } \vec{x} \neq \pi^{-1}(\vec{0}), \end{cases}$$

удовлетворяет условиям теоремы 1. Число таких функций равно $2^{n/2!} \cdot 4^{2^{n/2}}$.

Теорема 1 показывает, что существует довольно широкий класс сбалансированных булевых функций f от n переменных алгебраической степени

$$\deg f \in \left\{ \frac{n}{2}, \frac{n}{2} + 1, \dots, n-1 \right\},$$

у которых $\sigma(f) \sim 2^{3n/2}$ при $n \rightarrow \infty$.

2. Мажоритарная функция

Пусть n — нечетное натуральное число. Обозначим через $\|\vec{a}\|$ вес вектора $\vec{a} \in \{0, 1\}^n$. Мажоритарная булева функция определяется равенствами

$$f(x_1, x_2, \dots, x_n) = \begin{cases} 0, & \text{если } \|(x_1, x_2, \dots, x_n)\| < \frac{n}{2}, \\ 1, & \text{если } \|(x_1, x_2, \dots, x_n)\| > \frac{n}{2}. \end{cases}$$

Она является сбалансированной симметрической пороговой функцией. Найдем для этой функции f сумму $\sigma(f) = \sigma(n)$ модулей ее коэффициентов Уолша – Адамара.

В [9] для коэффициентов $W_f(\vec{a})$ Уолша – Адамара функции f получены равенства

$$W_f(\vec{a}) = \begin{cases} 0, & \text{если } \|\vec{a}\| = k \text{ и } k \text{ четное,} \\ 2 \sum_{i=0}^{(n-1)/2} K_i(k, n), & \text{если } \|\vec{a}\| = k \text{ и } k \text{ нечетное,} \end{cases} \quad (5)$$

где

$$K_i(k, n) = \sum_{j=0}^i (-1)^j \binom{k}{j} \binom{n-k}{i-j}$$

— значение многочлена Кравчука $K_i(x, n)$ в точке $x = k$.

Как показано в [10, формулы (7.79), (7.86)], для всех нечетных чисел k

$$\sum_{i=0}^{(n-1)/2} K_i(k, n) = (-1)^{\frac{k-1}{2}} \frac{(k-1)! \frac{n-k}{2}!}{\frac{n-1}{2}! \frac{k-1}{2}!} \binom{n-k}{\frac{n-k}{2}}. \quad (6)$$

Следующая теорема описывает свойства величины $\sigma(n)$.

Теорема 2. Пусть f — мажоритарная булева функция от нечетного числа переменных. Тогда

1) справедлива формула

$$\sigma(n) = 2n \binom{n-1}{\frac{n-1}{2}} \sum_{i=0}^{\frac{n-1}{2}} \frac{1}{2i+1} \binom{\frac{n-1}{2}}{i},$$

2) имеет место рекуррентное соотношение

$$\sigma(n) = 4\sigma(n-2) + 2^{\frac{n+1}{2}} \binom{n-1}{\frac{n-1}{2}}, \quad n \geq 3,$$

3) при всех $n \geq 9$ верна оценка

$$\sigma(n) > \frac{n-2}{n-3} \binom{n-1}{\frac{n-1}{2}} 2^{(n+3)/2},$$

4) для всех n верна оценка

$$\sigma(n) < \frac{n+3}{n+1} \binom{n-1}{\frac{n-1}{2}} 2^{(n+3)/2},$$

5) при $n \rightarrow \infty$ имеет место соотношение

$$\sigma(n) \sim \frac{2}{\sqrt{\pi n}} 2^{3n/2}.$$

Доказательство. 1) С использованием формул (5) и (6) получим

$$\begin{aligned} \sigma(n) &= \sum_{\vec{a}: \|\vec{a}\|=k} |W_f(\vec{a})| = 2 \binom{n}{k} \frac{(k-1)! (n-k)!}{\frac{n-1}{2}! \frac{k-1}{2}! \frac{n-k}{2}!} = \\ &= 2n \binom{n-1}{\frac{n-1}{2}} \frac{1}{k} \binom{\frac{n-1}{2}}{\frac{k-1}{2}} = 2n \binom{n-1}{\frac{n-1}{2}} \sum_{i=0}^{\frac{n-1}{2}} \frac{1}{2i+1} \binom{\frac{n-1}{2}}{i}. \end{aligned}$$

2) Для каждого нечетного числа n рассмотрим величину

$$\varkappa(n) = \sum_{i=0}^{\frac{n-1}{2}} \frac{1}{2i+1} \binom{\frac{n-1}{2}}{i}.$$

Заметим, что

$$\varkappa(n) = \sum_{i=0}^{\frac{n-1}{2}} \binom{\frac{n-1}{2}}{i} \int_0^1 x^{2i} dx = \int_0^1 (1+x^2)^{(n-1)/2} dx.$$

Осуществив замену $x = \operatorname{tg} t$, получим

$$\varkappa(n) = \int_0^{\pi/4} \frac{1}{\cos^{n+1} t} dt.$$

Так как

$$\begin{aligned} & \int_0^{\pi/4} \frac{1}{\cos^{n+1} t} dt - \frac{n-1}{n} \int_0^{\pi/4} \frac{1}{\cos^{n-1} t} dt = \\ & = \int_0^{\pi/4} \frac{\cos^2 t + n \sin^2 t}{n \cos^{n+1} t} dt = \frac{\sin t}{n \cos^n t} \Big|_0^{\pi/4} = \frac{2^{(n-1)/2}}{n}, \end{aligned}$$

то справедливо равенство

$$\varkappa(n) - \frac{n-1}{n} \varkappa(n-2) = \frac{2^{(n-1)/2}}{n}. \quad (7)$$

Используя соотношение (7), находим, что

$$\begin{aligned} \sigma(n) &= 2n \binom{n-1}{\frac{n-1}{2}} \varkappa(n) = \\ &= 2(n-1) \binom{n-1}{\frac{n-1}{2}} \varkappa(n-2) + 2^{(n+1)/2} \binom{n-1}{\frac{n-1}{2}} = \\ &= 8(n-2) \binom{n-3}{\frac{n-3}{2}} \varkappa(n-2) + 2^{(n+1)/2} \binom{n-1}{\frac{n-1}{2}} = \\ &= 4\sigma(n-2) + 2^{(n+1)/2} \binom{n-1}{\frac{n-1}{2}}. \end{aligned}$$

3) Достаточно доказать, что при $n \geq 9$ верно неравенство

$$\kappa(n) > \frac{(n-2) 2^{(n+1)/2}}{(n-3)n}.$$

Воспользуемся методом математической индукции по параметру n . Несложно проверить, что $\kappa(9) = 4,2158\dots$, а правая часть доказываемого неравенства равна $4,148\dots$. Для доказательства индуктивного перехода, используя формулу (7), при $n = 9$ получим:

$$\begin{aligned} \kappa(n) &= \frac{n-1}{n} \kappa(n-2) + \frac{2^{(n-1)/2}}{n} > \\ &> \frac{(n-1)(n-4)2^{(n-1)/2}}{n(n-2)(n-5)} + \frac{2^{(n-1)/2}}{n} = \\ &= \frac{2^{(n-1)/2}}{n} \left(1 + \frac{(n-1)(n-4)}{(n-2)(n-5)} \right). \end{aligned}$$

Остается проверить, что

$$1 + \frac{(n-1)(n-4)}{(n-2)(n-5)} \geq \frac{2(n-2)}{n-3}.$$

Последнее неравенство выполнено при всех $n \geq 9$.

4) Доказываемая верхняя оценка вытекает из неравенства

$$\kappa(n) < \frac{(n+3) 2^{(n+1)/2}}{(n+1)n},$$

которое доказывается методом математической индукции аналогично п. 3.

5) Из пп. 3 и 4 следует, что при $n \rightarrow \infty$

$$\sigma(n) \sim 2^{(n+3)/2} \binom{n-1}{\frac{n-1}{2}}.$$

Остается заметить, что имеет место соотношение

$$\binom{n-1}{\frac{n-1}{2}} \sim \frac{2^n}{\sqrt{2\pi n}},$$

вытекающее из формулы Стирлинга. □

Отметим, что не удастся получить более простую формулу для величины $\sigma(n)$ по сравнению с формулой из п. 1 теоремы 2. Тем не менее имеется тесная связь величины $\sigma(n)$ со значениями так называемой гипергеометрической функции Гаусса $F(a, b, c, z)$ (см., например, [11]), определяемой для всех $a, b, c \in \mathbb{R}$ равенством

$$F(a, b, c, z) = \sum_{i=0}^{\infty} \frac{(a)_i (b)_i}{(c)_i i!} z^i,$$

где $(x)_i = x(x+1) \cdots (x+i-1)$, $i \in \mathbb{N}$, $(x)_0 = 1$. Несложно показать, что

$$\sigma(n) = 2n \binom{n-1}{\frac{n-1}{2}} F\left(\frac{1}{2}, -\frac{n-1}{2}, \frac{3}{2}, -1\right).$$

3. Функции, построенные с помощью операции сложения по модулю 2^n и выделения старшего бита

Пусть n — натуральное число, $R = \mathbb{Z}_{2^n} = \{0, 1, \dots, 2^n - 1\}$ — кольцо вычетов по модулю 2^n . Каждому элементу $c \in R$ однозначно сопоставляется вектор $\vec{c} = (c_{n-1}, c_{n-2}, \dots, c_0) \in \{0, 1\}^n$, состоящий из разрядов в двоичном представлении числа c :

$$c = c_0 + 2c_1 + 2^2c_2 + \dots + 2^{n-1}c_{n-1}. \quad (8)$$

Пусть отображение $\varkappa_{n-1}: R \rightarrow \{0, 1\}$ действует по правилу

$$\varkappa_{n-1}(c) = c_{n-1}, \quad c \in R, \quad (9)$$

где c_{n-1} — старший бит из равенства (8). Зададим отображение $\varphi_c: R \rightarrow \{0, 1\}$ равенством

$$\varphi_c(x) = \varkappa_{n-1}(x+c), \quad x \in R,$$

где операция сложения рассматривается как операция сложения в кольце R , т. е. осуществляется по модулю 2^n . Заметим, что при $c \leq 2^{n-1}$

$$(\varphi_c(0), \varphi_c(1), \dots, \varphi_c(2^n - 1)) = (\underbrace{0, 0, \dots, 0}_{2^{n-1}-c}, \underbrace{1, 1, \dots, 1}_{2^{n-1}}, \underbrace{0, 0, \dots, 0}_c),$$

а при $c > 2^{n-1}$

$$(\varphi_c(0), \varphi_c(1), \dots, \varphi_c(2^n - 1)) = (\underbrace{1, 1, \dots, 1}_{2^{n-c}}, \underbrace{0, 0, \dots, 0}_{2^{n-1}}, \underbrace{1, 1, \dots, 1}_{c-2^{n-1}}).$$

Сопоставим отображению φ_c , $c \in R$, булеву функцию $f_c: \{0, 1\}^n \rightarrow \{0, 1\}$ по следующему правилу:

$$f_c(\vec{x}) = f_c(x_{n-1}, x_{n-2}, \dots, x_0) = \varphi_c(x) = \kappa_{n-1}(x+c), \quad (10)$$

где $x = x_0 + 2x_1 + 2^2x_2 + \dots + 2^{n-1}x_{n-1}$, $\vec{x} = (x_{n-1}, x_{n-2}, \dots, x_0)$. В частности, $f_0(\vec{x}) = x_{n-1}$, $f_{2^{n-1}}(\vec{x}) = \bar{x}_{n-1}$. Семейство булевых функций $f_c(\vec{x})$, $c \in R$, состоит из всех сбалансированных булевых функций, у которых в табличном задании (при лексикографическом расположении векторов $\vec{x}$) столбец значений получается из столбца значений функции $f_0(\vec{x})$ циклическим сдвигом.

Нам понадобится результат из [12], содержащий формулу для старшего бита при сложении целых чисел. Пусть $R = \mathbb{Z}_{2^n}$, $a, b \in R$, $\vec{a} = (a_{n-1}, \dots, a_0)$, $\vec{b} = (b_{n-1}, \dots, b_0)$. Введем обозначение

$$a^{[b]} = a_0^{b_0} \cdot a_1^{b_1} \cdots a_{n-1}^{b_{n-1}},$$

где используются соглашения $0^0 = 1$, $0^1 = 0$, $1^0 = 1$, $1^1 = 1$.

Лемма 1 ([12]). Для всех $n \in \mathbb{N}$, $c \in R$ верно сравнение

$$\kappa_{n-1}(x+c) \equiv \sum_{N=0}^{2^{n-1}} x^{[N]} c^{[2^{n-1}-N]} \pmod{2}. \quad (11)$$

Обозначим через $\|\vec{c}\|$ вес вектора $\vec{c}$.

Лемма 2. Пусть $n \in \mathbb{N}$, $n \geq 2$ и булева функция $f_c(\vec{x})$ определена равенством (10). Тогда при всех $c \in R$ функция $f_c(\vec{x})$ линейна по переменной x_{n-1} .

Доказательство. Согласно равенствам (10) и (11) многочлен Жегалкина функции $f_c(\vec{x})$ содержит слагаемое $x^{[2^{n-1}]}c^{[0]} = x_{n-1}$, кроме того, $x^{[N]} = x_0^{N_0} \cdots x_{n-2}^{N_{n-2}}$ при $N < 2^{n-1}$, т.е. переменная x_{n-1} не входит в другие слагаемые многочлена Жегалкина. Значит, $f_c(\vec{x})$ линейна по x_{n-1} . $\square$

Рассмотрим коэффициенты Уолша–Адамара булевых функций $f(\vec{x}) = f_c(\vec{x})$. Пусть $\vec{c} = (c_{n-1}, \dots, c_1, c_0)$, $c' = c - 2^{n-1}c_{n-1} = c_0 + 2c_1 + \dots + 2^{n-2}c_{n-2}$. Введем следующие обозначения: $\vec{x} = (x_{n-1}, \dots, x_1, x_0)$, $\vec{x}' = (x_{n-2}, \dots, x_1, x_0)$, $x' = x_0 + 2x_1 + \dots + 2^{n-2}x_{n-2}$ и определим булеву функцию $f_{c'}(\vec{x}')$ от $n-1$ переменных равенством

$$f_{c'}(\vec{x}') = \kappa_{n-2}(x' + c'). \quad (12)$$

Лемма 3. Если $n \geq 2$, то для всех $c \in R$

$$f_c(\vec{x}) = x_{n-1} \oplus x_{n-2} \oplus c_{n-1} \oplus c_{n-2} \oplus c_{n-2} f_{c'}(\vec{x}') \oplus x_{n-2} f_{c'}(\vec{x}') \oplus c_{n-2} x_{n-2}.$$

Доказательство. Рассматривая все возможные значения пар (c_{n-1}, c_{n-2}) , осуществляя сложение x и c в двоичном представлении столбиком и перебирая значения x_{n-2} , $\chi_{n-2}(x' + c')$, получим:

- 1) если $(c_{n-1}, c_{n-2}) = (0, 0)$, то $\chi_{n-1}(x+c) = x_{n-1} \oplus x_{n-2} \oplus x_{n-2} \chi_{n-2}(x'+c')$,
- 2) если $(c_{n-1}, c_{n-2}) = (0, 1)$, то $\chi_{n-1}(x+c) = x_{n-1} \oplus x_{n-2} \chi_{n-2}(x'+c') \oplus \chi_{n-2}(x'+c') \oplus 1$,
- 3) если $(c_{n-1}, c_{n-2}) = (1, 0)$, то $\chi_{n-1}(x+c) = x_{n-1} \oplus x_{n-2} \oplus x_{n-2} \chi_{n-2}(x'+c') \oplus 1$,
- 4) если $(c_{n-1}, c_{n-2}) = (1, 1)$, то $\chi_{n-1}(x+c) = x_{n-1} \oplus x_{n-2} \chi_{n-2}(x'+c') \oplus \chi_{n-2}(x'+c')$.

Остается воспользоваться равенствами (10) и (12). $\square$

Лемма 4. Если $n \geq 2$, то для коэффициентов Уолша – Адамара булевых функций $f(\vec{x}) = f_c(\vec{x})$ и $g(\vec{x}') = f_{c'}(\vec{x}')$ справедливы соотношения

$$W_f(a_{n-1}, \dots, a_1, a_0) = \begin{cases} 0, & \text{если } a_{n-1} = 0, \\ (-1)^{c_{n-1} \oplus c_{n-2}} (2^{n-1} + W_g(1, 0, \dots, 0)), & \text{если } \vec{a} = (1, 0, \dots, 0), \\ (-1)^{c_{n-1} \oplus c_{n-2}} W_g(1, a_{n-3}, \dots, a_0), & \text{если } \vec{a} = (1, 0, \underbrace{a_{n-3}, \dots, a_0}_{\neq \vec{0}}), \\ (-1)^{c_{n-1}} (2^{n-1} - W_g(1, 0, \dots, 0)), & \text{если } \vec{a} = (1, 1, 0, \dots, 0), \\ (-1)^{c_{n-1} \oplus 1} W_g(1, a_{n-3}, \dots, a_0), & \text{если } \vec{a} = (1, 1, \underbrace{a_{n-3}, \dots, a_0}_{\neq \vec{0}}). \end{cases}$$

Доказательство. Из леммы 2 следует, что функция f линейна по переменной x_{n-1} . Следовательно, $W_f(a_{n-1}, \dots, a_1, a_0) = 0$ при $a_{n-1} = 0$. Всюду далее рассматриваем векторы $\vec{a} = (1, a_{n-2}, \dots, a_1, a_0)$. Выделим два случая в соответствии со значением величины c_{n-2} .

Пусть $c_{n-2} = 0$. Тогда по лемме 3

$$f(\vec{x}) = x_{n-1} \oplus x_{n-2} \oplus c_{n-1} \oplus x_{n-2} g(\vec{x}'). \quad (13)$$

Из равенств (13) и $a_{n-1} = 1$ получим

$$W_f(\vec{a}) = 2(-1)^{c_{n-1}} \sum_{b_0, \dots, b_{n-2} \in \{0,1\}} (-1)^{b_{n-2} \oplus b_{n-2} g(b_{n-2}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-2} b_{n-2}}.$$

Рассматривая суммирование в соответствии со значением b_{n-2} , имеем

$$\begin{aligned} W_f(\vec{a}) = & 2(-1)^{c_{n-1}} \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}} + \\ & + 2(-1)^{c_{n-1} \oplus a_{n-2} \oplus 1} \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{g(1, b_{n-3}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}}. \end{aligned}$$

Значит,

$$\begin{aligned} W_f(\vec{a}) = & (-1)^{c_{n-1}} 2^{n-1} \delta_{a_0,0} \delta_{a_1,0} \dots \delta_{a_{n-3},0} + \\ & + 2(-1)^{c_{n-1} \oplus a_{n-2} \oplus 1} \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{g(1, b_{n-3}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}}, \end{aligned} \quad (14)$$

где $\delta_{a,0}$ — символ Кронекера:

$$\delta_{a,0} = \begin{cases} 1, & \text{если } a = 0, \\ 0, & \text{если } a = 1. \end{cases}$$

Из соотношений

$$\begin{aligned} W_g(1, a_{n-3}, \dots, a_1, a_0) = & \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{g(0, b_{n-3}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}} + \\ & + \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{g(1, b_{n-3}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3} \oplus 1} \end{aligned}$$

и равенства $1 \oplus g(1, b_{n-3}, \dots, b_0) = g(0, b_{n-3}, \dots, b_0)$ получим

$$W_g(1, a_{n-3}, \dots, a_0) = -2 \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{g(1, b_{n-3}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}}. \quad (15)$$

Таким образом, из равенств (14) и (15) следует, что

$$W_f(\vec{a}) = (-1)^{c_{n-1}} 2^{n-1} \delta_{a_0,0} \dots \delta_{a_{n-3},0} + (-1)^{c_{n-1} \oplus a_{n-2}} W_g(1, a_{n-3}, \dots, a_0),$$

и при $c_{n-2} = 0$ формулы доказаны.

Пусть $c_{n-2} = 1$. Тогда по лемме 3

$$f(\vec{x}) = x_{n-1} \oplus c_{n-1} \oplus 1 \oplus \bar{x}_{n-2} g(\vec{x}'). \quad (16)$$

Из равенств (16) и $a_{n-1} = 1$ получим

$$\begin{aligned} W_f(\vec{a}) = & 2(-1)^{c_{n-1} \oplus 1} \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{g(0, b_{n-3}, \dots, b_0) \oplus a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}} + \\ & + 2(-1)^{c_{n-1} \oplus a_{n-2} \oplus 1} \sum_{b_0, \dots, b_{n-3} \in \{0,1\}} (-1)^{a_0 b_0 \oplus \dots \oplus a_{n-3} b_{n-3}}. \end{aligned}$$

Тогда в силу формулы (15)

$$W_f(\vec{a}) = (-1)^{c_{n-1} \oplus 1} W_g(1, a_{n-3}, \dots, a_0) + (-1)^{c_{n-1} \oplus a_{n-2} \oplus 1} 2^{n-1} \delta_{a_0, 0} \dots \delta_{a_{n-3}, 0},$$

и при $c_{n-2} = 1$ формулы доказаны. $\square$

Лемма 5. При всех $n \geq 2$, $c \in R$ для булевой функции $f = f_c(x_{n-1}, \dots, x_0)$ верны равенства

$$\begin{aligned} W_f(1, 0, \dots, 0) &= \begin{cases} 2^n - 4c, & \text{если } 0 \leq c \leq 2^{n-1} - 1, \\ 4c - 3 \cdot 2^n, & \text{если } 2^{n-1} \leq c \leq 2^n - 1, \end{cases} \\ W_f(1, 1, 0, \dots, 0) &= \begin{cases} 4c, & \text{если } 0 \leq c \leq 2^{n-2} - 1, \\ 2^{n+1} - 4c, & \text{если } 2^{n-2} \leq c \leq 2^{n-1} + 2^{n-2} - 1, \\ 4c - 2^{n+2}, & \text{если } 2^{n-1} + 2^{n-2} \leq c \leq 2^n - 1. \end{cases} \end{aligned}$$

Доказательство. Методом математической индукции по параметру $n = 2, 3, \dots$ докажем, что

$$W_f(1, 0, \dots, 0) = (-1)^{c_{n-1}} \left(2 + \sum_{i=1}^{n-1} (-1)^{c_{i-1}} 2^i \right). \quad (17)$$

Пусть $n = 2$, $c = c_0 + 2c_1$, $c_0, c_1 \in \{0, 1\}$. Согласно равенству (11)

$$f_c(x_1, x_0) = x^{[0]} c^{[2]} \oplus x^{[1]} c^{[1]} \oplus x^{[2]} c^{[0]} = c_1 \oplus x_0 c_0 \oplus x_1.$$

Тогда

$$W_f(1, 0) = \sum_{b_0, b_1 \in \{0,1\}} (-1)^{b_1 \oplus b_0 c_0 \oplus c_1 \oplus b_1} = 4(-1)^{c_1} \delta_{c_0, 0} = 2(-1)^{c_1} + 2(-1)^{c_1 \oplus c_0},$$

и равенство (17) при $n = 2$ выполнено.

Допустим, что формула (17) верна при некотором числе $n - 1$. Используя лемму 4 и предположение индукции, получим

$$\begin{aligned} W_f(1, 0, \dots, 0) &= (-1)^{c_{n-1} \oplus c_{n-2}} 2^{n-1} + (-1)^{c_{n-1} \oplus c_{n-2}} W_g(1, 0, \dots, 0) = \\ &= (-1)^{c_{n-1} \oplus c_{n-2}} 2^{n-1} + (-1)^{c_{n-1}} \left(2 + \sum_{i=1}^{n-2} (-1)^{c_{i-1}} 2^i \right) = \\ &= (-1)^{c_{n-1}} \left(2 + \sum_{i=1}^{n-1} (-1)^{c_{i-1}} 2^i \right). \end{aligned}$$

Формула (17) доказана. Из равенства $(-1)^x = 1 - 2x$, $x \in \{0, 1\}$, и формулы (17) следует, что при $c_{n-1} = 0$

$$W_f(1, 0, \dots, 0) = 2 + \sum_{i=1}^{n-1} 2^i (1 - 2c_{i-1}) = 2^n - 4c.$$

Если $c_{n-1} = 1$, то

$$W_f(1, 0, \dots, 0) = -2 - \sum_{i=1}^{n-1} 2^i (1 - 2c_{i-1}) = -(2^n - 4(c - 2^{n-1})) = 4c - 3 \cdot 2^n.$$

Рассмотрим коэффициент Уолша–Адамара $W_f(1, 1, 0, \dots, 0)$. Согласно лемме 4

$$W_f(1, 1, 0, \dots, 0) = (-1)^{c_{n-1}} 2^{n-1} + (-1)^{c_{n-1} \oplus 1} W_g(1, 0, \dots, 0).$$

По доказанному выше для $c' = c - 2^{n-1}c_{n-1} \leq 2^{n-2} - 1$ получаем

$$\begin{aligned} W_f(1, 1, 0, \dots, 0) &= (-1)^{c_{n-1}} 2^{n-1} + (-1)^{c_{n-1} \oplus 1} (2^{n-1} - 4c') = 4c' (1 - 2c_{n-1}) = \\ &= \begin{cases} 4c, & \text{если } 0 \leq c \leq 2^{n-2} - 1, \\ 2^{n+1} - 4c, & \text{если } 2^{n-1} \leq c \leq 2^{n-1} + 2^{n-2} - 1. \end{cases} \end{aligned}$$

Если $c' = c - 2^{n-1}c_{n-1} \geq 2^{n-2}$, то

$$\begin{aligned} W_f(1, 1, 0, \dots, 0) &= (-1)^{c_{n-1}} 2^{n-1} + (-1)^{c_{n-1} \oplus 1} (4c' - 3 \cdot 2^{n-1}) = \\ &= (2^{n+1} - 4c') (1 - 2c_{n-1}) = \\ &= \begin{cases} 2^{n+1} - 4c, & \text{если } 2^{n-2} \leq c \leq 2^{n-1} - 1, \\ 4c - 2^{n+2}, & \text{если } 2^{n-1} + 2^{n-2} \leq c \leq 2^n - 1. \end{cases} \quad \square \end{aligned}$$

Рассмотрим функции $f = f_c(\vec{x})$, $c = 0, 1, \dots, 2^n - 1$, определенные равенством (10).

Введем обозначения: $\vec{c} = (c_{n-1}, \dots, c_0)$, $c(i) = c_0 + 2c_1 + \dots + 2^{i+1}c_{i+1}$, $i = 0, 1, \dots, n-2$. Вычислим величину $\sigma(f)$.

Лемма 6. При $n \geq 2$ справедливо равенство

$$\sigma(f_c) = (n-1)2^n - \sum_{i=1}^{n-2} 2^i |W_{f_{c(n-2-i)}}(\underbrace{1, 0, \dots, 0}_{n-i})|.$$

Доказательство. Если $n = 2$, то согласно формуле (11) имеем

$$f_c(x_1, x_0) = x_1 \oplus x_0 c_0 \oplus c_1, \quad \sigma(f_c) = 4.$$

Таким образом, равенство верно. Допустим, что оно верно при некотором $n-1$. Докажем, что тогда оно верно и при n . Пусть

$$g = g(x_{n-2}, \dots, x_0) = \kappa_{n-2}(x(n-3) + c(n-3)),$$

где $x(n-3) = x_0 + 2x_1 + \dots + 2^{n-2}x_{n-2}$. Используя лемму 4 и неравенство $|W_g(\vec{b})| \leq 2^{n-2}$, $\vec{b} \in \{0, 1\}^{n-1}$, получим

$$\begin{aligned} \sigma(f) &= 2^{n-1} + W_g(1, 0, \dots, 0) + 2^{n-1} - W_g(1, 0, \dots, 0) + \\ &+ 2 \sum_{\mathcal{A}_n} |W_g(1, a_{n-3}, \dots, a_0)| = 2^n + 2\sigma(g) - 2|W_g(1, 0, \dots, 0)|. \end{aligned}$$

где $\mathcal{A}_n = \{(a_{n-3}, a_{n-2}, \dots, a_0) \in \{0, 1\}^{n-2} \setminus \{\vec{0}\}\}$. В силу предположения индукции

$$\begin{aligned} \sigma(f) &= 2^n - 2|W_g(1, 0, \dots, 0)| + \\ &+ 2 \left((n-2)2^{n-1} - \sum_{i=1}^{n-3} 2^i |W_{f_{c(n-3-i)}}(\underbrace{1, 0, \dots, 0}_{n-1-i})| \right) = \\ &= (n-1)2^n - \sum_{i=1}^{n-2} 2^i |W_{f_{c(n-2-i)}}(\underbrace{1, 0, \dots, 0}_{n-i})|. \quad \square \end{aligned}$$

Теорема 3. Пусть $n \geq 3$, $\vec{c} = (c_{n-1}, c_{n-2}, \dots, c_0)$, $\|(c_{n-3}, c_{n-2}, \dots, c_0)\| = t$, $0 \leq l_1 < l_2 < \dots < l_t \leq n-3$ и $c_{l_1} = c_{l_2} = \dots = c_{l_t} = 1$. Тогда

$$\sigma(f_c) = 2^n + 2^{n+1}t - 8(2^{l_1} + 2^{l_2} + \dots + 2^{l_t}) - 2^{n+1} \sum_{1 \leq i < j \leq t} 2^{l_i - l_j}.$$

Доказательство. Из лемм 5 и 6 следует, что

$$\sigma(f) = (n-1)2^n - \sum_{j=0}^{n-3} 2^{n-2-j} |W_{f_{c(j)}}(\underbrace{1, 0, \dots, 0}_{j+2})|,$$

где

$$W_{f_{c(j)}}(1, 0, \dots, 0) = \begin{cases} 2^{j+2} - 4c(j), & \text{если } 0 \leq c(j) \leq 2^{j+1} - 1, \\ 4c(j) - 3 \cdot 2^{j+2}, & \text{если } 2^{j+1} \leq c(j) \leq 2^{j+2} - 1. \end{cases}$$

Тогда

$$\begin{aligned} & |2^{n-2-j} W_{f_{c(j)}}(1, 0, \dots, 0)| = \\ & = \begin{cases} 2^n - 2^{n-j}c(j), & \text{если } 0 \leq c(j) \leq 2^j - 1, \\ 2^{n-j}c(j) - 2^n, & \text{если } 2^j \leq c(j) \leq 2^{j+1} - 1, \\ 3 \cdot 2^n - 2^{n-j}c(j), & \text{если } 2^{j+1} \leq c(j) \leq 2^{j+1} + 2^j - 1, \\ 2^{n-j}c(j) - 3 \cdot 2^n, & \text{если } 2^{j+1} + 2^j \leq c(j) \leq 2^{j+2} - 1, \end{cases} \end{aligned}$$

а значит,

$$\begin{aligned} & |2^{n-2-j} W_{f_{c(j)}}(1, 0, \dots, 0)| = \\ & = (-1)^{c_j} (2^n - 2^{n-j}(c(j) - 2^{j+1}c_{j+1})) = (-1)^{c_j} (2^n - 2^{n-j}r(j)), \end{aligned} \quad (18)$$

где $r(j) = c_0 + 2c_1 + \dots + 2^j c_j$. Поэтому

$$\begin{aligned} \sigma(f) &= (n-1)2^n - 2^n \sum_{j=0}^{n-3} (-1)^{c_j} + \sum_{j=0}^{n-3} (-1)^{c_j} 2^{n-j} r(j) = \\ &= (n-1)2^n - 2^n \sum_{j=0}^{n-3} (1 - 2c_j) + \sum_{j=0}^{n-3} (1 - 2c_j) 2^{n-j} r(j). \end{aligned}$$

Следовательно,

$$\sigma(f) = 2^n + 2^{n+1} \sum_{j=0}^{n-3} c_j + S_1 - 2S_2, \quad (19)$$

где

$$S_1 = \sum_{j=0}^{n-3} 2^{n-j} r(j), \quad S_2 = \sum_{j=0}^{n-3} c_j 2^{n-j} r(j).$$

Для величины S_1 справедливо равенство

$$\begin{aligned} S_1 &= \sum_{j=0}^{n-3} 2^{n-j} \sum_{s=0}^j c_s 2^s = \\ &= \sum_{s=0}^{n-3} c_s \sum_{j=s}^{n-3} 2^{n+s-j} = \sum_{s=0}^{n-3} c_s (2^{n+1} - 2^{s+3}) = \\ &= 2^{n+1} (c_0 + c_1 + \dots + c_{n-3}) - 8r(n-3). \end{aligned}$$

Вычислим S_2 , используя значения $j = l_1, l_2, \dots, l_t$:

$$\begin{aligned} S_2 &= \sum_{s=1}^t 2^{n-l_s} (2^{l_1} + \dots + 2^{l_{s-1}} + 2^{l_s}) = \\ &= 2^n t + \sum_{1 \leq i < j \leq t} 2^{n-l_j+l_i}. \end{aligned}$$

Подставляя вычисленные значения S_1 и S_2 в формулу (19), получим:

$$\begin{aligned} \sigma(f) &= 2^n + 2^{n+1}t - 8(2^{l_1} + 2^{l_2} + \dots + 2^{l_t}) - \\ &\quad - 2^{n+1} \sum_{1 \leq i < j \leq t} 2^{l_i-l_j}. \end{aligned} \quad \square$$

Формула теоремы 3 не очень удобна для использования. Получим оценку сверху величины $\sigma(f_c)$. Для этого понадобится несколько вспомогательных результатов.

Лемма 7. Пусть $n \geq 3$, $\vec{c} = (0, 0, c_{n-3}, \dots, c_0) \in \{0, 1\}^n$, $d = 2^{n-2} - c$. Тогда

$$\sigma(f_c) = \sigma(f_d).$$

Доказательство. Из равенства (11) следует, что

$$f_0(\vec{x}) = x_{n-1}, \quad f_{2^{n-2}}(\vec{x}) = x_{n-1} \oplus x_{n-2} \quad \text{и} \quad \sigma(f_0) = \sigma(f_{2^{n-2}}) = 2^n.$$

Будем рассматривать теперь ненулевые векторы $\vec{c}$. Если $k \in \{0, 1, \dots, n-3\}$ выбрано так, что $c_k = 1$, $c_{k-1} = \dots = c_0 = 0$, то

$$\vec{d} = (0, 0, d_{n-3}, \dots, d_0) = (0, 0, \bar{c}_{n-3}, \bar{c}_{n-4}, \dots, \bar{c}_{k+1}, c_k, 0, 0, \dots, 0).$$

Пусть

$$r(j) = \sum_{i=0}^j c_i 2^i, \quad r'(j) = \sum_{i=0}^j d_i 2^i,$$

где $j = 0, 1, \dots, n-3$. Тогда

$$r'(j) = \begin{cases} r(j), & \text{если } j = 0, 1, \dots, k, \\ 2^{j+1} - r(j), & \text{если } j = k+1, k+2, \dots, n-3. \end{cases} \quad (20)$$

Из доказательства теоремы 3 следует, что

$$\begin{aligned} \sigma(f_c) &= (n-1) 2^n - \sum_{j=0}^{n-3} (-1)^{c_j} (2^n - 2^{n-j} r(j)) = \\ &= (n-1) 2^n - k 2^n - \sum_{j=k+1}^{n-3} (-1)^{c_j} (2^n - 2^{n-j} r(j)). \end{aligned}$$

Для величины $\sigma(f_d)$ согласно (20) имеем

$$\begin{aligned} \sigma(f_d) &= (n-1) 2^n - k 2^n - \sum_{j=k+1}^{n-3} (-1)^{\bar{c}_j} (2^n - 2^{n-j} r'(j)) = \\ &= (n-1) 2^n - k 2^n - \sum_{j=k+1}^{n-3} (-1)^{\bar{c}_j} (2^{n-j} r(j) - 2^n) = \\ &= (n-1) 2^n - k 2^n - \sum_{j=k+1}^{n-3} (-1)^{c_j} (2^n - 2^{n-j} r(j)) = \\ &= \sigma(f_c). \end{aligned} \quad \square$$

Лемма 8. Если $n \geq 2$,

$$a = \frac{2^{n-2} + (-1)^{n-1}}{3},$$

то

$$\sigma(f_a) = \frac{2^n (6n-1) + 8(-1)^{n-1}}{9}.$$

Доказательство. Заметим, что

$$\vec{a} = \begin{cases} (0, 0, 0, 1, 0, 1, \dots, 0, 1), & \text{если } n \text{ четное,} \\ (0, 0, 1, 0, 1, 0, \dots, 1, 0, 1), & \text{если } n \text{ нечетное.} \end{cases}$$

Пусть n – четное число. В обозначениях, использованных при доказательстве леммы 7, для всех $s = 0, 1, \dots, (n-4)/2$ получим $r(2s) = r(2s+1) = (4^{s+1} - 1)/3$, поэтому

$$\begin{aligned}\sigma(f_a) &= (n-1)2^n - \sum_{s=0}^{(n-4)/2} (-1)^{a_{2s}} (2^n - 2^{n-2s} r(2s)) - \\ &\quad - \sum_{s=0}^{(n-4)/2} (-1)^{a_{2s+1}} (2^n - 2^{n-2s-1} r(2s+1)) = \\ &= (n-1)2^n - \sum_{s=0}^{(n-4)/2} \left(-2^n + 2^{n-2s} \frac{4^{s+1} - 1}{3} \right) - \\ &\quad - \sum_{s=0}^{(n-4)/2} \left(2^n - 2^{n-2s-1} \frac{4^{s+1} - 1}{3} \right) = \\ &= (n-1)2^n - \frac{1}{3} \sum_{s=0}^{(n-4)/2} 2^{n-2s-1} (2^{2s+2} - 1) = \\ &= (n-1)2^n - \frac{2^{n+1}(n-2)}{6} + \frac{2^n}{3} \sum_{s=0}^{(n-4)/2} \frac{1}{2^{2s+1}} = \\ &= (n-1)2^n - \frac{2^n(n-2)}{3} + \frac{2^n \cdot 2}{9} \left(1 - \frac{4}{2^n} \right) = \\ &= \frac{2^n(6n-1) - 8}{9}.\end{aligned}$$

Аналогично доказывается, что при нечетном n

$$\sigma(f_a) = \frac{2^n(6n-1) + 8}{9}. \quad \square$$

Лемма 9. Если $n \geq 3$,

$$a = \frac{2^{n-2} + (-1)^{n-1}}{3},$$

то для всех $c \in \{0, 1, \dots, 2^{n-3}\}$

$$\sigma(f_a) - \sigma(f_c) \geq 8|c - a|. \quad (21)$$

Доказательство. Докажем неравенство методом математической индукции по параметру $n = 3, 4, \dots$. При $n = 3$ имеем $a = 1$, а согласно формуле (11) $f_0(x_2, x_1, x_0) = x_2$, $f_1(x_2, x_1, x_0) = x_2 \oplus x_1 x_0$, $\sigma(f_0) = 8$, $\sigma(f_1) = 16$, и неравенство (21) выполнено.

Допустим, что соотношение (21) выполнено для $n-1$. Докажем, что оно выполняется и для n . Если $c = a$, то неравенство очевидно. Рассмотрим случай, когда $c \neq a$. Из теоремы 3 следует, что если $c < 2^{n-2}$, $g_c(x_{n-2}, \dots, x_0) = \varkappa_{n-2}(x(n-3) + c)$, то

$$\sigma(f_c) = 2\sigma(g_c) + 8c. \quad (22)$$

Пусть $a' = (2^{n-3} + (-1)^{n-2})/3$, $c' \leq 2^{n-4}$. По предположению индукции

$$\sigma(g_{a'}) - \sigma(g_{c'}) \geq 8|c' - a'|. \quad (23)$$

Рассмотрим два случая.

1) Пусть $c < a$. Согласно (22)

$$\sigma(f_a) - \sigma(f_c) = 2(\sigma(g_a) - \sigma(g_c)) + 8(a - c). \quad (24)$$

По предположению индукции a' — единственное число, при котором величина $\sigma(g_{c'})$, $c' \in \{0, 1, \dots, 2^{n-4}\}$, принимает максимальное значение. Кроме того, $\sigma(g_{c'}) = \sigma(g_{2^{n-3}-c'})$ по лемме 7. Значит, максимальное значение величины $\sigma(g_c)$, $c \in \{0, 1, \dots, 2^{n-3}\}$, достигается только в точках $c = a'$ и $c = 2^{n-3} - a' = a$. Таким образом, из соотношения (24) следует, что

$$\sigma(f_a) - \sigma(f_c) \geq 8(a - c).$$

2) Пусть $c > a$. Введем обозначение $\widehat{c} = 2^{n-3} - c$, тогда $\widehat{c} \leq 2^{n-4}$. Заметим, что согласно (22) и лемме 7

$$\sigma(f_c) = 2\sigma(g_c) + 8c, \quad \sigma(f_{\widehat{c}}) = 2\sigma(g_{\widehat{c}}) + 8\widehat{c} = 2\sigma(g_c) + 8\widehat{c},$$

а значит,

$$\sigma(f_c) = \sigma(f_{\widehat{c}}) + 8(c - \widehat{c}). \quad (25)$$

Используя (22) и (25), находим, что

$$\begin{aligned} \sigma(f_a) - \sigma(f_c) &= 2\sigma(g_a) + 8a - \sigma(f_{\widehat{c}}) + 8(\widehat{c} - c) = \\ &= 2\sigma(g_a) + 8a - (2\sigma(g_{\widehat{c}}) + 8\widehat{c}) + 8(\widehat{c} - c) = \\ &= 2(\sigma(g_a) - \sigma(g_{\widehat{c}})) + 8(a - c). \end{aligned}$$

Так как $\sigma(g_a) = \sigma(g_{a'})$, то

$$\sigma(f_a) - \sigma(f_c) = 2(\sigma(g_{a'}) - \sigma(g_{\widehat{c}})) + 8(a - c).$$

Учитывая неравенство (23), получим

$$\begin{aligned} \sigma(f_a) - \sigma(f_c) &\geq 16(a' - \widehat{c}) + 8(a - c) = \\ &= 16((2^{n-3} - a) - (2^{n-3} - c)) + 8(a - c) = 8(c - a). \quad \square \end{aligned}$$

Теорема 4. Пусть $n \geq 2$. Максимальное значение величин $\sigma(f_c)$, где $c \in R$, равно

$$\frac{2^n(6n-1) + 8(-1)^{n-1}}{9}.$$

Оно достигается только при следующих значениях c :

$$c = 2^{n-1}\varepsilon_1 + 2^{n-2}\varepsilon_2 + \frac{2^{n-2} + (-1)^{n-1}}{3}, \quad c = 2^{n-1}\varepsilon_1 + 2^{n-2}\varepsilon_2 + \frac{2^{n-1} + (-1)^n}{3},$$

где $\varepsilon_1, \varepsilon_2$ — произвольные числа из множества $\{0, 1\}$.

Доказательство. При $n = 2$ согласно доказательству леммы 6 все функции f_c , $c \in R$, являются аффинными, поэтому $\sigma(f_c) = 4$ и теорема справедлива. Будем считать, что $n \geq 3$. Найдем c , при которых $\sigma(f_c)$ принимает максимальное значение. Согласно теореме 3 величина $\sigma(f_c)$ не зависит от значений c_{n-1}, c_{n-2} вектора $\vec{c} = (c_{n-1}, c_{n-2}, \dots, c_0)$, следовательно, достаточно рассмотреть случай, когда $c_{n-1} = c_{n-2} = 0$, т.е. $c < 2^{n-2}$. По лемме 7 для всех таких c выполнено соотношение $\sigma(f_c) = \sigma(f_{2^{n-2}-c})$. Пусть $a = (2^{n-2} + (-1)^{n-1})/3$. Так как $2^{n-2} - a = (2^{n-1} + (-1)^n)/3$, то достаточно доказать, что для всех таких c , что $c \leq 2^{n-3}$, выполнено неравенство $\sigma(f_c) \leq \sigma(f_a)$, которое обращается в равенство только при $c = a$. Это следует из леммы 9. Для завершения доказательства остается воспользоваться леммой 8. $\square$

Следствие 1. Если $n \geq 2$, то для всех $c \in R$ верно неравенство

$$\sigma(f_c) \leq \frac{n2^{n+1}}{3},$$

которое обращается в равенство только при $n = 3$.

Доказательство. При $n = 2$ неравенство выполнено. Остается заметить, что при $n \geq 3$

$$\frac{2^n(6n-1) + 8(-1)^{n-1}}{9} \leq \frac{n2^{n+1}}{3}$$

и неравенство обращается в равенство только при $n = 3$. $\square$

Из теоремы следует, что для рассматриваемых функций $f = f_c(\vec{x})$ при $n \rightarrow \infty$ верно соотношение $\sigma(f) = O(n2^n)$. Параметр $\sigma(f)$ для данного класса функций значительно меньше величины $2^{3n/2}$.

Список литературы

- [1] Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2012, 584 с.
- [2] Камловский О. В., “Количество появлений элементов в выходных последовательностях фильтрующих генераторов”, *Прикладная дискретная математика*, № 3(21) (2013), 11–25.
- [3] Камловский О. В., “Количество появлений векторов на циклах выходных последовательностей двоичных комбинирующих генераторов”, *Проблемы передачи информации*, **53**:1 (2017), 92–100.
- [4] Де Ла Крус Хименес Р. А., Камловский О. В., “Суммы модулей коэффициентов Уолша – Адамара булевых функций”, *Дискретная математика*, **27**:4 (2015), 49–66.
- [5] Dobbertin H., “Construction of bent functions and balanced Boolean functions with high nonlinearity”, *Lect. Notes Comput. Sci.*, **1008**, 1995, 61–74.
- [6] McFarland R. L., “A family of noncyclic difference sets”, *J. Comb. Theory. Ser. A.*, № 15 (1973), 1–10.
- [7] Carlet C., “A large class of cryptographic Boolean functions via a study of the Maiorana–McFarland construction”, *Lect. Notes Comput. Sci.*, **2442**, 2002, 549–564.
- [8] Canteaut A., Daum M., Dobbertin H., Leander G., “Finding nonnormal bent functions”, *Discrete Appl. Math.*, **154**: 2 (2006), 202–218.
- [9] Dalai D. K., Maitra S., Sarkar S., “Basic theory in construction of Boolean functions with maximum possible annihilator immunity”, *Designs, codes and cryptography*, **40**:1 (2006), 41–58.
- [10] Titsworth R. C., *Correlation properties of cyclic sequences*: Calif. Inst. Technol., 1962, 244 p.
- [11] Бейтмен Г., Эрдейи А., *Высшие трансцендентные функции. Гипергеометрическая функция. Функции Лежандра*, М.: Наука, 1973, 296 с.
- [12] Богонатов Р. В., “Ранг суммы двух рекуррент максимального периода над $\mathbb{Z}_{2^n}$ ”, *Обозрение прикл. и промышл. матем.*, **16**:6 (2009), 1027–1028.