Math-Net.Ru

Общероссийский математический портал

Р. А. Де Ла Крус Хименес, О. В. Камловский, Суммы модулей коэффициентов Уолша–Адамара булевых функций, *Дискрет. матем.*, 2015, том 27, выпуск 4, 49–66

DOI: <https://doi.org/10.4213/dm1347>

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: 3.95.254.165

26 апреля 2023 г., 16:45:37

Суммы модулей коэффициентов Уолша–Адамара булевых функций

© 2015 г. Р. А. Де Ла Крус Хименес*, О. В. Камловский**

В работе приводятся достижимые оценки снизу и сверху для сумм модулей коэффициентов Уолша–Адамара булевых функций от n переменных. Вычисляются средние значения рассматриваемых сумм в классе всех булевых функций от n переменных и его подклассе, состоящем из всех сбалансированных функций. Строятся классы сбалансированных нелинейных функций у которых суммы модулей коэффициентов Уолша–Адамара близки к соответствующим нижним и верхним оценкам

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

Введение

Пусть n — натуральное число, $f = f(x_1, x_2, \dots, x_n)$ — булева функция от n переменных. Обозначим через $F(n)$ множество всех булевых функций от n переменных. Для каждого вектора $\vec{a} = (a_1, a_2, \dots, a_n) \in \{0, 1\}^n$ коэффициент $W_f(\vec{a})$ Уолша–Адамара булевой функции f определяется равенством (см., например, [1; стр. 76])

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

Введем обозначение

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

В [2] величина $\sigma(f)$ была использована для вывода оценок частот появлений элементов на отрезках выходных последовательностей двоичного фильтрующего генератора с фильтрующей функцией f . Чем меньше значение $\sigma(f)$, тем более точные оценки рассматриваемых частот удастся получить.

В § 1 данной работы получены следующие оценки:

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

*Место работы: ООО «Центр сертификационных исследований»,
e-mail: reyniereuler123@gmail.com

**Место работы: ООО «Центр сертификационных исследований»,
e-mail: ov-kam@yandex.ru

справедливые для каждой $f \in F(n)$. 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.

Пусть $G(n)$ — множество всех сбалансированных булевых функций из множества $F(n)$, т. е. функций, принимающих значения 0 и 1 ровно на половине векторов из множества $\{0, 1\}^n$. В § 2 работы доказываются следующие утверждения:

$$M(n) = \sum_{f \in F(n)} \sigma(f) = 2^{2n} \binom{2^n}{2^{n-1}};$$

$$S(n) = \sum_{f \in G(n)} \sigma(f) = (2^n - 1)2^{n-1} \binom{2^{n-1}}{2^{n-2}}^2, \quad n \geq 2.$$

В частности, отсюда для средних значений следуют соотношения

$$\frac{M(n)}{|F(n)|} \sim \frac{S(n)}{|G(n)|} \sim \sqrt{\frac{2}{\pi}} 2^{\frac{3n}{2}}, \quad n \rightarrow \infty.$$

В § 3 приводятся классы булевых функций $f \in G(n)$ с максимально возможной алгебраической степенью $\deg f = n - 1$, у которых $\sigma(f) = O(2^n)$ и $\sigma(f) = O(2^{\frac{3n}{2}})$ при $n \rightarrow \infty$. В § 4 для некоторых классов функций $f \in G(n)$, построенных с использованием конструкции Мэйорана–Мак–Фарланда (см., например, [3], [4]) доказывается, что $\sigma(f) = 2^{\frac{3n}{2}-1}$, а для некоторых классов функций $f \in G(n)$, построенных с использованием конструкции Доббертина (см. [5]), что $\sigma(f) \sim 2^{\frac{3n}{2}}$ при $n \rightarrow \infty$.

1. Оценки величины $\sigma(f)$

Получим оценки для суммы $\sigma(f)$ модулей коэффициентов Уолша–Адамара булевой функции f .

Теорема 1. *При всех $n \in \mathbb{N}$ и $f \in F(n)$ имеют место соотношения*

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

Верхняя оценка достигается тогда и только тогда, когда f — бент-функция, а нижняя оценка обращается в равенство тогда и только тогда, когда f — аффинная функция.

Доказательство. Для коэффициентов Уолша–Адамара булевой функции справедливо равенство Парсеваля (см., например, [1; стр. 80]):

$$\sum_{\vec{a} \in \{0,1\}^n} |W_f(\vec{a})|^2 = 2^{2n}.$$

Согласно неравенству Коши–Буняковского (см., например, [6; стр. 115])

$$\sigma(f) = \sum_{\vec{a} \in \{0,1\}^n} |W_f(\vec{a})| \leq \left(\sum_{\vec{a} \in \{0,1\}^n} |W_f(\vec{a})|^2 \right)^{\frac{1}{2}} \cdot 2^{\frac{n}{2}}.$$

Воспользовавшись равенством Парсеваля, получим

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

Из равенства

$$(-1)^{f(x_1, \dots, x_n)} = \frac{1}{2^n} \sum_{\vec{a} \in \{0,1\}^n} W_f(\vec{a}) (-1)^{a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n}$$

и неравенства треугольника имеем

$$\sigma(f) \geq \left| \sum_{\vec{a} \in \{0,1\}^n} W_f(\vec{a}) \right| = |2^n (-1)^{f(0, \dots, 0)}| = 2^n.$$

Неравенство Коши–Буняковского обращается в равенство тогда и только тогда, когда все числа $|W_f(\vec{a})|$, $\vec{a} \in \{0,1\}^n$, одинаковы (см., например, [6; стр. 131]). Это согласно равенству Парсеваля означает, что $|W_f(\vec{a})| = 2^{\frac{n}{2}}$ для всех $\vec{a}$, т. е. f — бент-функция. Для всех аффинных булевых функций справедливо равенство $\sigma(f) = 2^n$. Пусть теперь f — произвольная булева функция и $\sigma(f) = 2^n$. Из определения коэффициента Уолша–Адамара следует, что

$$0 \leq |W_f(\vec{a})| \leq 2^n.$$

Если бы существовал такой набор $\vec{a} \in \{0,1\}^n$, что $0 < |W_f(\vec{a})| < 2^n$, то получили бы согласно равенству Парсеваля

$$1 = \frac{\sigma(f)}{2^n} = \sum_{\vec{a} \in \{0,1\}^n} \frac{|W_f(\vec{a})|}{2^n} > \sum_{\vec{a} \in \{0,1\}^n} \frac{|W_f(\vec{a})|^2}{2^{2n}} = 1.$$

Таким образом, среди чисел $|W_f(\vec{a})|$, $\vec{a} \in \{0,1\}^n$, имеются только нулевые и равные 2^n , т. е. f — аффинная булева функция.

Отметим, что нижняя оценка из теоремы 1 достижима при всех $n \in \mathbb{N}$, а верхняя оценка, только для четных чисел n .

2. Среднее значение величины $\sigma(f)$

В этом параграфе рассмотрим величину

$$M(n) = \sum_{f \in F(n)} \sigma(f).$$

Теорема 2. Для всех $n \in \mathbb{N}$ имеет место равенство

$$M(n) = 2^{2n} \binom{2^n}{2^{n-1}}.$$

Доказательство. При $n = 1$ доказываемое равенство очевидно. Рассмотрим случай когда $n \geq 2$. Справедливо равенство

$$M(n) = \sum_{\vec{a} \in \{0,1\}^n} \sum_{f \in F(n)} \left| \sum_{\vec{b} \in \{0,1\}^n} (-1)^{f(\vec{b}) \oplus a_1 b_1 \oplus \dots \oplus a_n b_n} \right|.$$

Заметим, что при каждом фиксированном $\vec{a} \in \{0,1\}^n$ если f пробегает все множество $F(n)$, то и булева функция $g(x_1, \dots, x_n) = f(x_1, \dots, x_n) \oplus a_1 x_1 \oplus \dots \oplus a_n x_n$ также пробегает все множество $F(n)$. Значит,

$$M(n) = \sum_{\vec{a} \in \{0,1\}^n} \sum_{f \in F(n)} \left| \sum_{\vec{b} \in \{0,1\}^n} (-1)^{g(\vec{b})} \right| = 2^n \sum_{g \in F(n)} \left| \sum_{\vec{b} \in \{0,1\}^n} (-1)^{g(\vec{b})} \right|.$$

Из равенства

$$\sum_{\vec{b} \in \{0,1\}^n} (-1)^{g(\vec{b})} = 2^n - 2\|g\|,$$

где $\|g\|$ — вес булевой функции g , имеем

$$M(n) = 2^{n+1} \sum_{g \in F(n)} |2^{n-1} - \|g\||.$$

Отсюда

$$M(n) = 2^{n+1} \sum_{g_1 \in F(n), \|g_1\| < 2^{n-1}} (2^{n-1} - \|g_1\|) + 2^{n+1} \sum_{g_2 \in F(n), \|g_2\| > 2^{n-1}} (\|g_2\| - 2^{n-1}).$$

Каждой булевой функции g_1 из первой суммы однозначно соответствует функция $g_2 = \bar{g}_1$ из второй суммы, поэтому

$$M(n) = 2^{n+1} \sum_{g_1 \in F(n), \|g_1\| < 2^{n-1}} (2^n - 2\|g_1\|) = M_1(n) - M_2(n), \quad (1)$$

где

$$M_1(n) = 2^{2n+1} |\{g_1 \in F(n) : \|g_1\| < 2^{n-1}\}|,$$

$$M_2(n) = 2^{n+2} \sum_{g_1 \in F(n), \|g_1\| < 2^{n-1}} \|g_1\|.$$

Вычислим $M_1(n)$. Имеем

$$M_1(n) = 2^{2n+1} \sum_{i=0}^{2^{n-1}-1} \binom{2^n}{i}.$$

Из равенств

$$\sum_{i=0}^{2^n} \binom{2^n}{i} = 2^{2^n}, \quad \binom{2^n}{i} = \binom{2^n}{2^n - i}, \quad i = 0, 1, \dots, 2^{n-1} - 1,$$

получим

$$M_1(n) = 2^{2n} \left(2^{2^n} - \binom{2^n}{2^{n-1}} \right). \quad (2)$$

Вычислим $M_2(n)$. Справедливо равенство

$$M_2(n) = 2^{n+2} \sum_{g_1 \in F(n), \|g_1\| < 2^{n-1}} \sum_{\vec{c} \in \{0,1\}^n} g_1(\vec{c}) = 2^{n+2} \sum_{\vec{c} \in \{0,1\}^n} D(\vec{c}), \quad (3)$$

где

$$D(\vec{c}) = \sum_{g_1 \in F(n), \|g_1\| < 2^{n-1}} g_1(\vec{c}).$$

Величина $D(\vec{c})$ равна числу булевых функций $g_1 \in F(n)$, имеющих вес $\|g_1\| < 2^{n-1}$ и принимающих значение 1 на векторе $\vec{c}$, поэтому

$$D(\vec{c}) = \sum_{i=0}^{2^{n-1}-2} \binom{2^n-1}{i}.$$

Из равенств

$$\sum_{i=0}^{2^n-1} \binom{2^n-1}{i} = 2^{2^n-1}, \quad \binom{2^n-1}{i} = \binom{2^n-1}{2^n-1-i}, \quad i = 0, 1, \dots, 2^{n-1}-1,$$

получим

$$D(\vec{c}) = \frac{1}{2} \left(2^{2^n-1} - 2 \binom{2^n-1}{2^{n-1}} \right).$$

Значит, согласно (3)

$$M_2(n) = 2^{2n+1} \left(2^{2^n-1} - 2 \binom{2^n-1}{2^{n-1}} \right). \quad (4)$$

Таким образом из равенств (1), (2), (4) и соотношения $\binom{2^n}{2^{n-1}} = 2 \binom{2^n-1}{2^{n-1}}$ получим

$$M(n) = 2^{2n+2} \binom{2^n-1}{2^{n-1}} - 2^{2n} \binom{2^n}{2^{n-1}} = 2^{2n} \binom{2^n}{2^{n-1}}.$$

Вычисление с использованием теоремы 2 величины $M(n)/|F(n)|$ является затруднительным ввиду больших значений соответствующих биномиальных коэффициентов. Приведем асимптотическую формулу.

Следствие 1. При $n \rightarrow \infty$ справедливы соотношения

$$\frac{M(n)}{|F(n)|} = \frac{\binom{2^n}{2^{n-1}}}{2^{2^n-2n}} \sim \sqrt{\frac{2}{\pi}} 2^{\frac{3n}{2}}.$$

Доказательство. Достаточно воспользоваться формулой Стирлинга

$$k! \sim \sqrt{2\pi k} \left(\frac{k}{e} \right)^k, \quad k \rightarrow \infty.$$

Обозначим через $F_i(n)$, $i = 1, 2, \dots, n$, множество всех булевых функций $f \in F(n)$, линейных по i -й переменной, т. е. функций вида

$$f(x_1, x_2, \dots, x_n) = x_i \oplus g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n), \quad x_1, \dots, x_n \in \{0, 1\}, \quad (5)$$

где g — произвольная булева функция из множества $F(n-1)$.

Следствие 2. При $n \rightarrow \infty$ справедливы соотношения

$$\frac{1}{|F_i(n)|} \sum_{f \in F_i(n)} \sigma(f) = \frac{\binom{2^{n-1}}{2^{n-2}}}{2^{2^{n-1}-2n+1}} \sim \sqrt{\frac{1}{\pi}} 2^{\frac{3n}{2}}.$$

Доказательство. Заметим, что коэффициенты Уолша–Адамара булевой функции f вида (5) удовлетворяют равенствам

$$W_f(\vec{a}) = W_f(a_1, a_2, \dots, a_n) = \begin{cases} 0, & \text{если } a_i = 0, \\ 2W_g(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n), & \text{если } a_i = 1. \end{cases}$$

Отсюда получим

$$\frac{1}{|F_i(n)|} \sum_{f \in F_i(n)} \sigma(f) = \frac{2M(n-1)}{|F(n-1)|}.$$

Остается воспользоваться теоремой 2 и формулой Стирлинга.

Пусть $G(n)$ — множество всех сбалансированных функций от n переменных. Рассмотрим величину

$$S(n) = \sum_{f \in G(n)} \sigma(f).$$

Теорема 3. Для всех $n \in \mathbb{N}$, $n \geq 2$ имеет место равенство

$$S(n) = (2^n - 1)2^{n-1} \binom{2^{n-1}}{2^{n-2}}^2.$$

Доказательство. При $n = 2$ равенство доказывается непосредственной проверкой. Рассмотрим случай когда $n \geq 3$. Справедливо равенство

$$S(n) = \sum_{\vec{a} \in \{0,1\}^n} \sum_{f \in G(n)} \left| \sum_{\vec{b} \in \{0,1\}^n} (-1)^{f(\vec{b}) \oplus a_1 b_1 \oplus \dots \oplus a_n b_n} \right|.$$

В силу сбалансированности функций f выполнено равенство $W_f(\vec{0}) = 0$, поэтому

$$S(n) = \sum_{\vec{a} \neq \vec{0}} \sum_{f \in G(n)} \left| \sum_{\vec{b} \in \{0,1\}^n} (-1)^{f(\vec{b}) \oplus a_1 b_1 \oplus \dots \oplus a_n b_n} \right|. \quad (6)$$

Для каждого вектора $\vec{a} \in \{0,1\}^n \setminus \{\vec{0}\}$ обозначим через $L(\vec{a})$ множество всех таких векторов $\vec{b} \in \{0,1\}^n$, что $a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_n b_n = 0$. Множество $L(\vec{a})$ образует

линейное пространство размерности $n - 1$ над полем из двух элементов и, в частности, $|L(\vec{a})| = 2^{n-1}$. Пусть $f_{\vec{a},0}$ — ограничение функции f на множество $L(\vec{a})$, а $f_{\vec{a},1}$ — ограничение функции f на множество $\{0,1\}^n \setminus L(\vec{a})$. Справедливы равенства

$$\begin{aligned} \sum_{\vec{b} \in \{0,1\}^n} (-1)^{f(\vec{b}) \oplus a_1 b_1 \oplus \dots \oplus a_n b_n} &= \sum_{\vec{b} \in L(\vec{a})} (-1)^{f(\vec{b})} - \sum_{\vec{b} \in \{0,1\}^n \setminus L(\vec{a})} (-1)^{f(\vec{b})} = \\ &= |\{\vec{b} \in L(\vec{a}) : f(\vec{b}) = 0\}| - |\{\vec{b} \in L(\vec{a}) : f(\vec{b}) = 1\}| - \\ &- |\{\vec{b} \in \{0,1\}^n \setminus L(\vec{a}) : f(\vec{b}) = 0\}| + |\{\vec{b} \in \{0,1\}^n \setminus L(\vec{a}) : f(\vec{b}) = 1\}| = \\ &= (2^{n-1} - \|f_{\vec{a},0}\|) - \|f_{\vec{a},0}\| - (2^{n-1} - \|f_{\vec{a},1}\|) + \|f_{\vec{a},1}\| = \\ &= 2\|f_{\vec{a},1}\| - 2\|f_{\vec{a},0}\| = 2(2^{n-1} - \|f_{\vec{a},0}\|) - 2\|f_{\vec{a},0}\| = 2^n - 4\|f_{\vec{a},0}\|. \end{aligned}$$

Из равенства (6) имеем

$$S(n) = \sum_{\vec{a} \neq \vec{0}} \sum_{f \in G(n)} |2^n - 4\|f_{\vec{a},0}\|| = \sum_{\vec{a} \neq \vec{0}} (S_1(\vec{a}) + S_2(\vec{a})), \quad (7)$$

где

$$\begin{aligned} S_1(\vec{a}) &= \sum_{f \in G(n), \|f_{\vec{a},0}\| < 2^{n-2}} (2^n - 4\|f_{\vec{a},0}\|), \\ S_2(\vec{a}) &= \sum_{f \in G(n), \|f_{\vec{a},0}\| > 2^{n-2}} (4\|f_{\vec{a},0}\| - 2^n). \end{aligned}$$

Каждой булевой функции f из суммы $S_1(\vec{a})$ однозначно соответствует функция $g = \bar{f}$ из суммы $S_2(\vec{a})$, поэтому

$$S_1(\vec{a}) + S_2(\vec{a}) = \sum_{\substack{f \in G(n), \\ \|f_{\vec{a},0}\| < 2^{n-2}}} (4\|\bar{f}_{\vec{a},0}\| - 4\|f_{\vec{a},0}\|) = 4 \sum_{\substack{f \in G(n), \\ \|f_{\vec{a},0}\| < 2^{n-2}}} (2^{n-1} - 2\|f_{\vec{a},0}\|).$$

Согласно равенству (7) имеем

$$S(n) = 4 \sum_{\vec{a} \neq \vec{0}} (2^{n-1} R_1(\vec{a}) - 2 R_2(\vec{a})), \quad (8)$$

где

$$R_1(\vec{a}) = |\{f \in G(n) : \|f_{\vec{a},0}\| < 2^{n-2}\}|, \quad R_2(\vec{a}) = \sum_{f \in G(n), \|f_{\vec{a},0}\| < 2^{n-2}} \|f_{\vec{a},0}\|.$$

Вычислим $R_1(\vec{a})$. Справедливо равенство

$$R_1(\vec{a}) = \sum_{i=0}^{2^{n-2}-1} \binom{2^{n-1}}{i} \binom{2^{n-1}}{2^{n-1}-i}, \quad (9)$$

где $\binom{2^{n-1}}{i}$ — число способов выбрать i единичных значений функции f на множестве $L(\vec{a})$, а $\binom{2^{n-1}}{2^{n-1}-i}$ — число способов задания оставшихся единичных значений

функции f на множестве $\{0, 1\}^n \setminus L(\vec{a})$. Используя соотношение Вандермонда (см., например, [7; стр. 18])

$$\binom{k+m}{t} = \sum_{i=0}^t \binom{k}{i} \binom{m}{t-i}, \quad (10)$$

справедливое для всех $k, m, t \in \mathbb{N}$, имеем

$$\sum_{i=0}^{2^{n-1}} \binom{2^{n-1}}{i} \binom{2^{n-1}}{2^{n-1}-i} = \binom{2^n}{2^{n-1}}.$$

Отсюда с использованием равенства

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

получаем

$$R_1(\vec{a}) = \frac{1}{2} \binom{2^n}{2^{n-1}} - \frac{1}{2} \binom{2^{n-1}}{2^{n-2}}. \quad (11)$$

Вычислим $R_2(\vec{a})$. Справедливы равенства

$$R_2(\vec{a}) = \sum_{f \in G(n), \|f_{\vec{a},0}\| < 2^{n-2}} \sum_{\vec{c} \in L(\vec{a})} f(\vec{c}) = \sum_{\vec{c} \in L(\vec{a})} T(\vec{c}, \vec{a}), \quad (12)$$

где

$$T(\vec{c}, \vec{a}) = \sum_{f \in G(n), \|f_{\vec{a},0}\| < 2^{n-2}} f(\vec{c}).$$

Найдем $T(\vec{c}, \vec{a})$. Величина $T(\vec{c}, \vec{a})$ равна числу таких булевых функций $f \in G(n)$, что $\|f_{\vec{a},0}\| < 2^{n-2}$ и $f(\vec{c}) = 1$. Значит,

$$T(\vec{c}, \vec{a}) = \sum_{i=0}^{2^{n-2}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}}{2^{n-1}-i-1}, \quad (13)$$

где $\binom{2^{n-1}-1}{i}$ — число способов выбрать единичные значения функции f на множестве $L(\vec{a}) \setminus \{\vec{c}\}$, а $\binom{2^{n-1}}{2^{n-1}-i-1}$ — число способов задания оставшихся единичных значений функции f на множестве $\{0, 1\}^n \setminus L(\vec{a})$. Используя равенство

$$\binom{2^{n-1}}{2^{n-1}-i-1} = \binom{2^{n-1}-1}{2^{n-1}-i-1} + \binom{2^{n-1}-1}{2^{n-1}-i-2}, \quad i = 0, 1, \dots, 2^{n-1}-2,$$

и формулу (13), получим

$$T(\vec{c}, \vec{a}) = T_1(\vec{c}, \vec{a}) + T_2(\vec{c}, \vec{a}), \quad (14)$$

где

$$T_1(\vec{c}, \vec{a}) = \sum_{i=0}^{2^{n-2}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-1},$$

$$T_2(\vec{c}, \vec{a}) = \sum_{i=0}^{2^{n-2}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-2}.$$

Вычислим $T_1(\vec{c}, \vec{a})$. Согласно тождеству (10)

$$\sum_{i=0}^{2^{n-1}-1} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-1} = \binom{2^n-2}{2^{n-1}-1}.$$

Тогда из равенства

$$\sum_{i=0}^{2^{n-2}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-1} = \sum_{i=2^{n-2}+1}^{2^{n-1}-1} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-1}$$

имеем

$$T_1(\vec{c}, \vec{a}) = \frac{1}{2} \binom{2^n-2}{2^{n-1}-1} - \binom{2^{n-1}-1}{2^{n-2}}. \quad (15)$$

Вычислим $T_2(\vec{c}, \vec{a})$. Согласно тождеству (10)

$$\sum_{i=0}^{2^{n-1}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-2} = \binom{2^n-2}{2^{n-1}-2}.$$

Из равенства

$$\sum_{i=0}^{2^{n-2}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-2} = \sum_{i=2^{n-2}}^{2^{n-1}-2} \binom{2^{n-1}-1}{i} \binom{2^{n-1}-1}{2^{n-1}-i-2}$$

получим

$$T_2(\vec{c}, \vec{a}) = \frac{1}{2} \binom{2^n-2}{2^{n-1}-2} - \frac{1}{2} \binom{2^{n-1}-1}{2^{n-2}}. \quad (16)$$

Согласно равенствам (14), (15), (16) находим

$$T(\vec{c}, \vec{a}) = \frac{1}{2} \binom{2^n-1}{2^{n-1}-1} - \frac{3}{2} \binom{2^{n-1}-1}{2^{n-2}}.$$

Тогда из равенства (12) имеем

$$R_2(\vec{a}) = 2^{n-2} \binom{2^n-1}{2^{n-1}} - 3 \cdot 2^{n-2} \binom{2^{n-1}-1}{2^{n-2}}. \quad (17)$$

Подставляя значения для $R_1(\vec{a})$ и $R_2(\vec{a})$ из формул (11) и (17) в формулу (8), получаем

$$S(n) = (2^n-1)2^n \left(\binom{2^n}{2^{n-1}} - \binom{2^{n-1}}{2^{n-2}}^2 - 2 \binom{2^n-1}{2^{n-1}} + 6 \binom{2^{n-1}-1}{2^{n-2}}^2 \right).$$

Таким образом, используя равенства

$$\binom{2^n}{2^{n-1}} = 2 \binom{2^n - 1}{2^{n-1}}, \quad \binom{2^{n-1}}{2^{n-2}}^2 = 4 \binom{2^{n-1} - 1}{2^{n-2}}^2,$$

имеем

$$S(n) = (2^n - 1)2^{n+1} \binom{2^{n-1} - 1}{2^{n-2}}^2 = (2^n - 1)2^{n-1} \binom{2^{n-1}}{2^{n-2}}^2.$$

Следствие 3. При $n \rightarrow \infty$ справедливы соотношения

$$\frac{S(n)}{|G(n)|} = \frac{(2^n - 1)2^{n-1} \binom{2^{n-1}}{2^{n-2}}^2}{\binom{2^n}{2^{n-1}}} \sim \sqrt{\frac{2}{\pi}} 2^{\frac{3n}{2}}.$$

Доказательство. Достаточно воспользоваться формулой Стирлинга.

Приведем результаты вычислений с использованием ЭВМ средних значений

$$a_n = \frac{M(n)}{|F(n)|} = \frac{1}{|F(n)|} \sum_{f \in F(n)} \sigma(f),$$

$$b_n = \frac{S(n)}{|G(n)|} = \frac{1}{|G(n)|} \sum_{f \in G(n)} \sigma(f)$$

сумм $\sigma(f)$ модулей коэффициентов Уолша–Адамара в классе $F(n)$ всех булевых функций от n переменных и его подклассе $G(n)$ всех сбалансированных функций соответственно. Кроме того, приведем результаты вычислений величин

$$c_n = \sqrt{\frac{2}{\pi}} 2^{\frac{3n}{2}},$$

представляющих согласно следствиям 1 и 3 асимптотические приближения для рассматриваемых средних значений. Результаты представлены в следующих таблицах, где все величины выписаны с точностью до трех десятичных знаков после запятой.

n	1	2	3	4	5	6	7	8
a_n	2	6	17, 5	50, 273	143, 308	406, 924	1153, 205	3264, 945
b_n	2	4	14, 4	45, 687	136, 680	397, 449	1139, 735	3245, 845
c_n	2, 256	6, 383	18, 054	51, 064	144, 432	408, 516	1155, 460	3268, 135

n	9	10	11	12	13	14
a_n	9239, 169	26138, 698	73940, 430	209147, 884	591577, 603	1673259, 670
b_n	9212, 123	26100, 425	73886, 286	209071, 300	591469, 287	1673106, 483
c_n	9243, 682	26145, 081	73949, 457	209160, 650	591595, 657	1673285, 200

n	15	16	17	18
a_n	4732729, 146	13386230, 556	37862049, 816	107090150, 828
b_n	4732512, 502	13385924, 171	37861616, 520	107089538, 054
c_n	4732765, 254	13386281, 620	37862122, 033	107090252, 957

n	19	20	21	22
a_n	302896831, 828	856721819, 399	2423175521, 216	6853775780, 746
b_n	302895965, 234	856720593, 850	2423173788, 027	6853773329, 645
c_n	302896976, 260	856722023, 658	2423175810, 081	6853776189, 263

Таблицы показывают, что величины a_n и b_n достаточно близки к величинам c_n .

3. Классы сбалансированных функций с максимальной алгебраической степенью

В данном параграфе изучаются сбалансированные функции $f(x_1, x_2, \dots, x_n)$, у которых многочлен Жегалкина содержит единственное слагаемое $x_1 x_2 \dots x_{n-1}$ максимальной степени. Использование таких функций в качестве функций усложнения в фильтрующих генераторах позволяет гарантировать нетривиальные нижние оценки линейной сложности (ранга) их выходных последовательностей (см., например, [8; р. 86]).

Рассмотрим булеву функцию f , заданную многочленом Жегалкина следующего вида:

$$f(x_1, \dots, x_n) = x_1 x_2 \dots x_{n-1} \oplus x_{i_1} x_{i_2} \dots x_{i_t} \oplus x_n, \quad (18)$$

где натуральные числа $t, i_1, \dots, i_t$ удовлетворяют неравенствам $2 \leq t \leq n-2$, $1 \leq i_1 < i_2 < \dots < i_t \leq n-1$. Число таких функций равно

$$\sum_{t=2}^{n-2} \binom{n-1}{t} = 2^{n-1} - n - 1.$$

Каждая из них сбалансирована и имеет алгебраическую степень $\deg f = n-1$.

Теорема 4. Пусть булева функция f задана равенством (18). Тогда

$$\sigma(f) = 5 \cdot 2^n - 2^{n-t+2} - 2^{t+3} + 8.$$

Доказательство. Рассмотрим коэффициенты Уолша–Адамара функции f :

$$W_f(a_1, \dots, a_n) = \sum_{b_1, \dots, b_n \in \{0,1\}} (-1)^{b_1 b_2 \dots b_{n-1} \oplus b_{i_1} b_{i_2} \dots b_{i_t} \oplus b_n \oplus a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_n b_n}.$$

Если $a_n = 0$, то, очевидно, $W_f(a_1, \dots, a_n) = 0$. Если $a_n = 1$, то

$$W_f(a_1, \dots, a_n) = 2 \sum_{b_1, \dots, b_{n-1} \in \{0,1\}} (-1)^{b_1 b_2 \dots b_{n-1} \oplus b_{i_1} b_{i_2} \dots b_{i_t} \oplus a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_{n-1} b_{n-1}}.$$

Отсюда

$$W_f(a_1, \dots, a_n) = 2S + 4(-1)^{a_1 \oplus a_2 \oplus \dots \oplus a_{n-1}}, \quad (19)$$

где

$$S = \sum_{b_1, \dots, b_{n-1} \in \{0,1\}} (-1)^{b_{i_1} b_{i_2} \dots b_{i_t} \oplus a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_{n-1} b_{n-1}}.$$

Пусть числа $j_1, \dots, j_{n-1-t}$ выбраны так, что

$$\{j_1, \dots, j_{n-1-t}\} \cup \{i_1, \dots, i_t\} = \{1, \dots, n-1\}.$$

Тогда

$$S = \sum_{b_{i_1}, \dots, b_{i_t} \in \{0,1\}} (-1)^{b_{i_1} b_{i_2} \dots b_{i_t} \oplus a_{i_1} b_{i_1} \oplus \dots \oplus a_{i_t} b_{i_t}} \sum_{b_{j_1}, \dots, b_{j_{n-1-t}} \in \{0,1\}} (-1)^{a_{j_1} b_{j_1} \oplus \dots \oplus a_{j_{n-1-t}} b_{j_{n-1-t}}}. \quad (20)$$

Справедливы равенства

$$\begin{aligned} & \sum_{b_{j_1}, \dots, b_{j_{n-1-t}} \in \{0,1\}} (-1)^{a_{j_1} b_{j_1} \oplus \dots \oplus a_{j_{n-1-t}} b_{j_{n-1-t}}} = \\ & = \begin{cases} 2^{n-t-1}, & \text{если } (a_{j_1}, \dots, a_{j_{n-1-t}}) = (0, \dots, 0) \\ 0, & \text{если } (a_{j_1}, \dots, a_{j_{n-1-t}}) \neq (0, \dots, 0) \end{cases} = 2^{n-t-1} \delta_{a_{j_1}, 0} \dots \delta_{a_{j_{n-1-t}}, 0}, \end{aligned}$$

где $\delta_{i,j}$ — символ Кронекера, т. е. $\delta_{i,j} = 0$, если $i \neq j$ и $\delta_{i,j} = 1$, если $i = j$. С их использованием из равенства (20) будем иметь

$$\begin{aligned} S &= 2^{n-t-1} \delta_{a_{j_1}, 0} \dots \delta_{a_{j_{n-1-t}}, 0} \sum_{b_{i_1}, \dots, b_{i_t} \in \{0,1\}} (-1)^{b_{i_1} b_{i_2} \dots b_{i_t} \oplus a_{i_1} b_{i_1} \oplus \dots \oplus a_{i_t} b_{i_t}} = \\ &= 2^{n-t-1} \delta_{a_{j_1}, 0} \dots \delta_{a_{j_{n-1-t}}, 0} \left(\sum_{b_{i_1}, \dots, b_{i_t} \in \{0,1\}} (-1)^{a_{i_1} b_{i_1} \oplus \dots \oplus a_{i_t} b_{i_t}} + 2(-1)^{1 \oplus a_{i_1} \oplus \dots \oplus a_{i_t}} \right) = \\ &= 2^{n-1} \delta_{a_{i_1}, 0} \dots \delta_{a_{i_t}, 0} + 2^{n-t} (-1)^{1 \oplus a_{i_1} \oplus \dots \oplus a_{i_t}} \delta_{a_{j_1}, 0} \dots \delta_{a_{j_{n-1-t}}, 0}. \end{aligned}$$

Из равенства (19) при $a_n = 1$ получим

$$\begin{aligned} W_f(a_1, \dots, a_n) &= 2^n \delta_{a_1, 0} \dots \delta_{a_{n-1}, 0} + \\ &+ 2^{n-t+1} (-1)^{1 \oplus a_{i_1} \oplus \dots \oplus a_{i_t}} \delta_{a_{j_1}, 0} \dots \delta_{a_{j_{n-1-t}}, 0} + 4(-1)^{a_1 \oplus \dots \oplus a_{n-1}}. \end{aligned}$$

Таким образом, общий вид коэффициента Уолша–Адамара будет следующим:

а) если $a_n = 0$, то

$$W_f(a_1, \dots, a_n) = 0;$$

б) если $(a_1, \dots, a_{n-1}, a_n) = (0, \dots, 0, 1)$, то

$$W_f(a_1, \dots, a_n) = 2^n - 2^{n-t+1} + 4;$$

в) если $(a_1, \dots, a_{n-1}) \neq (0, \dots, 0)$, $a_n = 1$, то

$$W_f(a_1, \dots, a_n) = 2^{n-t+1} (-1)^{1 \oplus a_{i_1} \oplus \dots \oplus a_{i_t}} \delta_{a_{j_1}, 0} \dots \delta_{a_{j_{n-1-t}}, 0} + 4(-1)^{a_1 \oplus \dots \oplus a_{n-1}}.$$

Найдем сумму модулей всех спектральных коэффициентов. Представим ее следующим образом:

$$\sigma(f) = \sum_{\vec{a} \in \{0,1\}^n} |W_f(\vec{a})| = |W_f(0, \dots, 0, 1)| + \sum_{\vec{a} \in M_1} |W_f(\vec{a})| + \sum_{\vec{a} \in M_2} |W_f(\vec{a})|,$$

где M_1 — множество всех векторов $\vec{a} = (a_1, \dots, a_n)$, у которых $a_n = 1$ и $(a_{j_1}, \dots, a_{j_{n-t-1}}) = (0, \dots, 0)$, а M_2 — множество всех векторов $\vec{a} = (a_1, \dots, a_n)$, у которых $a_n = 1$ и $(a_{j_1}, \dots, a_{j_{n-t-1}}) \neq (0, \dots, 0)$. Из общего вида коэффициентов Уолша–Адамара, с использованием равенств $|M_1| = 2^t - 1$, $|M_2| = (2^{n-1} - 2^t)$, следует, что

$$\sigma(f) = 2^n - 2^{n-t-1} + 4 + (2^t - 1)(2^{n-t+1} - 4) + (2^{n-1} - 2^t)4 = 5 \cdot 2^n - 2^{n-t+2} - 2^{t+3} + 8.$$

Теорема 4 показывает, что существуют сбалансированные булевы функции f от n переменных с максимальной алгебраической степенью $\deg f = n - 1$, удовлетворяющие условию $\sigma(f) = O(2^n)$ при $n \rightarrow \infty$.

Рассмотрим для построенных функций f нелинейность $\text{nl}(f)$ (расстояние до класса всех аффинных булевых функций от n переменных), которая вычисляется (см., например, [1; стр. 82]) по формуле

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

Из доказательства теоремы 4 следует, что

$$\max_{\vec{a} \in \{0,1\}^n} |W_f(\vec{a})| = W_f(0, \dots, 0, 1) = 2^n - 2^{n-t+1} + 4,$$

а значит, $\text{nl}(f) = 2^{n-t} - 2$.

Рассмотрим еще один класс булевых функций. Пусть n — четное натуральное число, $n \geq 4$, φ — произвольная бент-функция от $n - 2$ переменных. Известно (см., например, [1; теорема 6.30]), что $\deg \varphi \leq \frac{n}{2} - 1$. Зададим функцию f равенством

$$f(x_1, \dots, x_n) = x_1 x_2 \cdots x_{n-1} \oplus \varphi(x_1, \dots, x_{n-2}) \oplus x_n. \quad (21)$$

Булева функция f является сбалансированной и имеет алгебраическую степень $\deg f = n - 1$.

Теорема 5. Пусть булева функция f задана равенством (21). Тогда

$$\sigma(f) = 2^{\frac{3n}{2}-1} + 2^n + (-1)^{f(1,1,\dots,1)} \cdot 2^{\frac{n}{2}+1}.$$

Доказательство. Коэффициенты Уолша–Адамара функции f равны

$$W_f(\vec{a}) = \sum_{x_1, x_2, \dots, x_n \in \{0,1\}} (-1)^{x_1 x_2 \cdots x_{n-1} \oplus \varphi(x_1, \dots, x_{n-2}) \oplus x_n \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n}.$$

Если $a_n = 0$, то очевидно, что $W_f(\vec{a}) = 0$. Если $a_n = 1$, то

$$W_f(a_1, \dots, a_{n-1}, 1) = 2S + 4(-1)^{a_1 \oplus \cdots \oplus a_{n-1}},$$

где

$$S = \sum_{x_1, x_2, \dots, x_{n-1} \in \{0,1\}} (-1)^{\varphi(x_1, x_2, \dots, x_{n-2}) \oplus a_1 x_1 \oplus \cdots \oplus a_{n-1} x_{n-1}}.$$

Несложно заметить, что $S = W_\varphi(a_1, \dots, a_{n-2})(1 + (-1)^{a_{n-1}})$. Таким образом,

$$W_f(a_1, \dots, a_n) = \begin{cases} 0, & \text{если } a_n = 0, \\ 4(-1)^{a_1 \oplus \dots \oplus a_{n-1}}, & \text{если } a_{n-1} = 1, a_n = 1, \\ 4W_\varphi(a_1, \dots, a_{n-2}) + 4(-1)^{a_1 \oplus \dots \oplus a_{n-2}}, & \text{если } a_{n-1} = 0, a_n = 1. \end{cases}$$

Обозначим через $\tilde{\varphi}$ булеву функцию, дуальную к бент-функции φ , т. е. удовлетворяющую соотношению

$$W_\varphi(\vec{a}) = (-1)^{\tilde{\varphi}(\vec{a})} 2^{\frac{n}{2}-1}, \quad \vec{a} \in \{0, 1\}^{n-2}.$$

Известно (см., например, [1; стр. 254]), что функция $\tilde{\varphi}$ является бент-функцией. Отсюда следует, что бент-функцией является и функция ψ , определенная равенством

$$\psi(x_1, \dots, x_{n-2}) = \tilde{\varphi}(x_1, \dots, x_{n-2}) \oplus x_1 \oplus \dots \oplus x_{n-2}.$$

Для ее веса (как и для веса любой бент-функции от $n-2$ переменных) справедливы равенства $\|\psi\| = 2^{n-3} \pm 2^{\frac{n}{2}-2}$. Из соотношения

$$(-1)^{a_1 \oplus \dots \oplus a_{n-2}} W_\varphi(a_1, \dots, a_{n-2}) = 2^{\frac{n}{2}-1} (-1)^{\psi(a_1, \dots, a_{n-2})}$$

получим, что среди чисел $(-1)^{a_1 \oplus \dots \oplus a_{n-2}} W_\varphi(a_1, \dots, a_{n-2})$ будет $\|\psi\|$ чисел, равных $-2^{\frac{n}{2}-1}$, и $2^{n-2} - \|\psi\|$ чисел, равных $2^{\frac{n}{2}-1}$. Если $\|\psi\| = 2^{n-3} - 2^{\frac{n}{2}-2}$, то

$$\sigma(f) = 2^{n-2} \cdot 4 + (2^{\frac{n}{2}+1} - 4) 2^{\frac{n}{2}-2} (2^{\frac{n}{2}-1} - 1) + (2^{\frac{n}{2}+1} + 4) 2^{\frac{n}{2}-2} (2^{\frac{n}{2}-1} + 1) = 2^{\frac{3n}{2}-1} + 2^n + 2^{\frac{n}{2}+1}.$$

Если $\|\psi\| = 2^{n-3} + 2^{\frac{n}{2}-2}$, то

$$\sigma(f) = 2^{n-2} \cdot 4 + (2^{\frac{n}{2}+1} - 4) 2^{\frac{n}{2}-2} (2^{\frac{n}{2}-1} + 1) + (2^{\frac{n}{2}+1} + 4) 2^{\frac{n}{2}-2} (2^{\frac{n}{2}-1} - 1) = 2^{\frac{3n}{2}-1} + 2^n - 2^{\frac{n}{2}+1}.$$

Для завершения доказательства остается заметить, что $\|\psi\| > 2^{n-3}$ тогда и только тогда, когда $W_\psi(\vec{0}) = W_{\tilde{\varphi}}(1, 1, \dots, 1) < 0$, что согласно равенству $\tilde{\tilde{\varphi}} = \varphi$, равносильно условию $\varphi(1, 1, \dots, 1) = 1$.

Теорема 5 показывает, что существуют сбалансированные булевы функции f от n переменных с максимальной алгебраической степенью $\deg f = n-1$, для которых $\sigma(f) = O(2^{\frac{3n}{2}})$ при $n \rightarrow \infty$. Из доказательства теоремы 5 следует, что для рассматриваемых функций

$$\max_{\vec{a} \in \{0, 1\}^n} |W_f(\vec{a})| = 2^{\frac{n}{2}+1} + 4, \quad \text{nl}(f) = 2^{n-1} - 2^{\frac{n}{2}} - 2.$$

4. Функции, построенные с помощью конструкций Мэйорана–Мак-Фарланда и Доббертина

Пусть $n = 2k$, где $k \geq 2$, $\Phi : \{0, 1\}^k \rightarrow \{0, 1\}^k$ — произвольное отображение с координатными функциями $\Phi_i : \{0, 1\}^k \rightarrow \{0, 1\}$, $i = 1, 2, \dots, k$, т. е. $\Phi(\vec{y}) = (\Phi_1(\vec{y}), \dots, \Phi_k(\vec{y}))$. Для $\vec{x} = (x_1, \dots, x_k)$, $\vec{y} = (y_1, \dots, y_k) \in \{0, 1\}^k$ введем обозначения

$$\langle \vec{x}, \vec{y} \rangle = x_1 y_1 \oplus x_2 y_2 \oplus \dots \oplus x_k y_k;$$

$$\langle \vec{x}, \Phi(\vec{y}) \rangle = \Phi_1(\vec{y})x_1 \oplus \Phi_2(\vec{y})x_2 \oplus \cdots \oplus \Phi_k(\vec{y})x_k.$$

Выберем произвольную булеву функцию $h(\vec{y})$ от k переменных. Определим следующую булеву функцию от n переменных:

$$f(\vec{z}) = f(\vec{x}, \vec{y}) = \langle \vec{x}, \Phi(\vec{y}) \rangle \oplus h(\vec{y}), \quad \vec{x}, \vec{y} \in \{0, 1\}^k, \vec{z} = (\vec{x}, \vec{y}). \quad (22)$$

В этом случае говорят (см., например, [4]), что f задана с помощью конструкции Мэйорана–Мак–Фарланда. Если Φ пробегает все подстановки на множестве $\{0, 1\}^k$, а h — все булевы функции от k переменных, то функции f , определенные равенством (22), образуют семейство бент-функций Мэйорана–Мак–Фарланда (см. [1; стр. 261], [3]).

Пусть $M = (m_{ij})_{k \times k}$ — матрица над полем $GF(2)$, $\text{rang } M = k - 1$. Рассмотрим отображение Φ

$$\Phi(\vec{y}) = \vec{y}M, \quad \vec{y} \in \{0, 1\}^k. \quad (23)$$

Теорема 6. Пусть булева функция $f(\vec{z})$ построена по правилу (22), где отображение Φ определено равенством (23). Тогда $\sigma(f) = 2^{\frac{3n}{2}-1}$.

Доказательство. Обозначим через L линейное подпространство, порожденное всеми строками матрицы M . Отображение Φ является линейным преобразованием, и для прообразов элементов при действии отображения Φ справедливы равенства

$$\Phi^{-1}(\vec{0}) = \{\vec{0}, \vec{c}\}, \quad \Phi^{-1}(\vec{v}) = \begin{cases} \emptyset, & \text{если } \vec{v} \notin L, \\ \{\vec{d}, \vec{d} \oplus \vec{c}\}, & \text{если } \vec{v} \in L \text{ и } \vec{d}M = \vec{v}. \end{cases} \quad (24)$$

Из формулы (24) и равенств

$$\begin{aligned} W_f(\vec{v}, \vec{w}) &= \sum_{(\vec{x}, \vec{y}) \in \{0, 1\}^n} (-1)^{f(\vec{x}, \vec{y}) \oplus \langle \vec{x}, \vec{y} \rangle, (\vec{v}, \vec{w})} = \\ &= \sum_{\vec{y} \in \{0, 1\}^k} (-1)^{h(\vec{y}) \oplus \langle \vec{y}, \vec{w} \rangle} \sum_{\vec{x} \in \{0, 1\}^k} (-1)^{\langle \vec{x}, \Phi(\vec{y}) \oplus \vec{v} \rangle}, \\ \sum_{\vec{x} \in \{0, 1\}^k} (-1)^{\langle \vec{x}, \Phi(\vec{y}) \oplus \vec{v} \rangle} &= \begin{cases} 2^k, & \text{если } \Phi(\vec{y}) = \vec{v}, \\ 0, & \text{если } \Phi(\vec{y}) \neq \vec{v}, \end{cases} \end{aligned}$$

получим

$$W_f(\vec{\alpha}) = W_f(\vec{v}, \vec{w}) = \begin{cases} 0, & \text{если } \vec{v} \notin L, \\ 2^k (-1)^{\langle \vec{d}, \vec{w} \rangle} \left((-1)^{h(\vec{d})} + (-1)^{h(\vec{d} \oplus \vec{c}) \oplus \langle \vec{c}, \vec{w} \rangle} \right), & \text{если } \vec{v} \in L. \end{cases} \quad (25)$$

Отсюда

$$|W_f(\vec{v}, \vec{w})| = \begin{cases} 2^{k+1}, & \text{если } \vec{v} \in L \text{ и } \langle \vec{c}, \vec{w} \rangle = h(\vec{d}) \oplus h(\vec{d} \oplus \vec{c}), \\ 0, & \text{если } \vec{v} \notin L \text{ или } \langle \vec{c}, \vec{w} \rangle \neq h(\vec{d}) \oplus h(\vec{d} \oplus \vec{c}). \end{cases}$$

Число ненулевых коэффициентов Уолша–Адамара функции f равно $|L| \cdot 2^{k-1} = 2^{n-2}$, а значит, $\sigma(f) = 2^{\frac{3n}{2}-1}$.

Отметим, что формула (25) является частным случаем равенств, полученных в [1; стр. 112], [9; равенство (55)]. Доказательство приведено лишь для полноты изложения.

Функции f , рассмотренные в теореме 6, являются сбалансированными тогда и только тогда, когда $W_f(\vec{0}) = 0$, т. е. (в соответствии с (25)) при условии $h(\vec{0}) \neq h(\vec{c})$. Из формулы

$$f(\vec{z}) = h(\vec{y}) \oplus \sum_{i,j=1}^k m_{ji} x_i y_j$$

следует, что их алгебраические степени удовлетворяют соотношениям

$$\deg f = \begin{cases} \deg h, & \text{если } \deg h \geq 3; \\ 2, & \text{если } \deg h \leq 2. \end{cases}$$

Из доказательства теоремы 6 следует, что

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

Пусть $g(\vec{x})$ — произвольная булева функция от k переменных. Выберем некоторую подстановку π , действующую на множестве $\{0,1\}^k$. Определим следующую булеву функцию от $n = 2k$ переменных:

$$f(\vec{z}) = f(\vec{y}, \vec{x}) = \begin{cases} g(\vec{x}), & \text{если } \vec{y} = \vec{0}, \\ \langle \pi(\vec{y}), \vec{x} \rangle, & \text{если } \vec{y} \neq \vec{0}. \end{cases} \quad (26)$$

Заметим, что функция $\langle \pi(\vec{y}), \vec{x} \rangle$ является бент-функцией из класса Мэйорана–Мак–Фарланда. Булевы функции $f(\vec{z})$, определенные равенством (26), являются частными примерами функций, рассмотренных Г. Доббертином в [5; утверждение 8].

Теорема 7. Пусть $\pi(\vec{0}) = \vec{0}$, $g(\vec{x})$ — сбалансированная булева функция и $f(\vec{z})$ — функция, определенная равенством (26). Тогда $\sigma(f) = 2^{\frac{3n}{2}} - 2^n$.

Доказательство. Вычислим спектральные коэффициенты функции f . Пусть $\vec{\alpha} = (\vec{v}, \vec{w})$ — произвольный вектор из $\{0,1\}^n$. Тогда

$$\begin{aligned} W_f(\vec{v}, \vec{w}) &= \sum_{(\vec{y}, \vec{x}) \in \{0,1\}^n} (-1)^{f(\vec{y}, \vec{x}) \oplus \langle (\vec{v}, \vec{w}), (\vec{y}, \vec{x}) \rangle} = \\ &= \sum_{\vec{x} \in \{0,1\}^k} (-1)^{g(\vec{x}) \oplus \langle \vec{w}, \vec{x} \rangle} + \sum_{(\vec{y}, \vec{x}) \in (\{0,1\}^k \setminus \vec{0}) \times \{0,1\}^k} (-1)^{\langle \pi(\vec{y}), \vec{x} \rangle \oplus \langle \vec{w}, \vec{x} \rangle \oplus \langle \vec{v}, \vec{y} \rangle} = W_g(\vec{w}) + S(\vec{v}, \vec{w}), \end{aligned}$$

где

$$S(\vec{v}, \vec{w}) = \sum_{(\vec{y}, \vec{x}) \in (\{0,1\}^k \setminus \vec{0}) \times \{0,1\}^k} (-1)^{\langle \pi(\vec{y}) \oplus \vec{w}, \vec{x} \rangle \oplus \langle \vec{v}, \vec{y} \rangle}.$$

Вычислим $S(\vec{v}, \vec{w})$. Справедливо равенство

$$S(\vec{v}, \vec{w}) = \sum_{\vec{y} \neq \vec{0}} (-1)^{\langle \vec{v}, \vec{y} \rangle} \sum_{\vec{x} \in \{0,1\}^k} (-1)^{\langle \pi(\vec{y}) \oplus \vec{w}, \vec{x} \rangle}.$$

В силу того, что

$$\sum_{\vec{x} \in \{0,1\}^k} (-1)^{\langle \pi(\vec{y}) \oplus \vec{w}, \vec{x} \rangle} = \begin{cases} 2^k, & \text{если } \pi(\vec{y}) = \vec{w}, \\ 0, & \text{если } \pi(\vec{y}) \neq \vec{w}, \end{cases}$$

получаем

$$S(\vec{v}, \vec{w}) = \begin{cases} 2^k (-1)^{\langle \vec{v}, \pi^{-1}(\vec{w}) \rangle}, & \text{если } \vec{w} \neq \vec{0}, \\ 0, & \text{если } \vec{w} = \vec{0}. \end{cases}$$

Откуда следует, что $S(\vec{v}, \vec{w}) = 2^k (-1)^{\langle \vec{v}, \pi^{-1}(\vec{w}) \rangle} (1 - \delta_{\vec{w}, \vec{0}})$, где

$$\delta_{\vec{w}, \vec{0}} = \begin{cases} 0, & \text{если } \vec{w} = \vec{0}, \\ 1, & \text{если } \vec{w} \neq \vec{0}, \end{cases}$$

а значит,

$$W_f(\vec{v}, \vec{w}) = W_g(\vec{w}) + 2^k (-1)^{\langle \vec{v}, \pi^{-1}(\vec{w}) \rangle} (1 - \delta_{\vec{w}, \vec{0}}). \quad (27)$$

Из соотношений $W_g(\vec{0}) = 0$, $|W_g(\vec{w})| \leq 2^k$, $\vec{w} \in \{0, 1\}^k$, имеем

$$|W_f(\vec{v}, \vec{w})| = \begin{cases} 0, & \text{если } \vec{w} = \vec{0}, \vec{v} \in \{0, 1\}^k, \\ 2^k - W_g(\vec{w}), & \text{если } \vec{w} \neq \vec{0}, \langle \pi^{-1}(\vec{w}), \vec{v} \rangle = 1, \\ 2^k + W_g(\vec{w}), & \text{если } \vec{w} \neq \vec{0}, \langle \pi^{-1}(\vec{w}), \vec{v} \rangle = 0. \end{cases}$$

Таким образом,

$$\sigma(f) = \sum_{\vec{w} \in \{0,1\}^k \setminus \vec{0}} 2^{k-1} \cdot 2^{k+1} = 2^{2k} (2^k - 1) = 2^n (2^{\frac{n}{2}} - 1).$$

Отметим, что равенство (27) непосредственно следует из [5; утверждение 8] и [9; равенство (55)]. Его доказательство приведено лишь для полноты изложения.

Все функции f , рассмотренные в теореме 7, являются сбалансированными. Из равенства

$$f(\vec{y}, \vec{x}) = (y_1 \oplus 1)(y_2 \oplus 1) \cdots (y_k \oplus 1)g(\vec{x}) \oplus \langle \pi(\vec{y}), \vec{x} \rangle$$

и соотношения $\deg(\pi_1(\vec{y})x_1 \oplus \cdots \oplus \pi_k(\vec{y})x_k) \leq k$ следует, что $\deg f = \frac{n}{2} + \deg g$. Из доказательства теоремы 7 получаем

$$\max_{\vec{\alpha} \in \{0,1\}^n} |W_f(\vec{\alpha})| = \max_{\vec{w} \in \{0,1\}^k} |W_g(\vec{w})| + 2^k, \quad \text{nl}(f) = 2^{n-1} - 2^{\frac{n}{2}} + \text{nl}(g).$$

Теорема 7 показывает, что существуют сбалансированные булевы функции f от n переменных алгебраической степени $\deg f = \frac{n}{2}, \frac{n}{2} + 1, \dots, n-1$ у которых $\sigma(f) \sim 2^{\frac{3n}{2}}$ при $n \rightarrow \infty$.

Список литературы

1. Логачев О.А., Сальников А.А., Смышляев С.В., Яценко 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*, 2013, № 3(21), 11–25.
- 3 Дискретная математика, т. 27 № 4

3. McFarland R.L., “A family of difference sets in non-cyclic groups”, *J. Comb. Theory. Ser. A*, **15**: 1 (1973), 1–10.
4. 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.
5. Dobbertin H., “Construction of bent functions and balanced Boolean functions with high nonlinearity”, *Lect. Notes Comput. Sci.*, **1008** (1995), 61–74.
6. Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра: Учебник, II*, М.: Гелиос АРВ, 2003, 416 с.
7. Риордан Д., *Комбинаторные тождества*, М.: Наука, 1982, 256 с.
8. Rueppel R.A., *Analysis and design of stream ciphers*, Springer-Verlag, 1986, 244 pp.
9. Carlet C., “Boolean functions for cryptography and error correcting codes”, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, eds. Y. Crama, P. L. Hammer, Cambridge Univ. Press, 2010, 257–397.

Статья поступила 07.08.2015.