Math-Net.Ru

Общероссийский математический портал

Г. И. Ивченко, Ю. И. Медведев, В. А. Миронова, Структура спектров булевых функций, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 1, 57–70

DOI: <https://doi.org/10.4213/mvk174>

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: 3.82.47.9

26 апреля 2023 г., 17:49:45

Структура спектров булевых функций

Г. И. Ивченко, Ю. И. Медведев, В. А. Миронова

МИЭМ НИУ Высшая школа экономики, Москва
Академия криптографии Российской Федерации, Москва

Получено 20.IV.2015

Для спектра Фурье булевой функции f от n переменных определяется понятие его структуры, исследуются различные его свойства, в том числе в стохастической постановке, когда функция f случайна и выбирается с равной вероятностью из множества $F_n = \{f\}$ всех булевых функций от n переменных.

Работа выполнена при финансовой поддержке Академии криптографии Российской Федерации.

Ключевые слова: булева функция, преобразование Уолша–Адамара, спектр функции, структура спектра, распределения элементов структуры, предельные теоремы

The structure of Boolean functions spectra

G. I. Ivchenko, Yu. I. Medvedev, V. A. Mironova

MIEM NRU Higher School of Economics, Moscow
Academy of Cryptography of the Russian Federation, Moscow

Abstract. The notion of the spectrum of the Boolean function f of n variables is defined, its properties are investigated. The stochastic case is considered also under the assumption that the function f has the uniform distribution on the set $F_n = \{f\}$ of all Boolean functions of n variables.

Keywords: Boolean function, Walsh–Hadamard transform, the spectrum of a Boolean function, structure of the spectrum, structure distribution, limit theorems

1. Введение

Пусть $V_n = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_{2^n-1}\}$ есть n -мерное векторное пространство над полем из двух элементов, векторы которого упорядочены по возрастанию соответствующих им чисел ($\mathbf{v}_i$ отвечает двоичному представлению числа $i = 0, 1, \dots, 2^n-1$), $f: V_n \rightarrow \{0, 1\}$ — булева функция от n переменных и $F_n = \{f\}$ — множество всех таких функций.

Целочисленная функция $w_f: V_n \rightarrow \mathbf{Z}$, определяемая выражением

$$w_f(\mathbf{u}) = \sum_{\mathbf{x} \in V_n} f(\mathbf{x})(-1)^{(\mathbf{u}, \mathbf{x})}, \quad \mathbf{u} \in V_n, \quad (1)$$

называется *преобразованием Фурье* булевой функции f ; величина $w_{ni} = w_f(\mathbf{v}_i)$ называется *коэффициентом Фурье* функции f , отвечающим вектору $\mathbf{v}_i$, а совокупность всех этих величин, составляющая вектор

$$\mathbf{w}_n = (w_{n0}, w_{n1}, \dots, w_{n,2^n-1}), \quad (2)$$

называется *спектром Фурье* функции f . Напомним, что скалярное произведение $(\mathbf{a}, \mathbf{b})$ векторов $\mathbf{a} = (a_1, a_2, \dots, a_n)$ и $\mathbf{b} = (b_1, b_2, \dots, b_n)$ из V_n вычисляется по формуле $(\mathbf{a}, \mathbf{b}) = a_1 b_1 \oplus a_2 b_2 \oplus \dots \oplus a_n b_n$ ($\oplus$ — знак сложения по mod 2).

Преобразование Уолша и *спектр Уолша* булевой функции f определяются выражениями

$$\hat{w}_f(\mathbf{u}) = \sum_{\mathbf{x} \in V_n} \hat{f}(\mathbf{x})(-1)^{(\mathbf{u}, \mathbf{x})}, \quad \mathbf{u} \in V_n, \quad (3)$$

где

$$\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})} = 1 - 2f(\mathbf{x}),$$

и, соответственно,

$$\hat{\mathbf{w}}_n = (\hat{w}_{n0}, \hat{w}_{n1}, \dots, \hat{w}_{n,2^n-1}). \quad (4)$$

Эти преобразования связаны, очевидно, соотношением

$$\hat{w}_f(\mathbf{u}) = 2^n I\{\mathbf{u}=\mathbf{0}\} - 2w_f(\mathbf{u}) \quad (5)$$

(здесь и далее $I\{\cdot\}$ — индикатор), в силу которого можно рассматривать лишь один из этих спектров (будем называть их кратко: спектр (2) и спектр (4)); мы выберем спектр (4), поскольку, как будет видно, работать с ним удобнее.

Замечание 1. В литературе нет однозначности в определении этих понятий. Каждое из преобразований (1) и (3) называют преобразованиями и Фурье, и Уолша, и Уолша–Адамара, и Адамара. Однако в последнее время прослеживается тенденция называть их именно так, как это указано выше (ср. [4]). Отметим также, что в книгах [1, с. 397–398] и [2, с. 204–205] суммы в формулах (1) и (3) дополнительно нормируются множителем, но мы останавливаемся на указанных в (1) и (3) вариантах определения, поскольку далее будет удобнее работать с целочисленными функциями $w_f(\mathbf{u})$ и $\hat{w}_f(\mathbf{u})$.

Объектом нашего внимания будут следующие функционалы от спектра Уолша (4):

$$\mu_r(f) = \sum_{\mathbf{u} \in V_n} I\{\hat{w}_f(\mathbf{u}) = r\}, \quad r = 0, \pm 1, \pm 2, \dots, \pm 2^n, \quad (6)$$

так что $\mu_r(f)$ есть число спектральных коэффициентов, имеющих значение r . Их совокупность (6) будем называть *структурой спектра* (или просто *структурой*) булевой функции f , а отдельные величины $\mu_r(f)$ — *элементами структуры* (в дальнейшем изложении аргумент f иногда будем опускать, если речь идет об одной и той же фиксированной функции). Эти «сводные» характеристики спектра важны при анализе различных свойств булевых функций, используемых в теории информации, кодирования и криптографии. При этом в некоторых задачах знаки спектральных коэффициентов $\hat{w}_{ni} = \hat{w}_f(\mathbf{v}_i)$ несущественны, поэтому, наряду со структурой (6), целесообразно ввести понятие *абсолютной структуры* — это вектор

$$|\mu| = (\mu_0, \mu_{|1|}, \mu_{|2|}, \dots, \mu_{|2^n|}), \quad \mu_{|r|} = \mu_r + \mu_{-r}, \quad r = 1, 2, \dots, 2^n. \quad (7)$$

В качестве иллюстрации отметим, в частности, что важнейшие криптографические параметры булевой функции f — ее *спектральная сложность* $s(f)$ и *нелинейность* $nl(f)$ (т. е. расстояние от f до множества аффинных функций $A_n = \{f \in F_n : f(\mathbf{x}) = (\mathbf{a}, \mathbf{x}) \oplus \varepsilon, \varepsilon = 0, 1\}$) — выражаются через элементы структуры следующим образом:

$$s(f) = 2^n - \mu_0(f), \quad (8)$$

т. е. $s(f)$ — это число ненулевых элементов спектра, а

$$nl(f) = 2^{n-1} - \frac{1}{2} l(f), \quad (9)$$

где $l(f) = \max\{|r| : \mu_r(f) > 0\}$ — максимальное по модулю значение спектра.

Наконец, еще одно важное структурное понятие связано с рангами спектральных коэффициентов: говорят, что спектральный коэффициент $\widehat{w}_f(\mathbf{u})$ имеет ранг k , если вес $\|\mathbf{u}\|$ вектора $\mathbf{u}$ (число его единичных координат) равен k . В соответствии с этим будем называть число спектральных коэффициентов ранга k , имеющих значение r , элементом ранговой структуры спектра и обозначать его символом $\mu_{r,k}$:

$$\mu_{r,k} = \sum_{\mathbf{u} \in V_n} I\{\widehat{w}_f(\mathbf{u}) = r, \|\mathbf{u}\| = k\}. \quad (10)$$

Совокупность же всех этих величин $\{\mu_{r,k}, k = 0, 1, \dots, n, -2^n \leq r \leq 2^n\}$ образует ранговую структуру спектра. Очевидно, что

$$\mu_r = \sum_{k=0}^n \mu_{r,k} \quad \text{и} \quad 0 \leq \mu_{r,k} \leq \binom{n}{k}.$$

В частности, $\mu_{r,0} \in \{0, 1\}$ и при этом $\mu_{r,0} = I\{2^n - 2\|f\| = r\}$ (напомним, что символом $\|f\|$ обозначается вес булевой функции f , т. е. число принимаемых ею единичных значений). В терминах ранговой структуры весьма просто формулируется критерий корреляционной иммунности заданного порядка t булевой функции — одного из важнейших понятий теории булевых функций, означающего статистическую независимость функции от любого подмножества ее t переменных ($1 \leq t \leq n$), т. е. (см., например, [8]) если переменные $x_1, x_2, \dots, x_n$ являются независимыми и равномерно распределенными двоичными случайными величинами, то случайная величина $f(x_1, x_2, \dots, x_n)$ не зависит от любого t -мерного случайного вектора $(x_{i_1}, x_{i_2}, \dots, x_{i_t})$, $1 \leq i_1 < i_2 < \dots < i_t \leq n$. Корреляционная иммунность эквивалентна, очевидно, условию $\mu_{0k} = \binom{n}{k}$ для всех рангов $k = 1, 2, \dots, t$.

Отметим еще две глобальные лавинные характеристики булевых функций, которые определяются через элементы структуры спектра. Это σ_f^2 — сумма квадратов коэффициентов спектра Уолша и Δ_f — абсолютный показатель (ср. [6]):

$$\sigma_f^2 = \sum_{\mathbf{a} \in V_n} \widehat{w}_{D_{\mathbf{a}}f}^2(\mathbf{0}), \quad (11)$$

$$\Delta_f = \max_{\substack{\mathbf{a} \in V_n \\ \mathbf{a} \neq \mathbf{0}}} |\widehat{w}_{D_{\mathbf{a}}f}(\mathbf{0})|, \quad (12)$$

где $D_{\mathbf{a}}f = f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})$ ($\mathbf{x}, \mathbf{a} \in V_n$) есть производная f по направлению $\mathbf{a}$,

$$\widehat{w}_{D_{\mathbf{a}}f}(\mathbf{0}) = \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})}$$

— автокорреляционный коэффициент, определяющий число изменений f при замене аргумента $\mathbf{x}$ на $\mathbf{x} \oplus \mathbf{a}$.

Отметим также, что если $\widehat{w}_{D_{\mathbf{a}}f}(\mathbf{0}) = 0$ для всех $\mathbf{a}$ с весами $\|\mathbf{a}\| \leq k$, то говорят, что f удовлетворяет важному в анализе булевых функций критерию распространения степени k (PC(k) – Propagation criterion).

Поскольку справедливо соотношение (ср. [6])

$$\widehat{w}_f^2(\mathbf{u}) = \sum_{\mathbf{a} \in V_n} (-1)^{(\mathbf{u}, \mathbf{a})} \widehat{w}_{D_{\mathbf{a}}f}(\mathbf{0}),$$

имеют место представления

$$\sigma_f^2 = \frac{1}{2^n} \sum_{\mathbf{u} \in V_n} \widehat{w}_f^4(\mathbf{u}) = \frac{1}{2^n} \sum_{r=0}^{2^n} r^4 \mu_{|r|},$$

а абсолютный показатель однозначно определяется условием

$$\Delta_f = \max_{\mathbf{a} \in V_n} \{r : \mu_r(D_{\mathbf{a}}(f)) > 0\}.$$

В практических задачах при выборе функции f предпочтение отдается функциям с малыми значениями этих характеристик. При этом $0 \leq \Delta_f \leq 2^n$, и нижняя граница достигается лишь на бент-функциях, а верхняя — лишь на функциях с линейной структурой, т. е. на функциях, для которых существуют такие векторы $\mathbf{a} \in V_n$, что $f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a}) = \text{const}$.

В следующем разделе приводится (для полноты картины) краткий обзор общих свойств (в ряде случаев — известных) элементов структуры спектров, а в разделах 3 и 4 исследуем их в стохастической постановке, когда функция f случайна и выбирается равновероятно из множества $F_n = \{f\}$ всех булевых функций от n переменных.

2. Основные свойства структуры спектра

1. Четность спектральных коэффициентов. Для спектра (3) можно получить и ряд других представлений, проясняющих его свойства. Так как для булевых переменных a и b выполняются равенства $a \oplus b = a + b - 2ab$ и $(-1)^a = 1 - 2a$, то можно записать цепочку соотношений

$$\begin{aligned} \widehat{w}_f(\mathbf{u}) &= \sum_{\mathbf{x} \in V_n} \widehat{f}(\mathbf{x}) (-1)^{(\mathbf{u}, \mathbf{x})} = \sum_{\mathbf{x} \in V_n} (1 - 2f(\mathbf{x})) (1 - 2(\mathbf{u}, \mathbf{x})) = \\ &= 2^n - 2 \|f(\mathbf{x})\| - 2 \|(\mathbf{u}, \mathbf{x})\| + 4 \|f(\mathbf{x})(\mathbf{u}, \mathbf{x})\|, \end{aligned}$$

из которой следует (см. (6)), что элементы структуры $\mu_r(f)$ могут быть отличными от нуля лишь при четных значениях r (четность спектральных коэффициентов $w_f(\mathbf{u})$ следует также из (5)).

Более того, поскольку $\|(\mathbf{u}, \mathbf{x})\| = 2^{n-1} I\{\mathbf{u} \neq \mathbf{0}\}$ при любом $\mathbf{u} \in V_n$, справедливо равенство

$$\widehat{w}_f(\mathbf{u}) = 2^n I\{\mathbf{u} = \mathbf{0}\} - 2\|f\| + 4\|f(\mathbf{x})(\mathbf{u}, \mathbf{x})\|,$$

и, значит, при $n \geq 2$ величины $\mu_r(f)$ могут быть отличными от нуля лишь при таких значениях r , для которых числа $2\|f\| + r$ кратны четырем.

2. Структура аффинно эквивалентных функций. Аффинным преобразованием в пространстве V_n называется отображение

$$\mathbf{x} \rightarrow \mathbf{x}' = \mathbf{x}A + \mathbf{b},$$

где A — невырожденная булева $(n \times n)$ -матрица, $\mathbf{b} \in V_n$. Функции f и f' называются *аффинно эквивалентными*, если существует аффинное преобразование, переводящее f в f' . Если существует линейное преобразование (аффинное с $\mathbf{b} = \mathbf{0}$), переводящее f в f' , то функции f и f' называются *линейно эквивалентными*.

Линейно эквивалентные функции имеют одинаковую структуру, а аффинно эквивалентные — одинаковую абсолютную структуру.

Указанное свойство есть прямое следствие известного соотношения

$$\widehat{w}_f(\mathbf{u}) = (-1)^{(b, \mathbf{u}A^{-1})} \widehat{w}_{f'}(\mathbf{u}A^{-1}),$$

из которого видно, что спектр функции f получается перестановкой компонент спектра функции f' и, возможно, изменением знаков.

3. Линейные соотношения для структур. Элементы структуры связаны соотношениями

$$\sum_{r=0}^{2^n-1} r \mu_r(f) = 2^n (-1)^{f(0)}, \quad \sum_{r=0}^{2^n-1} r^2 \mu_r(f) = 2^{2n}.$$

Первое соотношение проверяется непосредственно:

$$\begin{aligned} \sum_{r=0}^{2^n-1} r \mu_r(f) &= \sum_{\mathbf{u} \in V_n} \widehat{w}_f(\mathbf{u}) = \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x})} \sum_{\mathbf{u} \in V_n} (-1)^{(\mathbf{u}, \mathbf{x})} = \\ &= \sum_{\mathbf{x} \in V_n} (-1)^{f(\mathbf{x})} 2^n I\{\mathbf{x} = \mathbf{0}\} = 2^n (-1)^{f(0)}, \end{aligned}$$

второе же есть не что иное, как известное равенство Парсеваля для спектра:

$$\sum_{r=0}^{2^n} r^2 \mu_r(f) = \sum_{\mathbf{u} \in V_n} \widehat{w}_f^2(\mathbf{u}) = 2^{2n}.$$

4. Связь между структурами Фурье и Уолша. По аналогии со структурой (6), которую более точно следует называть *структурой Уолша*, поскольку она определяется для спектра Уолша (3)–(4), можно определить, основываясь на (1)–(2), *структуру Фурье*

$$\mu'_r(f) = \sum_{\mathbf{u} \in V_n} I\{w_f(\mathbf{u}) = r\}, \quad r = 0, \pm 1, \dots, \pm 2^n. \quad (13)$$

Между структурами $\mu_r(f)$ и $\mu'_r(f)$, в силу (5), существует взаимно однозначная связь, которая устанавливается непосредственно. Именно,

$$\begin{aligned} \mu_{2m}(f) &= \sum_{\mathbf{u} \in V_n} I\{\hat{w}_f(\mathbf{u}) = 2m\} = \\ &= \sum_{\mathbf{u} \in V_n} I\{2^n I\{\mathbf{u} = \mathbf{0}\} - 2w_f(\mathbf{u}) = 2m\} = \\ &= I\{2^n - 2w_f(\mathbf{0}) = 2m\} + \sum_{\mathbf{u} \neq \mathbf{0}} I\{-2w_f(\mathbf{u}) = 2m\} = \\ &= \mu'_{-m}(f) + I\{\|f\| = 2^{n-1} - m\} - I\{\|f\| = -m\}, \end{aligned}$$

поскольку $w_f(\mathbf{0}) = \|f\|$. Обращая эту формулу, окончательно находим:

$$\mu'_m(f) = \begin{cases} \mu_{-2m}(f) - 1 & \text{при } m = 2^{n-1} - \|f\|, \\ \mu_{-2m}(f) + 1 & \text{при } m = -\|f\|, \\ \mu_{-2m}(f) & \text{при остальных значениях } m. \end{cases} \quad (14)$$

5. Элемент $\mu_0(f)$. Важнейшей характеристикой структуры спектра и в целом самого спектра булевой функции f является $\mu_0(f)$ — число нулевых элементов спектра (как уже отмечалось во введении, через нее выражается спектральная сложность $s(f)$ булевой функции). Детальные исследования свойств этой характеристики достаточно полно представлены в литературе, и мы приведем здесь лишь некоторые оценки для нее.

Выделим в левой части равенства Парсеваля максимальное слагаемое и обозначим его $l^2(f)$. Пусть это слагаемое соответствует $\mathbf{u} = \mathbf{u}_0$. Тогда это равенство можно переписать в виде

$$1 + \sum_{\mathbf{u} \in V_n, \mathbf{u} \neq \mathbf{u}_0} \frac{\hat{w}_f^2(\mathbf{u})}{l^2(f)} = \frac{2^{2n}}{l^2(f)}.$$

В сумме в левой части этого равенства число ненулевых слагаемых равно $2^n - 1 - \mu_0(f)$, и все они не больше единицы. Поэтому, мажорируя все слагаемые единицей, получаем неравенство

$$2^n - \mu_0(f) \geq \frac{2^{2n}}{l^2(f)}$$

или неравенство

$$\mu_0(f) \leq 2^n - \frac{2^{2n}}{l^2(f)}. \quad (15)$$

При этом равенство достигается тогда и только тогда, когда все ненулевые коэффициенты спектра Уолша (3) равны $\pm l(f)$.

Известны также следующие оценки:

а) если n четное и $l(f) \leq 2^{(n+2)/2}$, то $\mu_0(f) \leq 3 \cdot 2^{n-2}$ и равенство достигается тогда и только тогда, когда носитель структуры спектра состоит из трех точек: (μ_0, μ_r, μ_{-r}) при $r = 2^{(n+2)/2}$;

б) если n нечетное и $l(f) \leq 2^{(n+1)/2}$, то $\mu_0(f) \leq 2^{n-1}$ и равенство достигается тогда и только тогда, когда носитель структуры спектра состоит из трех точек: (μ_0, μ_r, μ_{-r}) при $r = 2^{(n+1)/2}$.

6. Бент-функции. Это один из важнейших классов булевых функций, представляющих особый интерес в связи с тем, что они и только они обладают максимальной нелинейностью $nl(f)$ (см. (9)) во всем множестве F_n . Они существуют при всех четных n , и для них $nl(f) = 2^{n-1} - 2^{n/2-1}$. Их характеристика в терминах структуры формулируется особенно просто: отличными от нуля структурными элементами являются лишь $\mu_{\pm 2^{n/2}}$, при этом

$$\mu_{2^{n/2}} = 2^{n-1} + (-1)^{f(0)} 2^{n/2-1}, \quad \mu_{-2^{n/2}} = 2^{n-1} - (-1)^{f(0)} 2^{n/2-1}.$$

7. Платовидные функции. Это еще один пример особого класса функций, для которых структура имеет весьма простой вид: ее отличными от нуля элементами являются лишь μ_0, μ_{-2^c} и μ_{2^c} при некотором c . При этом, как следует из равенства Парсеваля, $\mu_{-2^c} + \mu_{2^c} = 4^{n-c}$.

8. Линейные функции. Пусть $f(\mathbf{x}) = (\mathbf{a}, \mathbf{x})$ при некотором $\mathbf{a} \in V_n$, $\mathbf{a} \neq 0$. Тогда $\hat{w}_f(\mathbf{u}) = 2^n I\{\mathbf{u} = \mathbf{a}\}$ и, следовательно,

$$\mu_r(f) = \begin{cases} 2^n - 1 & \text{при } r = 0, \\ 0 & \text{при } r = 1, 2, \dots, 2^n - 1, \\ 1 & \text{при } r = 2^n. \end{cases}$$

Такую структуру имеют только линейные функции.

3. Стохастическая модель

Пусть на множестве $F_n = \{f\}$ задана равномерная мера, т. е. любая функция может наблюдаться с вероятностью 2^{-2^n} . Вопросы исследования распределений спектра (2) в такой модели рассматривались в работе [3], где, в частности, получены точные и предельные распределения компонент этого вектора и их пар. Для дальнейшего анализа будет удобнее рассматривать спектр (4), поскольку все его компоненты имеют одинаковые распределения (в отличие от спектра (2)). Используя связь (5), нетрудно переформулировать результаты работы [3] в терминах спектра (4). А именно справедливы следующие утверждения, вытекающие из теорем 1 и 5 указанной работы.

Теорема 1. *В рассматриваемой модели все компоненты вектора (4) являются одинаково распределенными центрированными некоррелированными случайными величинами, дисперсии которых равны 2^n , а их одномерные и двумерные распределения имеют следующий вид:*

$$\begin{aligned} \mathbf{P}\{\hat{w}_{ni}=2u\} &= \binom{2^n}{2^{n-1}+u} 2^{-2^n} \stackrel{\text{def}}{=} p_{2^{n-1}}(u), \quad u=0, \pm 1, \dots, \pm 2^{n-1}, \\ \mathbf{P}\{\hat{w}_{ni}=2u, \hat{w}_{nj}=2v\} &= p_{2^{n-2}}\left(\frac{u+v}{2}\right) p_{2^{n-2}}\left(\frac{u-v}{2}\right), \quad u \equiv v \pmod{2}. \end{aligned} \quad (16)$$

В проверке здесь нуждается лишь утверждение об одинаковой распределенности компонент вектора (4). Она вытекает из вида их совместной производящей функции (см. формулу (9) в [3])

$$\mathbf{E} \prod_j z_j^{\hat{w}_{nj}} = z_0^{2^n} \mathbf{E} \prod_j \left(\frac{1}{z_j^2}\right)^{\hat{w}_{nj}} = \left(\frac{z_0}{2}\right)^{2^n} \prod_j \left(1 + \prod_i \left(\frac{1}{z_j^2}\right)^{(-1)^{(v_i, v_j)}}\right).$$

Нетрудно убедиться, что производящая функция

$$\mathbf{E} z_0^{\hat{w}_{n0}} = \left(\frac{z_0}{2}\right)^{2^n} \left(1 + \frac{1}{z_0^2}\right)^{2^n} = \frac{1}{2^{2^n}} \left(z_0 + \frac{1}{z_0}\right)^{2^n} = \frac{1}{2^{2^n}} \left[\left(1 + \frac{1}{z_0^2}\right)(1 + z_0^2)\right]^{2^{n-1}} \quad (17)$$

первой компоненты и производящая функция

$$\mathbf{E} z_i^{\hat{w}_{ni}} = \frac{1}{2^{2^n}} \prod_j \left(1 + \left(\frac{1}{z_j^2}\right)^{(-1)^{(v_i, v_j)}}\right) = \frac{1}{2^{2^n}} \left[\left(1 + \frac{1}{z_i^2}\right)(1 + z_i^2)\right]^{2^{n-1}}$$

любой другой компоненты w_{ni} ($i=1, 2, \dots, 2^n$) идентичны (использовано известное (см. [1, с. 396]) соотношение ортогональности $\sum_{j=0}^{2^n} (-1)^{(v_i, v_j)} = 0$, если $i=1, 2, \dots, 2^n$, означающее, что среди слагаемых этой суммы одинаковое число 2^{n-1} положительных и отрицательных единиц). $\square$

Подчеркнем следующее обстоятельство. Из вида производящей функции (17) (третья форма) следует, что распределение величины $\hat{w}_{n0}/2$ совпадает с распределением разности двух независимых биномиальных $\text{Bi}(2^{n-1}, \frac{1}{2})$ случайных величин, которое в [3] названо *симметризованным биномиальным распределением* $\text{Bis}(2^{n-1}, \frac{1}{2})$. Через него же выражается и распределение пары $(\hat{w}_{ni}/2, \hat{w}_{nj}/2)$, указанное в (16). Вторая форма в (17) говорит о том, что это распределение совпадает с распределением суммы 2^n независимых случайных величин, с равными вероятностями принимающих значения ± 1 . Наконец, первая форма в (17) есть выражение того факта, что $w_{n0}/2 = 2^{n-1} - \|f\|$, а величина $\|f\|$ имеет биномиальное распределение $\text{Bi}(2^n, \frac{1}{2})$, что, в свою очередь, влечет за собой асимптотическую нормальность с параметрами $(0, 2^n)$ всех спектральных коэффициентов.

Перейдем к нашей основной задаче — анализу структуры (6) — и, прежде всего, установим следующие свойства их моментов.

Теорема 2. *Явные и асимптотические при $n \rightarrow \infty$ выражения для первых и вторых моментов элементов структуры (6) имеют следующий вид:*

$$\begin{aligned} \mathbf{E} \mu_{2r} &= \mathbf{E} \mu_{-2r} = \\ &= 2^n \mathbf{P} \{ \hat{w}_{ni} = 2r \} = \\ &= \binom{2^n}{2^{n-1}+r} \frac{1}{2^{2^n-n}} \quad \text{при } r=0, \pm 1, \dots, \pm 2^{n-1}, \end{aligned} \quad (18)$$

$$\mathbf{E} \mu_{2r} = \sqrt{\frac{2}{\pi}} 2^{n/2} \begin{cases} (1+o(1)) & \text{при } r = o(2^{n/2}), \\ e^{-\alpha} (1+o(1)) & \text{при } r = \alpha 2^{n/2}, 0 < c_1 \leq \alpha \leq c_2 < \infty; \end{cases} \quad (19)$$

$$\begin{aligned} \mathbf{D} \mu_{2r} &= \mathbf{D} \mu_{-2r} = \\ &= \frac{1}{2^{2^n-n}} \binom{2^n}{2^{n-1}+r} \left[1 - \binom{2^n}{2^{n-1}+r} \frac{1}{2^{2^n}} \right] + \\ &+ 2^n (2^n - 1) \left[\binom{2^{n-1}}{2^{n-2}} \binom{2^{n-1}}{2^{n-2}+r} \frac{1}{2^{2^n}} - \binom{2^n}{2^{n-1}+r}^2 \frac{1}{2^{2^{n+1}}} \right], \end{aligned} \quad (21)$$

$$\mathbf{D} \mu_{2r} = \frac{2^{n+1}}{\pi} (1+o(1)) \quad \text{при } r = o(2^{2n/3}); \quad (22)$$

$$\begin{aligned}
\text{cov}(\mu_{2l}, \mu_{2s}) &= \\
&= 2^n(2^n - 1) \binom{2^{n-1}}{2^{n-2} + \frac{l+s}{2}} \binom{2^{n-1}}{2^{n-2} + \frac{l-s}{2}} \frac{1}{2^{2^n}} - \\
&\quad - 2^{2n} \binom{2^n}{2^{n-1} + l} \binom{2^n}{2^{n-1} + s} \frac{1}{2^{2^{n+1}}} \quad \text{при } l \neq s,
\end{aligned} \tag{23}$$

при фиксированных l, s

$$\text{cov}(\mu_{2l}, \mu_{2s}) \approx \begin{cases} \frac{2^{n+1}}{\pi}, & \text{если четности } l \text{ и } s \text{ одинаковы,} \\ -\frac{2^{n+1}}{\pi}, & \text{если четности } l \text{ и } s \text{ различны.} \end{cases} \tag{24}$$

Доказательство. Учитывая четность и симметрию спектральных коэффициентов, из (6) и (16) убеждаемся в справедливости формулы (18). Из формулы (18) видно, что эти средние монотонно убывают с ростом $|r|$ и что наибольшее среднее имеет величина μ_0 .

Соотношения (19) и (20) выводятся из (18) применением формулы Стирлинга и соответствующих разложений в ней (рутинные выкладки мы опускаем).

Для исследования вторых моментов введем индикаторы $I_{ir} = I\{\hat{w}_{ni} = 2r\}$. Имеем:

$$\mathbf{D} \mu_{2r} = \mathbf{D} \sum_{i=0}^{2^n-1} I_{ir} = \sum_i \mathbf{D} I_{ir} + \sum_{i \neq j} \text{cov}(I_{ir}, I_{jr}) =$$

$$= 2^n \mathbf{D} I_{0r} + 2^n(2^{n-1} - 1) \text{cov}(I_{0r}, I_{1r}).$$

Здесь (см. (16))

$$\begin{aligned}
\mathbf{D} I_{0r} &= \mathbf{P}\{\hat{w}_{n0} = 2r\} (1 - \mathbf{P}\{\hat{w}_{n0} = 2r\}) = \\
&= \binom{2^n}{2^{n-1} + r} \left(1 - \binom{2^n}{2^{n-1} + r} \frac{1}{2^{2^n}}\right) \frac{1}{2^{2^n}},
\end{aligned}$$

$$\begin{aligned}
\text{cov}(I_{0r}, I_{1r}) &= \mathbf{E} I_{0r} I_{1r} - \mathbf{E} I_{0r} \mathbf{E} I_{1r} = \\
&= \mathbf{P}\{\hat{w}_{n0} = 2r, \hat{w}_{n1} = 2r\} - \mathbf{P}^2\{\hat{w}_{n0} = 2r\} = \\
&= \binom{2^{n-1}}{2^{n-2} + r} \binom{2^{n-1}}{2^{n-2} + r} \frac{1}{2^{2^n}} - \left(\binom{2^n}{2^{n-1} + r}\right)^2 \frac{1}{2^{2^{n+1}}}.
\end{aligned}$$

В итоге получаем представление (21) для дисперсии.

Асимптотический анализ формулы (21) проводится аналогично анализу формулы (18) и в итоге дает соотношение (22).

Исследование смешанных моментов проводится аналогично исследованию дисперсии:

$$\begin{aligned} \text{cov}(\mu_{2l}, \mu_{2s}) &= \\ &= \text{cov}\left(\sum_{i=0}^{2^n} I_{il}, \sum_{j=0}^{2^n} I_{js}\right) = \sum_{i,j=0}^{2^n} \text{cov}(I_{il}, I_{js}) = \\ &= \sum_{i,j=0}^{2^n} [\mathbf{P}\{\hat{w}_{ni}=2l, \hat{w}_{nj}=2s\} - \mathbf{P}\{\hat{w}_{ni}=2l\} \mathbf{P}\{\hat{w}_{nj}=2s\}] = \\ &= 2^n(2^n-1) \mathbf{P}\{\hat{w}_{n0}=2l, \hat{w}_{nl}=2s\} - 2^{2n} \mathbf{P}\{\hat{w}_{n0}=2l\} \mathbf{P}\{\hat{w}_{nl}=2s\}, \end{aligned}$$

что и влечет за собой (23).

Асимптотическая формула (24) получается из (23) с помощью тех же рассуждений, что использованы выше. $\square$

Замечание 2. Случайная величина μ_0 изучалась в [7], где для ее моментов любого фиксированного порядка $r = 1, 2, \dots$ получено асимптотическое выражение

$$\mathbf{E} \mu_0^r \approx \frac{1}{2} \left(\frac{2^{n+3}}{\pi} \right)^{r/2}, \quad n \rightarrow \infty,$$

согласующееся с (19) и (22) и означающее, что нормированная величина

$$\hat{\mu}_0(n) = \sqrt{\frac{\pi}{2^{n+3}}} \mu_0$$

имеет в пределе равновероятное распределение Бернулли.

4. Подвекторы спектра и их структура

Более содержательные заключения можно сделать, если рассматривать не весь спектр Уолша (4), а его отрезки — подвекторы

$$\hat{\mathbf{w}}_n^{(k)} = (\hat{w}_{n0}, \hat{w}_{n1}, \dots, \hat{w}_{n,2^k-1}), \quad \hat{\mathbf{w}}_n^{(n)} = \hat{\mathbf{w}}_n, \quad (25)$$

— и для них изучать не элементы структуры, а *интервальные характеристики структуры*

$$\mu_{nk}(a, b) = \sum_{i=0}^{2^k-1} I\{a < \hat{w}_{ni} < b\}. \quad (26)$$

Аналогичные характеристики $w_n^{(k)}$ и $\mu'_{nk}(a, b)$ определяются и для спектра Фурье (2). Как показано в [3, теорема 3], для подвекторов $\mathbf{w}_n^{(k)}$ имеет место представление $\mathbf{w}_n^{(k)} = \boldsymbol{\eta}_n^{(k)} H_k$, где вектор $\boldsymbol{\eta}_n^{(k)} = (\eta_{n0}, \eta_{n1}, \dots, \eta_{n,2^k-1})$ состоит из независимых в совокупности биномиальных $\text{Bi}(2^{n-k}, \frac{1}{2})$ компонент, а H_k есть $(2^k \times 2^k)$ -матрица Сильвестра–Адамара. Свойства этих матриц подробно описаны в литературе (см., например, [1, с. 396] и [3]).

Нетрудно проверить, что аналогичное представление для подвекторов (25), в силу связи (5), имеет следующий вид:

$$\widehat{\mathbf{w}}_n^{(k)} = 2 \overline{\boldsymbol{\eta}}_n^{(k)} H_k, \quad (27)$$

где вектор $\overline{\boldsymbol{\eta}}_n^{(k)} = (\overline{\eta}_{n0}, \overline{\eta}_{n1}, \dots, \overline{\eta}_{n,2^k-1})$ состоит из независимых в совокупности симметризованных биномиальных $\text{Bis}(2^{n-k-1}, \frac{1}{2})$ компонент (см. выше комментарий к теореме 1).

Представление (27) позволяет сделать следующий важный вывод, дополняющий теорему 2.

Теорема 3. Пусть $n \rightarrow \infty$, а k — фиксированный параметр. Тогда компоненты вектора $2^{-n/2} \widehat{\mathbf{w}}_n^{(k)}$ асимптотически независимы и асимптотически нормальны с параметрами $(0, 1)$.

Доказательство основано на том, что в указанных в теореме условиях компоненты вектора $\overline{\boldsymbol{\eta}}_n^{(k)}$ асимптотически нормальны с центром в нуле, а преобразование (27) ортогонально (при ортогональном преобразовании центрированных случайных величин свойства нормальности и независимости, как известно, сохраняются). $\square$

Из теоремы 3 сразу же следует ответ на вопрос об асимптотическом поведении величин $\mu_{nk}(a, b)$, определенных в (26). Действительно, если в (26) положить $a = \alpha 2^{n/2}$, $b = \beta 2^{n/2}$, где α и β ($\alpha < \beta$) — фиксированные числа, то в условиях этой теоремы индикаторы в (26) будут асимптотически независимыми одинаково распределенными величинами, средние значения которых будут стремиться к $\Phi(\beta) - \Phi(\alpha)$, где Φ — функция стандартного нормального распределения. Таким образом, справедливо следующее утверждение.

Теорема 4. Пусть $n \rightarrow \infty$, а k — фиксированный параметр. Тогда случайная величина $\mu_{nk}(\alpha 2^{n/2}, \beta 2^{n/2})$, $\alpha < \beta$, асимптотически имеет биномиальное распределение $\text{Bi}(2^k, p)$, где $p = \Phi(\beta) - \Phi(\alpha)$.

В заключение выражаем благодарность О. В. Денисову за внимательное прочтение рукописи и замечания, способствовавшие улучшению изложения содержания работы.

Список литературы

- [1] Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, 2-е изд., М.: МЦНМО, 2004, 385 с.
- [2] Глухов М. М., Шишков А. Б., *Математическая логика. Дискретные функции. Теория алгоритмов*, СПб.: Лань, 2012, 416 с.
- [3] Ивченко Г. И., Медведев Ю. И., “Спектр случайной булевой функции и его производящая функция”, *Матем. вопросы криптографии*, **2:2** (2011), 41–54.
- [4] Таранников Ю. В. О корреляционно-иммунных и устойчивых булевых функциях. In: “*Матем. вопросы кибернетики*” /под общ. ред. О. Б. Лупанова, 2002, 91–148.
- [5] Zhang Xian-Mo, Zheng Yuliang, “GAC — the criterion for global avalanche characteristics of cryptographic functions”, *J. Univ. Comput. Sci.*, **1:5** (1995), 320–327.
- [6] Canteaut A., Carlet C., Charpin P., Fontaine C., “On cryptographic properties of the cosets of $R(1, m)$ ”, *IEEE Trans. Inform. Theory*, **IT-47:4** (2001), 1494–1513.
- [7] Рязанов Б. В., “О распределении спектральной сложности булевых функций”, *Дискретн. матем.*, **6:2** (1994), 111–119.
- [8] Логачев О. А., Сальников А. П., Ященко В. В., *Булевы функции в теории кодирования и криптографии*, 2-е изд., М.: МЦНМО, 2004, 470 с.