МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2012 Т. 3 № 3 С. 21–34

УДК: 519.212.2

Стохастические булевы функции и их спектры

Г. И. Ивченко, Ю. И. Медведев

Академия криптографии Российской Федерации, Москва

Получено 20.V.2011

Предлагается общая вероятностная модель для булевых функций от n переменных, задаваемая произвольной вероятностной мерой на множестве всех таких функций. Выводится характеристическая функция спектра Уолша случайной функции и находятся точные и асимптотические (при $n \to \infty$) распределения некоторых его характеристик для случая параметрической меры.

Ключевые слова: булева функция, преобразование Уолша, спектр функции, характеристическая функция, параметрическая мера, спектральные характеристики, предельные теоремы

Stochastic Boolean functions and their spectra

G. I. Ivchenko, Yu. I. Medvedev

Academy of Cryptography of the Russian Federation, Moscow

Abstract. General probabilistic model for Boolean functions of n variables with arbitrary probabilistic measure on the set of such functions is proposed. The characteristic function of Walsh spectrum of random function is defined and exact and asymptotic distributions of some spectrum characteristics for $n \to \infty$ are obtained in the parametric measure case.

Key words: Boolean function, Walsh transform, spectrum of function, characteristic function, parametric measure, spectrum characteristics, limit theorems

Citation: *Mathematical Aspects of Cryptography*, 2012, vol. 3, no. 3, pp. 21–34 (Russian).

§ 1. Введение

Пусть $V_n = \{v_0, v_1, \ldots, v_{2^n-1}\}$ — n-мерное векторное пространство над полем из двух элементов, векторы которого упорядочены по возрастанию соответствующих им чисел, где $v_i = (v_{1i}, v_{2i}, \ldots, v_{ni})$ отвечает двоичному представлению числа $i = \{0, 1, \ldots, 2^n - 1\}$:

$$i = v_{1i}2^{n-1} + v_{2i}2^{n-2} + \ldots + v_{n-1,i}2 + v_{ni}.$$

Пусть, далее, $f : V_n \to \{0, 1\}$ — булева функция от n переменных и $F_n = \{f\}$ — множество всех таких функций. Любую булеву функцию можно записать в виде вектора

$$f_n = \big(f(v_0), f(v_1), \ldots, f(v_{2^n-1})\big) \equiv \big(f_{n0}, f_{n1}, \ldots, f_{n,2^n-1}\big), \tag{1}$$

называемого ее *таблицей истинности*.

Символом $\|f\|$ будем обозначать *вес* функции f (число единичных компонент вектора (1)); скалярное произведение векторов $a = (a_1, \ldots, a_n)$ и $b = (b_1, \ldots, b_n)$ из V_n вычисляется по формуле

$$(a, b) = a_1b_1 \oplus \ldots \oplus a_nb_n$$

($\oplus$ — знак сложения по $\mathrm{mod}\ 2$).

Целочисленная функция $w_f : V_n \to R$, определяемая соотношением

$$w_f(u) = \sum_{x \in V_n} f(x)\,(-1)^{(u,x)}, u \in V_n, \tag{2}$$

называется *преобразованием Уолша* булевой функции f; величина $w_{ni} = w_f(v_i)$ называется *спектральным коэффициентом функции f, отвечающим вектору* v_i, а совокупность всех этих величин — вектор

$$w_n = \big(w_{n0}, w_{n1}, \ldots, w_{n,2^n-1}\big) \tag{3}$$

— называется *спектром Уолша* (или просто *спектром*) функции f.

Известно, что функция f однозначно определяется своим спектром по *формуле обращения*

$$f(x) = 2^{-n} \sum_{u \in V_n} w_f(u)\,(-1)^{(u,x)}, \quad x \in V_n. \tag{4}$$

Далее, введем матрицы $H_0 = (1)$, $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ и вообще

$$H_k = \begin{pmatrix} H_{k-1} & H_{k-1} \\ H_{k-1} & -H_{k-1} \end{pmatrix} = H_1 \otimes H_{k-1}, \quad k \geq 2 \tag{5}$$

($\otimes$ — знак кронекеровского произведения). Матрицы такого вида называются *матрицами Сильвестра – Адамара* [1, с. 396]. Отметим некоторые их свойства, необходимые нам в дальнейшем. Они симметричны: $H_n' = H_n$ (здесь и далее «штрих» означает транспонирование), удовлетворяют условию ортогональности $H_n H_n = 2^n I_{2^n}$ (I_r — единичная матрица порядка r), откуда следует, что $H_n^{-1} = 2^{-n} H_n$; наконец, имеют место представления

$$H_n = \left((-1)^{(v_i, v_j)}\right) = \left(l_0', l_1', \ldots, l_{2^n-1}'\right), \tag{6}$$

где вектор-строка

$$l_j = \left((-1)^{(v_j, v_0)}, (-1)^{(v_j, v_1)}, \ldots, (-1)^{(v_j, v_{2^n-1})}\right)$$

есть $(+1, -1)$-последовательность для линейной функции

$$l_j(x) = (v_j, x), \quad x \in V_n;$$

при этом

$$\sum_{j=0}^{2^n-1} (-1)^{(v_j, v_i)} = \begin{cases} 2^n & \text{при} \quad i = 0, \\ 0 & \text{при} \quad i > 0 \end{cases} \tag{7}$$

(в строках и столбцах матрицы H_n, за исключением первых строки и столбца, одинаковое число «1» и «-1»).

В терминах матриц Сильвестра – Адамара преобразование Уолша (2) и формула обращения (4) могут быть записаны в виде

$$w_n = f_n H_n, \quad f_n = 2^{-n} w_n H_n. \tag{8}$$

Дальнейшие детали этой темы можно найти, например, в монографии [1, гл. 9].

Булевы функции широко используются в реальных криптографических системах, и потому они являются популярным объектом систематического и всестороннего математического и криптографического анализа. Соответствующая литература огромна, и она частично отражена в обзорах [2, 3].

Объект нашего интереса — спектр (3) булевой функции: многие криптографические свойства булевой функции выражаются именно в терминах ее спектральных характеристик. В последние годы для исследования спектра (3) весьма эффективно применяется вероятностный подход, когда на множестве $F_n = \{f\}$ вводится равномерная мера, приписывающая каждой функции этого множества вес $|F_n|^{-1} = 2^{-2^n}$. В этом случае компоненты вектора (таблицы истинности) f_n, определенного в (1), становятся независимыми бернуллиевскими случайными величинами с равновероятными значениями, а спектр (3) случайно выбранной функции — случайным вектором, и для исследования различных его особенностей «в среднем» успешно применяются методы теории вероятностей, в особенности ее предельные теоремы, позволяющие устанавливать полезные асимптотические (при $n \to \infty$) оценки для различных характеристик спектра.

Вместе с тем следует отметить, что вероятностная модель с равномерной мерой на всем множестве $F_n = \{f\}$ не всегда адекватна реальным ситуациям. Например, такая модель не позволяет анализировать ситуации, когда класс используемых булевых функций представляет собой то или иное подмножество множества F_n или когда компоненты вектора f_n принимают значения 0 и 1 с неодинаковыми вероятностями. Мы предлагаем общую вероятностную модель для булевых функций, в рамках которой выводится характеристическая функция для спектра Уолша случайной функции, и находим точные и асимптотические (при $n \to \infty$) распределения различных характеристик спектра в следующей *параметрической модели*: компоненты вектора f_n являются независимыми и одинаково распределенными бернуллиевскими случайными величинами с произвольным распределением $\mathbf{P}\left(f_{nj} = 1\right) = 1 - \mathbf{P}\left(f_{nj} = 0\right) = p$, $0 < p < 1$. О такой модели мы будем далее говорить кратко как о p-модели.

§ 2. Характеристическая функция спектра случайной булевой функции

Зададим на множестве $F_n = \{f\}$ вероятностную меру, приписывающую каждой функции этого множества вес $P(f)$, и пусть

$$\varphi_n(t) = \mathbf{E}e^{itf_n'}, \quad t = (t_0, t_1, \ldots, t_{2^n-1}),$$

есть соответствующая характеристическая функция (вектор f_n определен в (1), $tf_n' = \sum t_j f_{nj}$ — обычное скалярное произведение векторов, это

обозначение используется везде далее):

$$\varphi_n(t) = \sum_{f \in F_n} e^{itf'_n} P(f). \tag{9}$$

Тогда с учетом (8) и (5) для характеристической функции случайного спектра w_n (см. (3)) будем иметь:

$$\Phi_n(t) = \mathbf{E} e^{itw'_n} = \mathbf{E} \exp\left\{i(tH_n) f'_n\right\} = \varphi_n(tH_n) = \varphi_n\left(tl'_0, tl'_1, \ldots, tl'_{2^n-1}\right). \tag{10}$$

Соотношениями (9) и (10) задается общая конструкция вероятностной модели на множестве всех булевых функций $F_n = \{f\}$, позволяющая, в принципе, проводить анализ спектра w_n для различных конкретных вариантов задания меры $P(f)$. Основная проблема при этом — нахождение характеристической функции (9).

Рассмотрим для иллюстрации простейший случай, когда мера $P(f)$ — равномерная:

$$P(f) = 2^{-2^n} \quad \text{для всех} \quad f \in F_n.$$

Тогда

$$\varphi_n(t) = \prod_{j=0}^{2^n-1} \mathbf{E} e^{it_j f_{nj}} = 2^{-2^n} \prod_{j=0}^{2^n-1} \left(1 + e^{it_j}\right),$$

и характеристическая функция спектра (10) принимает вид

$$\Phi_n(t) = 2^{-2^n} \prod_{j=0}^{2^n-1} \left(1 + e^{itl'_j}\right). \tag{11}$$

Этот случай и был до сих пор объектом рассмотрения в литературе, посвященной случайным булевым функциям (соответствующую библиографию см. в [4]).

Настоящая работа посвящена детальному анализу следующей параметрической модели: пусть мера $P(f)$ такова, что компоненты вектора (таблицы истинности) f_n, определенного в (1), являются независимыми и одинаково распределенными бернуллиевскими случайными величинами с распределением

$$\mathbf{P}\left(f_{nj} = 1\right) = p, \quad \mathbf{P}\left(f_{nj} = 0\right) = q, \quad p + q = 1. \tag{12}$$

В такой p-модели характеристическая функция $\varphi_n(t)$ принимает вид (см. (9))

$$\varphi_n(t) = \prod_{j=0}^{2^n-1} \mathbf{E} e^{it_j \hat{f}_{nj}} = \prod_{j=0}^{2^n-1} \left(q + pe^{it_j}\right),$$

а характеристическая функция спектра (10) — вид

$$\Phi_n(t) = \prod_{j=0}^{2^n-1} \left(q + pe^{itl'_j}\right), \tag{13}$$

где векторы l_j определены в (6).

Это представление является основой для анализа распределений различных характеристик спектра в $p-$модели, чему посвящены следующие разделы.

Замечание. Эквивалентным образом параметрическую модель (12) можно определить и так: каждой функции $f \in F_n$ приписывается вес, пропорциональный $\theta^{\|f\|}$, где $\theta > 0$ — параметр меры. Именно:

$$P(f) = \theta^{\|f\|} (1+\theta)^{-2^n}.$$

Эти два распределения совпадают, если $\theta = \dfrac{p}{q}$.

§ 3. Распределения спектральных коэффициентов

Перейдем теперь к вопросу о распределениях различных спектральных характеристик в рассматриваемой параметрической модели, и прежде всего установим одно важное свойство спектра в p-модели, обобщающее представление (8).

Введем следующую систему *спектральных подвекторов*:

$$w_n^{(k)} = (w_{n0}, w_{n1}, \ldots, w_{n,2^k-1}), \quad k = 1, 2, \ldots, n, w_n^{(n)} = w_n. \tag{14}$$

Имеет место следующее утверждение о структуре этих подвекторов (везде далее равенство случайных векторов понимается как равенство их распределений).

Теорема 1. *В p-модели для любого* $k = 1, 2, \ldots, n$ *справедливо представление*

$$w_n^{(k)} = \eta_n^{(k)} H_k, \tag{15}$$

где вектор $\eta_n^{(k)} = \left(\eta_{n0}, \eta_{n1}, \ldots, \eta_{n,2^k-1}\right)$ *состоит из независимых и одинаково распределенных компонент, имеющих биномиальное распределение* $\mathrm{Bi}\left(2^{n-k}, p\right)$.

Доказательство. Характеристическая функция вектора $w_n^{(k)}$ получается из (13) при $t_r = 0$ для $r \geq 2^k$ и имеет вид

$$\Phi_{nk}\left(t_0, \ldots, t_{2^k-1}\right) = \prod_{j=0}^{2^n-1} \left(q + pe^{it^{(k)} l_j^{(k)\prime}}\right), \tag{16}$$

где $t^{(k)} = \left(t_0, \ldots, t_{2^k-1}\right)$, а вектор $l_j^{(k)}$ составлен из первых 2^k компонент вектора l_j.

Векторы $l_j^{(k)}$, $j = 0, 1, \ldots, 2^k - 1$, составляют главный минор (подматрицу) H_k в матрице H_n, как это следует из структуры матриц Сильвестра – Адамара. Более того, если рассмотреть в матрице H_n первые 2^k строк, то эта часть матрицы H_n будет представлять собой последовательное повторение минора H_k, т. е. она имеет вид $(H_k H_k \ldots H_k)$. Отсюда следует, что все произведение в (16) представляет собой 2^{n-k} повторений произведения первых 2^k сомножителей, таким образом,

$$\Phi_{nk}\left(t^{(k)}\right) = \prod_{j=0}^{2^k-1} \left(q + pe^{it^{(k)} l_j^{(k)\prime}}\right)^{2^{n-k}}. \tag{17}$$

В свою очередь, как легко видеть, правая часть (17) представляет собой характеристическую функцию случайного вектора $\eta_n^{(k)} H_k$ (надо повторить те же рассуждения, что и в (10)). Это и доказывает представление (15). Теорема доказана.

Следующее утверждение о моментах спектра является простым следствием теоремы 1, известных соотношений для первых и вторых моментов случайных векторов при их линейных преобразованиях:

$$\mathbf{E} w_n^{(k)} = \left(\mathbf{E}\eta_n^{(k)}\right) H_k, \quad \mathbf{D} w_n^{(k)} = H_k \left(\mathbf{D}\eta_n^{(k)}\right) H_k,$$

свойств матриц Сильвестра – Адамара и очевидных формул:

$$\mathbf{E}\eta_n^{(k)} = 2^{n-k} p l_0^{(k)}, \quad \mathbf{D}\eta_n^{(k)} = 2^{n-k} pq I_{2^k}.$$

Теорема 2. *В p-модели для любого* $k = 1, 2, \ldots, n$ *справедливы соотношения*

$$\mathbf{E}w_n^{(k)} = (2^n p, 0, \ldots, 0), \quad \mathbf{D}w_n^{(k)} = 2^n pq I_{2^k}. \tag{18}$$

Таким образом, в рассматриваемой модели спектральные коэффициенты некоррелированы и, за исключением первого коэффициента $w_{n0} = \|f\|$, центрированы.

В качестве еще одного следствия теоремы 1 получим распределения некоторых линейных функционалов от спектра. Простейшими функционалами от спектра w_n являются линейные комбинации спектральных коэффициентов

$$L_n(c) = cw_n' = \sum_{j=0}^{2^n-1} c_j w_{nj}, \quad c = (c_0, c_1, \ldots, c_{2^n-1}). \tag{19}$$

Характеристическая функция произвольного линейного функционала имеет представление (см. (13))

$$\mathbf{E}e^{i\tau L_n(c)} = \mathbf{E}e^{i\tau cw_n'} = \Phi_n(\tau c) = \prod_{j=0}^{2^n-1} \left(q + pe^{i\tau c l_j'}\right). \tag{20}$$

Эта, вообще говоря, весьма сложная формула значительно упрощается при выборе коэффициентов c в виде $c = l_r$, $r = 0, 1, \ldots, 2^n - 1$, поскольку

$$l_r l_j' = \begin{cases} 2^n & \text{при } r = j, \\ 0 & \text{при } r \neq j. \end{cases}$$

Таким образом, из (20) следует, что

$$\mathbf{E}e^{i\tau L_n(l_r)} = q + pe^{i\tau 2^n}.$$

В итоге мы имеем следующее утверждение.

Теорема 3. *В p-модели для любого* $r, 0 \le r \le 2^n - 1$, *линейный функционал* $L_n(l_r) = l_r w_n'$ *имеет двухточечное распределение вида*

$$\mathbf{P}(L_n(l_r) = 0) = q, \quad \mathbf{P}(L_n(l_r) = 2^n) = p; \tag{21}$$

при этом

$$\mathbf{E}L_n(l_r) = 2^n p, \quad \mathbf{D}L_n(l_r) = 2^{2n} pq.$$

Добавим к этому результату некоторые комментарии. Двухточечность распределений рассматриваемых функционалов непосредственно следует из представления (8), так как всегда

$$L'_n \equiv (L_n(l_0), \ldots, L_n(l_{2^n-1}))' = H_n w'_n = H_n H'_n f'_n = 2^n f'_n, \tag{22}$$

то есть сумма $l_r w'_{\mathrm{n}}$ принимает лишь значения 0 и 2^n, а соответствующие вероятности уже зависят от выбора модели. В целом же распределение вектора $2^{-n}L_n$, определенного в (22), всегда совпадает с распределением вектора (таблицы истинности) f_n.

Выделим еще частный случай (сумма всех спектральных коэффициентов)

$$L_n(l_0) = \sum_{j=0}^{2^n-1} w_{nj}.$$

В этой сумме первое слагаемое $w_{n0} = \|f\|$, очевидно, имеет биномиальное распределение $\mathrm{Bi}(2^n, p)$. Таким образом, сумма остальных слагаемых имеет двухточечное распределение вида

$$\mathbf{P}\left(\sum_{j=1}^{2^n-1} w_{nj} = 2^n - k \,|\, w_{n0} = k\right) = 1 - \mathbf{P}\left(\sum_{j=1}^{2^n-1} w_{nj} = -k \,|\, w_{n0} = k\right) = p.$$

Еще один тип линейных функционалов, распределения которых могут быть точно описаны, представляют собой частичные суммы

$$S_{nk} = \sum_{j=0}^{2^k-1} w_{nj}, k = 1, 2, \ldots, n. \tag{23}$$

Теорема 4. *В p-модели случайные величины* $2^{-k}S_{nk}$ *имеют биномиальные распределения* $\mathrm{Bi}\left(2^{n-k}, p\right)$.

Доказательство следует из цепочки соотношений (см. (15) и доказательство теоремы 1)

$$S_{nk} = l_0^{(k)} w_n^{(k)\prime} = l_0^{(k)} H_k \eta_n^{(k)\prime} = \left(2^k, 0, \ldots, 0\right) \eta_n^{(k)\prime} = 2^k \eta_{n0}.$$

§ 4. Распределения спектральных коэффициентов (продолжение)

Перейдем теперь к более детальному анализу распределений спектральных коэффициентов. Хотя в представлении (15) и заложен общий ответ о виде их различных совместных распределений, все же интересно получить явный вид хотя бы одномерных и двумерных распределений. Ответ на этот вопрос дается в нижеследующей теореме 5 в терминах *симметризованного биномиального распределения* $\mathrm{Bis}\,(N,p)$, введенного и описанного в [4]. Напомним, что так называется распределение разности $\xi_N^- = \xi_{N1} - \xi_{N2}$ независимых случайных величин, имеющих одно и то же биномиальное распределение $\mathrm{Bi}\,(N,p)$:

$$p_N(u) = \mathbf{P}\left(\xi_N^- = u\right) = \sum_{r=0}^{N-u} C_N^r C_N^{r+u} p^{2r+u} q^{2N-2r-u}, \quad 0 \le u \le N, \qquad p_N(-u) = p_N(u)\,. \tag{24}$$

Общий результат об одномерных и двумерных распределениях спектральных коэффициентов формулируется следующим образом.

Теорема 5. *В p-модели справедливы следующие утверждения:*

1) *спектральный коэффициент* $w_{n0} = \|f\|$ *имеет распределение* $\mathrm{Bi}\,(2^n,p)$*;*

2) *коэффициенты* w_{nj}*,* $j = 1,2,\ldots,2^n-1$*, имеют одно и то же распределение* $\mathrm{Bis}\left(2^{n-1},p\right)$*;*

3) *распределение любой пары* $\left(w_{n0},w_{nj}\right)$*,* $j \ge 1$*, задается вероятностями*

$$\mathbf{P}\left(w_{n0}=u, w_{nj}=v\right) = C_{2^{n-1}}^{\frac{u+v}{2}} C_{2^{n-1}}^{\frac{u-v}{2}} p^u q^{2^n-u}, \quad (u,v) \in T_n, \tag{25}$$

где носитель имеет вид

$$T_n = \left\{(u,v) : 0 \le u \le 2^n, -2^{n-1} \le v \le 2^{n-1}, |v| \le u, u \equiv v \bmod 2\right\};$$

4) *распределение любой пары* $\left(w_{ni},w_{nj}\right)$*,* $1 \le i < j \le 2^n-1$*, совпадает с распределением пары* $\left(\xi^-_{2^{n-2},1} + \xi^-_{2^{n-2},2}, \xi^-_{2^{n-2},1} - \xi^-_{2^{n-2},2}\right)$*, где случайные величины* $\xi^-_{2^{n-2},i}$*,* $i = 1,2$*, независимы и каждая имеет распределение* $\mathrm{Bis}\left(2^{n-2},p\right)$*, при этом* (*см.* (24))

$$\mathbf{P}\left(w_{ni}=u, w_{nj}=v\right) = p_{2^{n-2}}\left(\frac{u+v}{2}\right) p_{2^{n-2}}\left(\frac{u-v}{2}\right), \quad u \equiv v\ (\mathrm{mod}2)\,. \tag{26}$$

Доказательство исходит из представлений $w_{nj} = f_n l'_j$, $j = 0, 1, \ldots, 2^n - 1$, и заключается в прямом использовании отмеченных во введении свойств матриц Сильвестра – Адамара. Первое утверждение непосредственно следует из определения модели.

Второе утверждение — также очевидное следствие представления (8) и свойства (7), так как выражение $w_{nj} = f_n l'_j$ при $j \geq 1$ распадается на разность двух независимых сумм, состоящих из 2^{n-1} независимых бернуллиевских слагаемых каждая, т. е.

$$w_{nj} = \xi_{2^{n-1},1} - \xi_{2^{n-1},2}.$$

Если к этому добавить очевидное представление

$$w_{n0} = \xi_{2^{n-1},1} + \xi_{2^{n-1},2},$$

то мы получаем утверждение 3; формула (25) следует при этом из равенства

$$\mathbf{P}\left(w_{n0} = u, w_{nj} = v\right) = \mathbf{P}\left(\xi_{2^{n-1},1} = \frac{u+v}{2}\right)\mathbf{P}\left(\xi_{2^{n-1},2} = \frac{u-v}{2}\right).$$

Рассмотрим, наконец, произвольную пару $\left(w_{ni}, w_{nj}\right) = \left(f_n l'_i, f_n l'_j\right)$ в утверждении 4). В силу свойства ортогональности векторов l_i и l_j, среди пар $\left(l_{ik}, l_{jk}\right)$ каждый из видов $(1,1)$, $(1,-1)$, $(-1,1)$, $(-1,-1)$ встречается ровно 2^{n-2} раз. В соответствии с этим, каждая из сумм разбивается на четыре независимых слагаемых (подсуммы):

$$\begin{aligned} f_n l'_i &= \sum\nolimits_{(1,1)} + \sum\nolimits_{(1,-1)} - \sum\nolimits_{(-1,1)} - \sum\nolimits_{(-1,-1)}, \\ f_n l'_j &= \sum\nolimits_{(1,1)} - \sum\nolimits_{(1,-1)} + \sum\nolimits_{(-1,1)} - \sum\nolimits_{(-1,-1)}, \end{aligned} \tag{27}$$

где обозначено

$$\sum\nolimits_{(\beta_1,\beta_2)} = \sum_{r:\,\left(l_{ir},l_{jr}\right)=(\beta_1,\beta_2)} f_{nr}, \quad \beta_1, \beta_2 = \pm 1.$$

При этом каждая из этих подсумм представляет собой биномиальную случайную величину с распределением $\mathrm{Bi}\left(2^{n-2}, p\right)$.

Полагая теперь

$$\begin{aligned} \xi^{-}_{2^{n-2},1} &= \sum\nolimits_{(1,1)} - \sum\nolimits_{(-1,-1)}, \\ \xi^{-}_{2^{n-2},2} &= \sum\nolimits_{(1,-1)} - \sum\nolimits_{(-1,1)}, \end{aligned}$$

можно переписать соотношения (27) в виде

$$f_n l'_i = \xi^-_{2^{n-2},1} + \xi^-_{2^{n-2},2},$$
$$f_n l'_j = \xi^-_{2^{n-2},1} - \xi^-_{2^{n-2},2}.$$

Тем самым первая часть утверждения 4 доказана.

Наконец, формула (26), с учетом соотношения (24), следует из равенства

$$\mathbf{P}\left(w_{ni} = u, w_{nj} = v\right) = \mathbf{P}\left(\xi^-_{2^{n-2},1} = \frac{u+v}{2}\right)\mathbf{P}\left(\xi^-_{2^{n-2},2} = \frac{u-v}{2}\right).$$

Теорема доказана.

Добавим к этой теореме еще и достаточно очевидный асимптотический результат. Из указанной в теореме структуры как отдельных спектральных коэффициентов, так и их пар, очевидно, что при $n \to \infty$ соответствующие двумерные распределения асимптотически нормальны с параметрами, данными в (18), следовательно, ввиду некоррелированности, спектральные коэффициенты попарно асимптотически независимы.

Более того, в представлении (15) вектор $\eta_n^{(k)} = \left(\eta_{n0}, \eta_{n1}, \ldots, \eta_{n,2^k-1}\right)$ при $n \to \infty$, $k = \text{const}$, асимптотически нормален; поскольку он состоит из независимых и одинаково распределенных компонент, а при ортогональном преобразовании H_k свойства нормальности и независимости сохраняются, то вектор $w_n^{(k)} = \left(w_{n0}, w_{n1}, \ldots, w_{n,2^k-1}\right)$ имеет асимптотически независимые и нормальные компоненты.

Таким образом, в отличие от точных распределений, которые уже в двумерном случае оказались весьма сложно устроенными, асимптотические (при $n \to \infty$) распределения спектральных коэффициентов являются достаточно простыми.

Отметим также, что при $n - k \to \infty$ частичные суммы, определенные в (23), также асимптотически нормальны, как это следует из теоремы 4. В то же время полная сумма S_{nn} устроена совсем иначе (см. теорему 3).

§ 5. Схема серий

Рассмотрим, наконец, схему серий, когда при $n \to \infty$ параметр $p = p(n) \to 0$ так, что

$$2^n p \to \lambda, \quad 0 < \lambda < \infty. \tag{28}$$

В этом случае к биномиальному распределению $\mathrm{Bi}\,(2^n, p)$ применима пуассоновская аппроксимация, в силу которой спектральный коэффициент $w_{n0} = \|f\|$ (см. теорему 5, п. 1) имеет в пределе распределение Пуассона $\Pi\,(\lambda)$.

Предельные распределения других спектральных коэффициентов также легко вывести из теоремы 5, и они будут, очевидно, выражаться через распределения сумм и разностей независимых пуассоновских случайных величин. Чтобы сформулировать соответствующие результаты, введем, по аналогии с предыдущим разделом, понятие симметризованного пуассоновского распределения.

Будем через $\eta_i(\lambda)$, $i = 1, 2$, обозначать независимые случайные величины, имеющие одно и то же распределение Пуассона $\Pi(\lambda)$. Как известно, их сумма $\eta^+(\lambda) = \eta_1(\lambda) + \eta_2(\lambda)$ имеет распределение $\Pi(2\lambda)$. Распределение же их разности $\eta^-(\lambda) = \eta_1(\lambda) - \eta_2(\lambda)$ мы будем называть *симметризованным пуассоновским распределением* и обозначать символом $\mathrm{Ps}(\lambda)$. Это распределение симметрично, имеет среднее 0, дисперсию 2λ и является предельным (при условии $Np \to \lambda$, $0 < \lambda < \infty$) для симметризованного биномиального распределения $\mathrm{Bis}(N, p)$. Соответствующие же вероятности легко выписываются с помощью формулы полной вероятности и имеют вид

$$\pi_j^-(\lambda) = \mathbf{P}\{\eta^-(\lambda) = j\} = e^{-2\lambda} \sum_{r=0}^{\infty} \frac{\lambda^{j+2r}}{r!\,(|j|+r)!} = \\ = e^{-2\lambda} I_{|j|}(2\lambda), \quad j = 0, \pm 1, \pm 2, \ldots, \tag{29}$$

где $I_k(x)$ — *функция Бесселя порядка* $k \geq 0$ (она определяется этим соотношением, см. [5, гл. 2, § 7 и задачу 14]), поэтому это распределение иногда называют также *распределением Бесселя*.

Приведем еще вид характеристической функции этого распределения:

$$\mathbf{E}e^{it\eta^-(\lambda)} = \exp\left\{-4\lambda \sin^2 \frac{t}{2}\right\}.$$

Сформулируем теперь общий результат об одномерных и двумерных распределениях спектральных коэффициентов в схеме серий (28), являющийся аналогом теоремы 5.

Теорема 6. *В p-модели при выполнении условия* (28) *справедливы следующие утверждения:*

1) *спектральный коэффициент* $w_{n0} = \|f\|$ *имеет в пределе распределение Пуассона* $\Pi(\lambda)$*;*

2) *спектральные коэффициенты* $w_{nj}, j = 1, 2, \ldots, 2^n - 1$, *имеют в пределе одно и то же распределение* $\mathrm{Ps}\left(\frac{\lambda}{2}\right)$*;*

3) *предельное распределение любой пары* $\left(w_{n0}, w_{nj}\right)$, $j \geq 1$, *совпадает с распределением пары* $\left(\eta^{+}\left(\frac{\lambda}{2}\right), \eta^{-}\left(\frac{\lambda}{2}\right)\right)$ *и задается вероятностями*

$$\mathbf{P}\left(w_{n0}=u, w_{nj}=v\right)=\frac{\left(\frac{\lambda}{2}\right)^{u} e^{-\lambda}}{\left(\frac{u+v}{2}\right)!\left(\frac{u-v}{2}\right)!}, \quad (u,v)\in T_n,$$

где носитель имеет вид

$$T_n=\{(u,v): u=0,1,2,\ldots, v=0,\pm1,\pm2,\ldots, v\leq u, u\equiv v\,(\mathrm{mod}2)\};$$

4) *предельное распределение любой пары* $\left(w_{ni}, w_{nj}\right)$, $1\leq i<j\leq 2^n-1$, *совпадает с распределением пары* $\left(\eta_1^{-}\left(\frac{\lambda}{4}\right)+\eta_2^{-}\left(\frac{\lambda}{4}\right), \eta_1^{-}\left(\frac{\lambda}{4}\right)-\eta_2^{-}\left(\frac{\lambda}{4}\right)\right)$, *где случайные величины* $\eta_i^{-}\left(\frac{\lambda}{4}\right)$, $i=1,2$, *независимы и каждая имеет распределение* $\Pi\mathrm{s}\left(\frac{\lambda}{4}\right)$, *при этом* (*см.* (29))

$$\mathbf{P}\left(w_{ni}=u, w_{nj}=v\right)=\pi_{\frac{u+v}{2}}\left(\frac{\lambda}{4}\right)\pi_{\frac{u-v}{2}}\left(\frac{\lambda}{4}\right), \quad u\equiv v \pmod 2.$$

В заключение выражаем признательность А. М. Зубкову за ценные замечания, способствовавшие улучшению изложения содержания статьи.

Список литературы

1. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. 2-е изд. — М.: МЦНМО, 2004.
2. *Логачёв О. А., Сальников А. Л., Ященко В. В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004.
3. *Cusick Th. W., Stanica P.* Cryptographic Boolean functions and applications. — AP Elsevier, Amsterdam etc., 2009.
4. *Ивченко Г. И., Медведев Ю. И.* Спектр случайной булевой функции и его производящая функция. // Математические вопросы криптографии. — 2011. — Т. 2. Вып. 2. — С. 41–54.
5. *Феллер В.* Введение в теорию вероятностей и ее приложения. Т. 2. — М. : Мир, 1984.