МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2011 Т. 2 № 2 С. 41–54

УДК 519.212.2

Спектр случайной булевой функции и его производящая функция

Г. И. Ивченко, Ю. И. Медведев

Академия криптографии Российской Федерации, Москва

Получено 22.IV.2010

Исследуются свойства спектра случайной булевой функции от n переменных. Выводится совместная производящая функция элементов спектра и находятся точные и асимптотические (при $n \to \infty$) распределения различных характеристик спектра.

Ключевые слова: булева функция, преобразование Уолша, спектр функции, производящая функция, спектральные характеристики, предельные теоремы

Spectrum of random Boolean function and its generating function

G. I. Ivchenko, Yu. I. Medvedev

Academy of Cryptography of Russian Federation, Moscow

Abstract. Properties of spectrum of random Boolean function of n variables are investigated. Joint generating function of spectrum elements is defined and exact and asymptotic distributions of some spectrum characteristics for $n \to \infty$ are obtained.

Key words: Boolean function, Walch transform, spectrum of function, generating function of spectrum, spectrum characteristics, limit theorems

Citation: *Mathematical Aspects of Cryptography*, 2011, vol. 2, no. 2, pp. 41–54 (Russian).

§ 1. Введение

Пусть $V_n = \{v_0,\ v_1,...,v_{2^n-1}\}$ — n-мерное векторное пространство над полем из двух элементов, векторы которого упорядочены лексикографически.

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

$$f_n = \left(f(v_0), f(v_1),..., f\left(v_{2^n-1}\right)\right), \tag{1}$$

называемого таблицей истинности функции f.

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, т. е. вектор

$$w_n = \left(w_{n0}, w_{n1},..., w_{n,2^n-1}\right), \tag{3}$$

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

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

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

($\oplus$ — знак сложения по mod 2).

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

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

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

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

($\otimes$ — знак кронекеровского произведения). Матрицы такого вида называются *матрицами Сильвестра–Адамара* [1, с. 396]. Отметим некоторые их свойства, необходимые нам в дальнейшем. Они симметричны — $H_n' = H_n$, 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

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

где штрих обозначает транспонирование, вектор-строка

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

соответствует линейной функции

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

при этом

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

(в строках и столбцах матрицы $\mathrm{H_n}$, за исключением первых, одинаковое число «1» и «-1»).

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

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

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

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 достаточно полно отражена в обзорах

[2–5]. Объект нашего интереса – спектр (3) булевой функции: многие криптографические свойства булевой функции выражаются именно в терминах её 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 $|F_n|^{-1} = 2^{-2^n}$. Тогда спектр случайно выбранной функции становится случайным вектором, и для исследования различных его особенностей «в среднем» успешно применяются методы теории вероятностей, в особенности её предельные теоремы, позволяющие устанавливать полезные асимптотические (при $n \to \infty$) оценки для различных характеристик спектра. В настоящей работе, в рамках такого подхода, мы получаем общую производящую функцию случайного спектра, с помощью которой эффективно решаются различные задачи анализа структуры спектра булевой функции.

2. Основная теорема

Условимся о некоторых дополнительных обозначениях. Для двух векторов $a = (a_1,...,a_k)$ и $b = (b_1,...,b_k)$ с действительными компонентами будем писать

$$a \times b = (a_1 b_1,...,a_k b_k),$$
$$a/b = (a_1/b_1,...,a_k/b_k), \ (b \neq 0),$$
$$a^b = a_1^{b_1} ... \, a_k^{b_k},$$

и пусть

$$F_n(z) = \mathbf{E} z^{w_n} = \mathbf{E} \prod_{j=0}^{2^n-1} z_j^{w_{nj}}, \quad z = (z_0, z_1, ..., z_{2^n-1}),$$

есть производящая функция случайного спектра (3).

Теорема 1. *Если случайная булева фукнция* $f_n : V_n \to \{0,1\}$ *имеет равномерное распределение на множестве всех* 2^{2^n} *таких функций, то производящая фукнция её спектра имеет вид*

$$F_n(z) = 2^{-2^n} \prod_{j=0}^{2^n-1} \left(1 + z^{l_j}\right), \tag{9}$$

где векторы l_j *определены в* (6). *Функция* $F_n(z)$ *удовлетворяет рекуррентному соотношению*

$$F_n(z) = F_{n-1}\left(z^{(1)} \times z^{(2)}\right)\, F_{n-1}\left(z^{(1)} / z^{(2)}\right), \quad n \geq 2, \tag{10}$$

где $z^{(1)} = \left(z_0, z_1, ..., z_{2^{n-1}-1}\right)$, $z^{(2)} = \left(z_{2^{n-1}}, z_{2^{n-1}+1}, ..., z_{2^n-1}\right)$

и $F_1(z_0, z_1) = U(z_0 z_1)\, U\left(z_0 z_1^{-1}\right)$, $U(z) = \dfrac{1}{2}(1+z)$. (11)

Доказательство. Для случайной функции f, выбираемой равновероятно из множества $F_n = \{f\}$, компоненты вектора (1) являются, как известно, независимыми бернуллиевскими случайными величинами, принимающими значения 0 и 1 с равными вероятностями. Следовательно, характеристическая функция случайного вектора f_n имеет вид

$$\phi_n(t) = \mathbf{E}e^{itf_n'} = \prod_{j=0}^{2^n-1} \mathbf{E}e^{it_j f(v_j)} = \prod_{j=0}^{2^n-1} U\left(e^{it_j}\right),$$

где $t = \left(t_0, t_1, ..., t_{2^n-1}\right)$ и функция $U(z)$ определена в (11). Отсюда, с учётом (7) и (6), для характеристической функции случайного спектра w_n имеем представление

$$\mathbf{\Phi}_n(t) = \mathbf{E}e^{itw_n'} = \mathbf{E}e^{i(tH_n)f_n'} = \phi_n(tH_n) = \prod_{j=0}^{2^n-1} U\left(e^{itl_j'}\right),$$

что эквивалентно (9).

Введём, далее, подвекторы $t^{(1)} = \left(t_0, t_1, ..., t_{2^{n-1}-1}\right)$, $t^{(2)} = \left(t_{2^{n-1}}, t_{2^{n-1}+1}, ..., t_{2^n-1}\right)$, тогда, воспользовавшись рекуррентой (5), можем записать цепочку соотношений

$$tH_n = \left(t^{(1)}, t^{(2)}\right)\begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix} = \left(\left(t^{(1)} + t^{(2)}\right)H_{n-1}, \left(t^{(1)} - t^{(2)}\right)H_{n-1}\right).$$

С учётом этого, вводя соответствующее разбиение $f_n = \left(f_n^{(1)}, f_n^{(2)}\right)$, получим:

$$\begin{aligned} \mathbf{\Phi}_n(t) &= \mathbf{E}\exp\left\{i\left(\left(t^{(1)} + t^{(2)}\right)H_{n-1}\right)f_n^{(1)\prime}\right\}\mathbf{E}\exp\left\{i\left(\left(t^{(1)} - t^{(2)}\right)H_{n-1}\right)f_n^{(2)\prime}\right\} = \\ &= \mathbf{\Phi}_{n-1}\left(t^{(1)} + t^{(2)}\right)\, \mathbf{\Phi}_{n-1}\left(t^{(1)} - t^{(2)}\right), \end{aligned} \tag{12}$$

поскольку подвекторы $f_n^{(1)}$ и $f_n^{(2)}$ независимы и имеют такое же распределение, как и вектор f_{n-1}. Переходя к производящим функциям (заменой e^{it_j} на z_j, $j=0,1,\ldots,2^n-1$), из (12) получаем (10). Наконец, формула (11) находится непосредственными вычислениями.

Теорема доказана.

ЗАМЕЧАНИЕ 1. Производящую функцию $F_n(z)$ можно представить и в другом, более наглядном, виде. Для этого заметим, что в представлении (9) каждый из сомножителей отвечает конкретной компоненте спектра (3) и, соответственно, конкретному вектору $u\in V_n$. Обозначим через $u_{i_1\ldots i_k}$ вектор $u\in V_n$, имеющий единицы на местах $1\le i_1<i_2<\ldots<i_k\le n$ и нули — на остальных местах; аналогично обозначим соответствующие спектральные коэффициенты $w_{i_1\ldots i_k}$ и соответствующие им переменные $z_{i_1\ldots i_k}$. Тогда в этих обозначениях для производящей функции $F_n(z)$ имеет место следующее представление:

$$2^{2^n}F_n(z)=z_0^{-2^{n-1}}\prod_{\beta_i=\pm1,i=1,\ldots,n}\left(1+z_0\prod_{k=1}^{n}\prod_{1\le i_1<\ldots<i_k\le n}z_{i_1\ldots i_k}^{\beta_{i_1}\ldots\beta_{i_k}}\right).$$

В частности,

$$2^2F_1(z_0,z_1)=z_0^{-1}\prod_{\beta_1\pm1}\left(1+z_0z_1^{\beta_1}\right),$$

$$2^4F_2(z_0,z_1,z_2,z_{12})=z_0^{-2}\prod_{\beta_1,\beta_2=\pm1}\left(1+z_0z_1^{\beta_1}z_2^{\beta_2}z_{12}^{\beta_1\beta_2}\right),$$

$$2^8F_3(z)=z_0^{-4}\prod_{\beta_1,\beta_2,\beta_3=\pm1}\left(1+z_0z_1^{\beta_1}z_2^{\beta_2}z_3^{\beta_3}z_{12}^{\beta_1\beta_2}z_{13}^{\beta_1\beta_3}z_{23}^{\beta_2\beta_3}z_{123}^{\beta_1\beta_2\beta_3}\right).$$

Такая форма записи производящей функции может представлять интерес в тех случаях, когда требуется провести анализ спектра при заданных весах векторов $u\in V_n$. Так, полагая здесь $z_{i_1\ldots i_k}=1$ для всех k, превышающих фиксированное значение m, получим производящую функцию тех коэффициентов $w_f(u)$, для которых вес вектора $u\in V_n$ не превышает m. Такая производящая функция может оказаться полезной при изучении корреляционно-иммунных булевых функций заданного порядка m, поскольку их спектральные коэффициенты равны нулю для всех векторов u с весами, не превосходящими m.

ЗАМЕЧАНИЕ 2. Из совместной производящей функции $F_n(z)$ можно получать производящие функции для тех или иных подмножеств булевых функций. Так, для подмножеств булевых функций с чётными и нечётными весами (обозначим соответствующие производящие функции $F_n'(z)$ и $F_n''(z)$ имеем:

$$F_n'(z) = \frac{1}{2}\left(F_n(z_0, z_1, ..., z_{12...n}) + F_n(-z_0, z_1, ..., z_{12...n})\right),$$

$$F_n''(z) = \frac{1}{2}\left(F_n(z_0, z_1, ..., z_{12...n}) - F_n(-z_0, z_1, ..., z_{12...n})\right).$$

ЗАМЕЧАНИЕ 3. Коэффициенты разложения производящей функции $F_n(z)$ по степеням аргумента z_0

$$F_n(z) = \sum_{k=-2^{n-1}}^{2^{n-1}} z_0^k \; V_k(z_1, ..., z_{12...n})$$

обладают следующими свойствами:

$$V_{-k}(z_1, ..., z_{12...n}) = V_k\left(z_1^{-1}, ..., z_{12...n}^{-1}\right), \quad k = 0,1,...,2^{n\text{-}1},$$

$$V_{-2^{n-1}} = V_{2^{n-1}} = 1.$$

Хорошо известно, что при исследовании структур различных комбинаторных объектов сложной природы (подстановки, отображения и разбиения конечных множеств, многочлены над конечными полями и т. д.) весьма эффективным оказывается аппарат производящих функций, и полученные нами представления (9)–(11), несмотря на кажущуюся громоздкость этих формул, открывают, на наш взгляд, новые возможности для решения интересных задач анализа случайного спектра. Ниже это будет продемонстрировано на ряде соответствующих примеров. Но прежде мы добавим ещё один общий результат, весьма просто вычислив с помощью представления (8) первые и вторые моменты спектра w_n.

Теорема 2. *Если выполнены условия теоремы 1, то*

$$\mathbf{E}w_n = \left(2^{n-1}, 0, ..., 0\right), \quad \mathbf{D}w_n = 2^{n-2} I_{2^n}. \tag{13}$$

Таким образом, компоненты спектра некоррелированы и, за исключением первой компоненты, центрированы.

Доказательство. Для первой компоненты $w_{n0} = \|f\|$ результат следует из того, что эта случайная величина имеет, очевидно, биномиальное распределение $\mathrm{Bi}\left(2^n, \frac{1}{2}\right)$.

В целом же формулы (13) следуют из соотношений

$$Ew_n = \left(Ef_n\right) H_n,$$

$$Dw_n = H_n \left(Df_n\right) H_n$$

и приведённых во введении свойств матриц Сильвестра–Адамара. Теорема доказана.

3. Дальнейшие результаты

1. *Спектральные подвекторы*. Положив в (10) $z^{(2)} = 1$, получим соотношение

$$F_n\left(z^{(1)}, 1\right) = F_{n-1}^2\left(z^{(1)}\right), \tag{14}$$

которое означает, что спектральный подвектор

$$w_n^{(n-1)} = \left(w_{n0}, w_{n1}, ..., w_{n,2^{n-1}-1}\right)$$

спектра w_n имеет такое же распределение, как сумма двух независимых копий спектра $w_{n-1} = f_{n-1}H_{n-1}$. Таким образом, можно записать, что

$$w_n^{(n-1)} = \eta_n^{(n-1)} H_{n-1},$$

где вектор $\eta_n^{(n-1)} = \left(\eta_{n0}, \eta_{n1}, ..., \eta_{n,2^{n-1}-1}\right)$ есть сумма двух независимых копий случайного вектора f_{n-1}, и тем самым его компоненты являются независимыми в совокупности биномиальными $\mathrm{Bi}\left(2, \frac{1}{2}\right)$ случайными величинами (здесь и далее равенство случайных величин понимается как равенство их распределений).

Аналогично, из (14) и рекурренты (10) следует соотношение

$$F_n\left(z_0, z_1, ..., z_{2^{n-2}-1}, 1, ..., 1\right) = F_{n-1}^2\left(z_0, z_1, ..., z_{2^{n-2}-1}, 1, ..., 1\right) =$$

$$= F_{n-2}^{2^2}\left(z_0, z_1, ..., z_{2^{n-2}-1}\right),$$

откуда, как и выше, вытекает представление спектрального подвектора

$$w_n^{(n-2)} = \left(w_{n0}, w_{n1}, ..., w_{n,2^{n-2}-1}\right)$$

в виде

$$w_n^{(n-2)} = \eta_n^{(n-2)} H_{n-2},$$

где случайный вектор $\eta_n^{(n-2)} = \left(\eta_{n0}, \eta_{n1}, ..., \eta_{n,2^{n-2}-1}\right)$ состоит из независимых в совокупности биномиальных $\mathrm{Bi}\left(2^2, \frac{1}{2}\right)$ компонент.

Этот процесс «спуска» можно продолжить, и общий результат формулируется в виде следующего утверждения.

Теорема 3. *Если выполнены условия теоремы 1, то для любого* $k = 1, 2, \ldots, n$ *спектральный подвектор*

$$w_n^{(k)} = \left(w_{n0}, w_{n1}, ..., w_{n,2^k-1} \right), \quad w_n^{(n)} = w_n, \tag{15}$$

можно представить в виде

$$w_n^{(k)} = \eta_n^{(k)} H_k, \tag{16}$$

где вектор $\eta_n^{(k)} = \left(\eta_{n0}, \eta_{n1}, ..., \eta_{n,2^k-1} \right)$ *состоит из независимых в совокупности биномиальных* $\mathrm{Bi}\left(2^{n-k}, \frac{1}{2} \right)$ *компонент, так что при* $k = n$ (16) *сводится к* (8).

2. *Распределения частичных сумм спектральных коэффициентов.* В качестве простого следствия теоремы 3 находятся распределения частичных сумм

$$S_{nk} = \sum_{i=0}^{2^k-1} w_{ni}, \; k = 1, 2, ..., n. \tag{17}$$

Пусть $\mathcal{L}(S)$ обозначает закон распределения S.

Теорема 4. *Если выполнены условия теоремы* 1, *то*

$$\mathcal{L}\left(2^{-k} S_{nk} \right) = \mathrm{Bi}\left(2^{n-k}, \frac{1}{2} \right), \tag{18}$$

$$\mathbf{E} S_{nk} = 2^{n-1}, \; \mathbf{D} S_{nk} = 2^{n+k-2}.$$

В частности, сумма S_{nn} *всех коэффициентов спектра* w_n *принимает лишь два значения:* 2^n *и* 0 *с равными вероятностями.*

Доказательство следует из цепочки соотношений (см. (16))

$$S_{nk} = 1 w_n^{(k)'} = 1 H_k \eta_n^{(k)'} = \left(2^k, 0, ..., 0 \right) \eta_n^{(k)'} = 2^k \eta_{n0},$$

в которой 1 обозначает 2^k-мерный вектор, все координаты которого равны 1.

Замечание. Для суммы квадратов всех спектральных коэффициентов имеем

$$\sum_{i=0}^{2^n-1} w_{ni}^2 = w_n w_n' = f_n H_n H_n f_n' = 2^n f_n f_n' = 2^n \| f \|.$$

Конечно, это является хорошо известным свойством преобразования Уолша [2].

3. *Распределения спектральных коэффициентов.* Перейдём теперь к более детальному анализу распределений спектральных коэффициентов. Хотя в представлении (16) и заложен общий ответ о виде их различных совместных распределений, всё же интересно получить явный вид хотя бы одномерных и двумерных распределений. Ответ на этот вопрос даётся в нижеследующей теореме 5, в терминах симметризованного биномиального распределения, с определения которого мы и начинаем эту тему.

В этом разделе через $\xi_{Ni}, i=1,2,$ обозначаются независимые случайные величины, имеющие одно и то же биномиальное распределение $\mathrm{Bi}(N,p)$. Как известно, их сумма $\xi_N^+ = \xi_{N1} + \xi_{N2}$ имеет биномиальное распределение $\mathrm{Bi}(2N,p)$. Распределение же их разности $\xi_N^- = \xi_{N1} - \xi_{N2}$ мы будем называть *симметризованным биномиальным распределением* и обозначать символом $\mathrm{Bis}(N,p)$. Это распределение симметрично, имеет среднее 0 и дисперсию $2Npq,\ q=1-p.$ Соответствующие же вероятности легко выписываются с помощью формулы полной вероятности и имеют вид

$$p_N(u) = \mathbf{P}\left(\xi_N^- = u\right) = \sum_{r=0}^{N-u} C_N^r C_N^{r+u} p^{2r+u} q^{2N-2r-u}, \quad 0 \le u \le N, \qquad p_N(-u) = p_N(u). \tag{19}$$

Приведём ещё вид соответствующей характеристической функции:

$$\mathbf{E}e^{it\xi_N^-} = \left(1 - 4pq\sin^2\frac{t}{2}\right)^N. \tag{20}$$

Сформулируем теперь общий результат об одномерных и двумерных распределениях спектральных коэффициентов.

Теорема 5. *Если выполнены условия теоремы* 1, *то*:

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

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

3) *распределение любой пары* $\left(w_{n0}, w_{nj}\right)$, $j \geq 1$, *совпадает с распределением пары* $\left(\xi^{+}_{2^{n-1}}, \xi^{-}_{2^{n-1}}\right)$ *с параметром* $p = \dfrac{1}{2}$ *и задаётся вероятностями*

$$\mathbf{P}\left(w_{n0} = u, w_{nj} = v\right) = 2^{-2^n} C_{2^{n-1}}^{\frac{u+v}{2}} C_{2^{n-1}}^{\frac{u-v}{2}}, \quad (u,v) \in T_n, \tag{21}$$

где носитель имеет вид

$$T_n = \left\{(u,v) : 0 \leq u \leq 2^n, |v| \leq \min\left\{u, \left|2^n - u\right|\right\}\right\};$$

4) *распределение любой пары* $\left(w_{ni}, w_{nj}\right)$, $1 \leq i < j \leq 2^n - 1$, *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* $\mathrm{Bis}\left(2^{n-2}, \dfrac{1}{2}\right)$, *при этом*

$$\mathbf{P}\left(w_{ni} = u, w_{nj} = v\right) = p_{2^{n-2}}\left(\frac{u+v}{2}\right) p_{2^{n-2}}\left(\frac{u-v}{2}\right) \tag{22}$$

(*см.* (19) *при значении* $p = 1/2$).

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, поэтому соответствующие технические детали мы опускаем.

Дополним эту теорему некоторыми комментариями. Поскольку $w_{n0} \geq w_{nj}$ и эти величины одинаковой чётности, распределение (21) можно записать и в таком виде:

$$\mathbf{P}\left(w_{n0} = l, w_{nj} = l - 2m\right) = \mathrm{bi}\left(l; 2^n, \frac{1}{2}\right) h\left(m; 2^{n-1}, 2^{n-1}, l\right),$$

где $\mathrm{bi}\left(l; N, p\right) = C_N^l p^l \left(1 - p\right)^{N-l}$ и $h\left(m; N_1, N_2, l\right) = C_{N_1}^m C_{N_2}^{l-m} \Big/ C_{N_1+N_2}^l$ — стандартные обозначения для биномиальных и гипергеометрических вероятностей с соответствующими параметрами.

Переписав в этих обозначениях формулу (21)

$$\mathbf{P}\left(w_{n0} = u, w_{nj} = v\right) = \mathrm{bi}\left(u; 2^n, \frac{1}{2}\right) h\left(\frac{u+v}{2}; 2^{n-1}, 2^{n-1}, u\right), \quad (u,v) \in T_n,$$

сразу находим условное распределение

$$\mathbf{P}\left(w_{nj}=v\,\middle|\,w_{n0}=u\right)=h\left(\frac{u+v}{2};2^{n-1},2^{n-1},u\right). \tag{23}$$

Отметим также симметрию распределения (23) относительно нуля.

Что касается распределения (22), то его также можно записать в явном виде через биномиальные и гипергеометрические вероятности (проверяется непосредственно):

$$\mathbf{P}\left(w_{ni}=u,w_{nj}=v\right)=$$
$$\sum_{r=0}^{2^{n-2}}\sum_{m=0}^{2^{n-2}}\mathrm{bi}\left(m;2^{n-2},\frac{1}{2}\right)\mathrm{bi}\left(r;2^{n-2},\frac{1}{2}\right)\mathrm{bi}\left(m+r+u;2^{n-1},\frac{1}{2}\right)h\left(r+\frac{u+v}{2};2^{n-2},2^{n-2},m+r+u\right).$$

Добавим к теореме 5 ещё и достаточно очевидный асимптотический результат. Из указанной в теореме структуры распределений как отдельных спектральных коэффициентов, так и их пар, следует, что при $n\to\infty$ эти распределения асимптотически нормальны с параметрами, данными в (13), следовательно, ввиду свойства некоррелированности компоненты предельных случайных векторов независимы.

Более того, в представлении (16) вектор $\eta_n^{(k)}=\left(\eta_{n0},\eta_{n1},...,\eta_{n,2^k-1}\right)$ при $n\to\infty$ и любом фиксированном k асимптотически нормален и его компоненты независимы и одинаково распределены; отсюда и из инвариантности сферически симметричных распределений относительно ортогонального преобразования H_k следует, что вектор $w_n^{(k)}=\left(w_{n0},w_{n1},...,w_{n,2^k-1}\right)$ имеет асимптотически независимые и нормальные компоненты.

ЗАМЕЧАНИЕ. В работах [6, 7] была доказана нормальная локальная предельная теорема для части спектра: совокупности тех спектральных коэффициентов (2), которые соответствуют векторам u веса $\|u\|\le k$ при фиксированном значении k, а в [8] этот результат расширен до значений $k=o\left(\sqrt{n}\right)$.

Таким образом, в отличие от точных распределений, которые уже в двумерном случае имеют весьма сложный вид, асимптотические (при $n\to\infty$) распределения спектральных коэффициентов оказываются достаточно простыми.

Отметим также, что при $n-k\to\infty$ частичные суммы, определённые в (17), также асимптотически нормальны с указанными в теореме 4 параметрами. В то же время полная сумма S_{nn} устроена совсем иначе (см. (18)).

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., Яценко 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. *Тарannиков Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях — Математические вопросы кибернетики. Вып. 11, 2002. С. 91—148.
5. *Кузнецов Ю. В., Шкарин С. А.* Коды Рида-Маллера (обзор публикаций) — Математические вопросы кибернетики. Вып. 6, 1996. С. 120—137.
6. *Рязанов Б. В.* О распределении спектральной сложности булевых функций — Дискретн. матем., 1994. Т. 6. № 2. С. 111–129.
7. *Рязанов Б. В., Чечёта С. И.* О приближении случайной булевой функции множеством квадратичных форм — Дискретн. матем., 1995. Т. 12. № 3. С. 129–145.
8. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции — Дискретн. матем., 2000. Т. 12. № 1. С. 82–95.