

УДК 519.7

Локальная предельная теорема для распределения части спектра случайной двоичной функции

© 2000 г. О.В. Денисов

Доказана локальная предельная теорема для распределения вектора растущей размерности, состоящего из некоторых спектральных коэффициентов случайной двоичной функции от n переменных. Исправлена ошибка, допущенная в асимптотической формуле для числа корреляционно-иммунных порядка k функций в одной из статей автора. Получена асимптотическая формула для числа $(n, 1, k)$ -устойчивых функций при $k = k(n) = o(\sqrt{n})$.

1. Введение

Пусть функция f выбирается случайно и равновероятно из множества V_n всех двоичных функций от n переменных. Это эквивалентно независимому равновероятному выбору ее значений $f(\alpha) \in \{0, 1\}$ для всех α из множества V_n двоичных векторов длины n . Для произвольного подмножества $I = \{i_1, \dots, i_{|I|}\}$ множества $\{1, \dots, n\}$ через w_I обозначим вес $\|f_{i_1, \dots, i_{|I|}}^{1, \dots, 1}\|$ подфункции $f_{i_1, \dots, i_{|I|}}^{1, \dots, 1}$ функции f , получаемой, если в функции f координаты с номерами $i_1, \dots, i_{|I|}$ положить равными единице. Таким же способом будем индексировать другие случайные величины (с. в.) и переменные, полагая, что I принимает значения подмножеств множества $\{1, \dots, n\}$ мощности от 0 до k . Если в формуле не указаны пределы изменения I , то подразумевается, что I принимает все значения из I в лексикографическом порядке.

Как в [1], определим случайный вектор (сл.в.)

$$\bar{w} = \bar{w}(f, n, k) = (w_I, 0 \leq |I| \leq k, I \subset \{1, \dots, n\})$$

длины

$$M = M(n, k) = \binom{n}{0} + \dots + \binom{n}{k}.$$

При $k = 1$ вектор \bar{w} можно представить как

$$\bar{w}(f, n, 1) = \sum_{x \in V_n} (1, x_1, \dots, x_n) f(x) = \left(\|f\|, \sum_{x \in f^{-1}(1)} (x_1, \dots, x_n) \right).$$

В таком виде он был введен в работе Чоу [6], в которой было доказано, что любая пороговая функция однозначно определяется этим вектором. С тех пор параметры Чоу являются одной из важнейших характеристик пороговых функций (см. [2]).

В [1] для произвольного фиксированного k был доказан ряд лемм, фактически определяющих предельное распределение \bar{w} , и получена асимптотическая формула для мощности класса $K(n, k)$ корреляционно-иммунных порядка k двоичных функций от n переменных. Как будет показано ниже, в результате ошибки автора в нее не был включен возникающий при $k \geq 2$ сомножитель

$$\left(1 + \sum_{i=2}^k (i-1)^2 \binom{n}{i}\right)^{-1/2}.$$

В данной статье по схеме, использовавшейся в [1], доказывается локальная предельная теорема (ЛПТ) для распределения \bar{w} при произвольном k , зависящем от n так, что $k(n) = o(\sqrt{n})$ при $n \rightarrow \infty$. Новые обозначения и идеи позволили существенно упростить формулировки и доказательства многих лемм. Из ЛПТ в качестве следствий выводятся асимптотические формулы для мощности класса $K(n, k)$ и класса

$$R(n, k) = K(n, k) \cap \{f \in B_n : \|f\| = 2^{n-1}\}$$

$(n, 1, k)$ -устойчивых функций, которые в двоичном случае представляют собой уравновешенные корреляционно-иммунные порядка k функции. Приближенные значения, вычисленные по этим формулам, сравниваются с точными значениями, найденными автором с помощью ЭВМ для $n = 4, 5, k = 1, 2$. Различные свойства корреляционно-иммунных и устойчивых функций изучались в ряде работ зарубежных авторов (см. обзор [3]).

Порядок корреляционной иммунности можно определить по вектору

$$\bar{F} = \bar{F}(f, n, k) = (F_I, 0 \leq |I| \leq k, I \subset \{1, \dots, n\}),$$

состоящему из первых (то есть соответствующих векторам веса от 0 до k) спектральных коэффициентов Фурье–Уолша–Адамара

$$\begin{aligned} F_I &= \frac{1}{2} \sum_{x \in V_n} (-1)^{f(x) + x_{i_1} + \dots + x_{i_{|I|}}} = 2^{n-1} - \|f(x) \oplus x_{i_1} \dots \oplus x_{i_{|I|}}\| \\ &= 2^{n-1} \text{Ind}\{I = \emptyset\} - \sum_{x \in V_n} (-1)^{x_{i_1} + \dots + x_{i_{|I|}}} f(x). \end{aligned}$$

Здесь $\text{Ind}(A)$ — индикатор события A .

ЛПТ для распределения фиксированного числа некоторых спектральных коэффициентов случайной двоичной функции была доказана в работах Б.В. Рязанова и С.И. Чечеты [4, 5]. В данной статье будет получена ЛПТ для распределения вектора \bar{F} экспоненциально растущей размерности $M(n, k)$.

2. ЛПТ для распределения вектора весов

В следующей теореме фактически утверждается, что распределение сл.в. \bar{w} можно приблизить плотностью соответствующего M -мерного нормального распределения. Здесь и далее $\exp_2 x = 2^x$, $\mathbf{E}\bar{w}$ — математическое ожидание сл.в. \bar{w} , Q^T — матрица, полученная транспонированием матрицы Q , $\det Q$ — определитель Q .

Теорема 1. Пусть $n \rightarrow \infty$, $k(n) = o(\sqrt{n})$, $Q = Q(n, k)$ — ковариационная матрица с.в. $(\bar{w} - \mathbf{E}\bar{w})/2^{n/2-1}$, $\bar{z}(n)2^{n/2-1}$ — последовательность целочисленных векторов размерности $M(n, k)$. Тогда равномерно относительно \bar{z}

$$\begin{aligned} \mathbf{P}\{\bar{w} = \mathbf{E}\bar{w} + \bar{z}(n)2^{n/2-1}\} &= \frac{\exp(-(1/2)\bar{z}^T Q^{-1}\bar{z}) + O(n^{5k+4}/2^n)}{(2^{n/2-1})^M \sqrt{(2\pi)^M \det Q}} \\ &= \frac{\exp(-(1/2)\sum_I (2^{|I|} z_I - \sum_{i \in I} 2^{|I|-1} z_{I \setminus \{i\}})^2) + O(n^{5k+4}/2^n)}{\exp_2 \left(\binom{n}{k} (n-k)/2 + M(n, k) \log_2 \sqrt{\pi/2} \right)}. \end{aligned}$$

Доказательство. Очевидно, что

$$\begin{aligned} w_I &= \sum_{\alpha \in V_n} \beta_I(\alpha) f(\alpha), \\ \mathbf{E}w_I &= 2^{n-1-|I|}, \\ w_I - \mathbf{E}w_I &= \sum_{\alpha \in V_n} \beta_I(\alpha) (f(\alpha) - 1/2), \end{aligned}$$

где $\beta_I(\alpha) = \alpha_{i_1} \dots \alpha_{i_{|I|}}$ (при $I = \emptyset$ считаем, что $\beta_I(\alpha) \equiv 1$). Тогда для векторов

$$\beta(\alpha) = (\beta_I(\alpha), 0 \leq |I| \leq k), \quad \xi(\alpha) = \beta(\alpha)(f(\alpha) - 1/2), \quad \xi = \bar{w} - \mathbf{E}\bar{w}$$

справедливо соотношение

$$\xi = \sum_{\alpha \in V_n} \xi(\alpha).$$

Характеристические функции случайных векторов $\beta(\alpha)$ и ξ равны соответственно

$$\varphi_\alpha(t) = \cos(\beta(\alpha), t/2), \quad \varphi_\xi(t) = \prod_{\alpha \in V_n} \varphi_\alpha(t),$$

где (x, y) — скалярное произведение векторов x, y . Умножив равенство

$$\varphi_\xi(t) = \sum_{a \in Z^M} \mathbf{P}(\xi = a) \exp(-i(t, a))$$

на $\exp(-i(t, z2^{n/2-1}))$ и проинтегрировав его по переменным t_I , $0 \leq |I| \leq k$, в пределах от $-\pi$ до π , находим, что

$$(2\pi)^M \mathbf{P}(\xi = z2^{n/2-1}) = \int_{-\pi}^{\pi} \dots \int_{-\pi}^{\pi} \varphi_\xi(t) \exp(-i(t, z2^{n/2-1})) dt.$$

Делая замену $x = t2^{n/2-1}$ и обозначая через G гиперкуб $[-2^{n/2}\pi/2, 2^{n/2}\pi/2]^M$, получаем, что

$$(\pi 2^{n/2})^M \mathbf{P}(\xi = z2^{n/2-1}) = \int_G \varphi_\xi(x/2^{n/2-1}) \exp(-i(x, z)) dx, \quad (1)$$

$$\varphi_\xi(x/2^{n/2-1}) = \prod_{\alpha} \cos(\beta(\alpha), x/2^{n/2}). \quad (2)$$

Для $i = 0, 1, \dots, k$ определим функцию

$$\Psi(n, i) = \left(\binom{n}{i} 2^{n/3+ki} \right)^{-1}$$

и разобьем G на попарно не пересекающиеся области

$$G_i = \{x \in G: \exists I: |I| = i, |x_I/2^{n/2}| > \Psi(n, |I|); \forall I: |I| \geq i + 1, |x_I/2^{n/2}| \leq \Psi(n, |I|)\},$$

$$G^* = G \setminus \left(\bigcup_{i=0}^k G_i \right) = \{x \in G: |x_I/2^{n/2}| \leq \Psi(n, |I|), 0 \leq |I| \leq k\}.$$

Далее доказательство разобьем на леммы, дающие оценки $\varphi_\xi(x/2^{n/2-1})$ во введенных областях. В следующей лемме и везде далее все неравенства выполняются начиная с некоторого n_0 .

Лемма 1. Если $x \in G_i$ для некоторого $i \in \{0, 1, \dots, k\}$, то не менее чем для 2^{n-i} векторов α из V_n выполняется неравенство

$$|\varphi_\alpha(x/2^{n/2-1})| \leq 1 - (\Psi(n, i)/2^{k+i+1})^2.$$

Доказательство. Если для $y = x/2^{n/2}$ справедливо равенство

$$(\beta(\alpha), y) = \rho(\alpha) + \pi t(\alpha),$$

где $|\rho(\alpha)| \leq \pi/2$, $t(\alpha)$ — целое число, то

$$|\varphi_\alpha(x/2^{n/2-1})| = |\cos(\beta(\alpha), y)| = \cos \rho(\alpha) \leq 1 - (\rho(\alpha)/2)^2.$$

Без ограничения общности можно считать, что $|y_I| > \Psi(n, i)$ для $I = \{1, \dots, i\}$. Разобьем V_n на 2^{n-i} групп векторов с одинаковыми последними $n-i$ координатами. Достаточно доказать, что в группе с произвольным вектором γ последних $n-i$ координат найдется вектор α , для которого

$$|\rho(\alpha)| \geq \Psi(n, i)/2^{k+i}.$$

Рассмотрим величины

$$p_0(\alpha_1, \dots, \alpha_i) = (\beta(\alpha_1, \dots, \alpha_i, \gamma), y) = \rho_0(\alpha_1, \dots, \alpha_i) + \pi t_0(\alpha_1, \dots, \alpha_i),$$

$$p_1(\alpha_2, \dots, \alpha_i) = \rho_0(1, \alpha_2, \dots, \alpha_i) - \rho_0(0, \alpha_2, \dots, \alpha_i),$$

...

$$p_i(\emptyset) = \rho_{i-1}(1) - \rho_{i-1}(0) = \rho_i(\cdot) + \pi t_i(\emptyset),$$

где $|\rho_j(\cdot)| \leq \pi/2$ и $t_j(\cdot)$ — целые числа для всех $j \in \{0, \dots, i\}$.

Предположим противное: пусть для всех $\alpha_1, \dots, \alpha_i$

$$|\rho_0(\alpha_1, \dots, \alpha_i)| < \Psi(n, i)/2^{k+i}.$$

С одной стороны, $\rho_i(\emptyset)$ есть линейная комбинация величин $\rho_0(\alpha_1, \dots, \alpha_i)$ с коэффициентами ± 1 , и тогда $|\rho_i(\emptyset)| < \Psi(n, i)/2^k$. С другой стороны,

$$\begin{aligned} p_1(\alpha_2, \dots, \alpha_i) &= \sum_I (\beta_I(1, \alpha_2, \dots, \alpha_i, \gamma) - \beta_I(0, \alpha_2, \dots, \alpha_i, \gamma)) y_I \\ &= \sum_{I \supset \{1\}} \beta_I(1, \alpha_2, \dots, \alpha_i, \gamma) y_I, \\ &\dots \\ p_i(\emptyset) &= \sum_{I \supset \{1, \dots, i\}} \beta_I(1, \dots, 1, \gamma) y_I \\ &\quad + y_{\{1, \dots, i\}} + \sum_{I \supset \{1, \dots, i\}, |I| > i} \beta_I(1, \dots, 1, \gamma) y_I. \end{aligned}$$

Поскольку $\Psi(n, i) < |y_{\{1, \dots, i\}}| < \pi/2$ и модуль последней суммы не превосходит величины

$$\begin{aligned} \sum_{j=1}^{k-i} \binom{n-i}{j} / \left(\binom{n}{i+j} 2^{-n/3-k(i+j)} \right) &\leq 2^{-n/3-ki} / \left(\binom{n}{i} 2^{-k} \sum_{j=1}^{k-i} \binom{i+j}{j} \right) \\ &\leq \Psi(n, i) 2^{-k} \sum_{j=1}^k k \binom{k}{j} \\ &= \Psi(n, i) (1 - 2^{-k}), \end{aligned}$$

справедлива оценка

$$\Psi(n, i) 2^{-k} < |p_i(\cdot)| \leq \pi/2 + \Psi(n, i) < \pi - \Psi(n, i)/2^k.$$

Следовательно, $|p_i(\emptyset)| > \Psi(n, i)/2^k$, что противоречит оценке, полученной из предположения. Лемма доказана.

Таким образом, для $x \in G_i$

$$\begin{aligned} |\varphi_\xi(x/2^{n/2-1})| &\leq \exp(-2^{n-i}(\Psi(n, i)/2^{k+i+1})^2) \\ &= \exp\left(-2^{n/3-2ki-3i-2} / \binom{n}{i}\right) \\ &\leq \exp\left(-2^{n/3-2k^2-5k-2} / \binom{n}{k}\right). \end{aligned}$$

Так как $k^2 = o(n)$, для всех $x \in G \setminus G^*$

$$|\varphi_\xi(x/2^{n/2-1})| \leq \exp(-2^{n/4}). \quad (3)$$

Лемма 2. Для $x \in G^*$ все величины $d_\alpha = (\beta(\alpha), x/2^{n/2})$ по модулю не превосходят $2^{1-n/3}$ и характеристическая функция может быть представлена в виде

$$\varphi_\xi(x/2^{n/2-1}) = \exp\left(-\frac{1}{2} x^T Q x (1 - \theta(x) \max_{\alpha \in V_n} d_\alpha^2)\right),$$

где Q — ковариационная матрица сл.в. $(\bar{w} - \mathbf{E}\bar{w})/2^{n/2-1}$, $0 \leq \theta(x) \leq 1/2$, и

$$x^T Q x = \sum_I \left(\sum_{J \supset I} x_J / 2^{|J|} \right)^2.$$

Доказательство. Очевидно, что

$$\begin{aligned} |d_\alpha| &\leq \sum_{i=0}^k \binom{n}{i} \Psi(n, i) \leq 2^{-n/3} (1 - 2^{-k}) \leq 2^{1-n/3}, \\ \cos d_\alpha &= 1 - d_\alpha^2/2 + \theta_1(x, \alpha) d_\alpha^4, \quad 0 \leq \theta_1(x, \alpha) \leq 1/4!. \end{aligned}$$

Отсюда,

$$\begin{aligned} \varphi_\alpha(x/2^{n/2-1}) &= \cos d_\alpha = \exp(\ln(1 - (d_\alpha^2/2 - \theta_1 d_\alpha^4))) \\ &= \exp\left(-d_\alpha^2/2 + \theta_1 d_\alpha^4 + \sum_{i=2}^{\infty} (d_\alpha^2/2 - \theta_1 d_\alpha^4)^i / i\right) \\ &= \exp(-d_\alpha^2/2 + \theta_2 d_\alpha^4) = \exp(-d_\alpha^2/2(1 - 2\theta_2 d_\alpha^2)), \end{aligned}$$

где $0 \leq \theta_2 = \theta_2(x, \alpha) \leq 1/4! + 1/(8((1 - d_\alpha^2/2))) < 1/4$. Далее,

$$\begin{aligned} \sum_\alpha d_\alpha^2/2 &= \sum_\alpha 2^{-n} \left(\sum_J \beta_J(\alpha) x_J \sum_K \beta_K(\alpha) x_K \right) \\ &= \sum_{J,K} x_J x_K / 2^{|J \cup K|} = \sum_{J,K} x_J x_K / 2^{|J|+|K|} \sum_{I \subset J \cap K} 1 \\ &= \sum_I \left(\sum_{J \supset I} x_J / 2^{|J|} \sum_{K \supset I} x_K / 2^{|K|} \right) = \sum_I \left(\sum_{J \supset I} x_J / 2^{|J|} \right)^2. \end{aligned}$$

Лемма доказана.

Из леммы 3 следует, что для всех $x \in G^*$

$$|\varphi_\xi(x/2^{n/2-1})| \leq \exp\left(-\frac{1 - 2^{n/3}}{2} x^T Q x\right). \quad (4)$$

Рассмотрим далее область

$$G^{**} = \{x \in G: |x_I| \leq 2^{|I|} \sqrt{n(n+1) \ln 4}, 0 \leq |I| \leq k\},$$

которая содержится в G^* . Для $x \in G^{**}$

$$\begin{aligned} d_\alpha^2(x) &\leq 2^{-n} \left(\sum_{i=0}^k \binom{n}{i} 2^{|I|} \sqrt{n(n+1) \ln 4} \right)^2 \\ &\leq 2^{-n} (M(n, k) 2^k O(n))^2 = O(n^{2k+2}/2^n), \\ x^T Q x &\leq \sum_{i=0}^k \binom{n}{i} \left(\sum_{t=0}^k \binom{n}{t} \sqrt{n(n+1) \ln 4} \right)^2 = O(n^{3k+2}). \end{aligned}$$

Здесь использованы оценки

$$M(n, k) / \binom{n}{k} - 1 = \sum_{i=0}^{k-1} \binom{n}{i} / \binom{n}{k} \leq k \binom{n}{k-1} / \binom{n}{k} = O(k^2/n) = o(1),$$

$$2^k \binom{n}{k} = O(n^k).$$

Следовательно, равномерно по $x \in G^*$

$$\begin{aligned} \varphi_\xi(x/2^{n/2-1}) &= \exp\left(-\frac{1}{2}x^T Q x\right) \exp(O(n^{5k+4}/2^n)) \\ &= \exp\left(-\frac{1}{2}x^T Q x\right) (1 + O(n^{5k+4}/2^n)). \end{aligned} \quad (5)$$

Лемма 3. *Справедливы равенства*

$$\begin{aligned} \det Q &= \exp_2\left(-2 \sum_{i=0}^k i \binom{n}{i}\right) = \exp_2\left((n-k) \binom{n}{k} - nM(n, k)\right), \\ z^T Q^{-1} z &= \sum_I (2^{|I|} z_I - \sum_{i \in I} 2^{|I|-1} z_{I \setminus \{i\}})^2. \end{aligned}$$

Доказательство. Положим

$$y_I = \sum_{J \supset I} x_J / 2^{|J|}.$$

Согласно лемме 3 для матрицы A перехода от x к y ($y = Ax$) справедливы равенства

$$x^T Q x = y^T (A^{-1})^T Q A^{-1} y = y^T y,$$

то есть

$$Q = A^T A, \quad Q^{-1} = A^{-1} (A^{-1})^T.$$

Элемент A_{IJ} равен $2^{-|J|}$, если $I \subset J$, и нулю в противном случае, поэтому A — верхнетреугольная матрица и

$$\det Q = (\det A)^2 = \exp_2\left(-2 \sum_{i=0}^k i \binom{n}{i}\right).$$

Для доказательства первого утверждения леммы остается заметить, что

$$\begin{aligned} M(n, k) &= \sum_{i=0}^k \left(\binom{n-1}{i-1} + \binom{n-1}{i} \right) = \sum_{i=0}^{k-1} \binom{n-1}{i} + \sum_{i=0}^k \binom{n-1}{i} \\ &= 2M(n-1, k-1) + \binom{n-1}{k}, \end{aligned}$$

$$\sum_{i=0}^k i \binom{n}{i} = nM(n-1, k-1), \quad n \binom{n-1}{k} = (n-k) \binom{n}{k}.$$

Чтобы найти A^{-1} , выразим x через y . При $|I| = k$ по определению $x_I/2^{|I|} = y_I$. Докажем индукцией по $|I|$ от $k - 1$ до 0 равенство

$$x_I/2^{|I|} = y_I - \sum_{i \notin I} y_{I \cup \{i\}}.$$

При $|I| = k - 1$ оно верно, так как

$$y_I = x_I/2^{k-1} + \sum_{i \notin I} x_{I \cup \{i\}}/2^k = x_I/2^{k-1} + \sum_{i \notin I} y_{I \cup \{i\}}.$$

Предположим, что равенство верно при $|I| = l + 1, \dots, k - 1$ и докажем его для $|I| = l$:

$$\begin{aligned} y_I &= x_I/2^l + \sum_{J \supset I, J \neq I} \left(y_J - \sum_{i \notin J} y_{J \cup \{i\}} \right) \\ &= x_I/2^l + \sum_{J \supset I, J \neq I} y_J - \sum_{K \supset I, |K| \geq |I|+2} y_K \\ &= x_I/2^l + \sum_{J \supset I, |J|=|I|+1} y_J. \end{aligned}$$

Таким образом,

$$(A^{-1})_{IJ} = \begin{cases} 2^{|I|}, & \text{если } I = J, \\ -2^{|I|}, & \text{если } J = I \cup \{i\}, i \notin I, \\ 0 & \text{в остальных случаях,} \end{cases}$$

$$((A^{-1})^T)_{IJ} = \begin{cases} 2^{|I|}, & \text{если } I = J, \\ -2^{|I|}, & \text{если } J = I \setminus \{i\}, i \in I, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Отсюда,

$$z^T Q^{-1} z = z^T A^{-1} (A^{-1})^T z = \sum_I \left(2^{|I|} z_I - \sum_{i \in I} 2^{|I|-1} z_{I \setminus \{i\}} \right)^2.$$

Лемма доказана.

Разобьем интеграл в (1) на сумму интегралов по областям $G \setminus G^*$, $G^* \setminus G^{**}$, G^{**} и обозначим их соответственно через J_1, J_2, J_3 . Из (2)–(3) следует, что

$$|J_1| \leq (\pi 2^{n/2})^M \exp(-2^{n/4}),$$

$$|J_2| \leq \sqrt{(2\pi)^M / \det((1 - 2^{1-n/3})Q)} \mathbf{P}(\eta \in G^* \setminus G^{**}),$$

где η — нормально распределенный вектор с параметрами $(\bar{0}, ((1 - 2^{1-n/3})Q)^{-1})$. Поскольку (см. доказательство леммы 4)

$$(Q^{-1})_{II} = \sum_I (A^{-1})_{IJ}^2 \leq 2^{2|I|} (1 + n - |I|),$$

справедливы оценки

$$\begin{aligned} \mathbf{P}(|\eta_I| > 2^{|I|} \sqrt{n+1} \sqrt{n \ln 4}) &\leq \frac{2}{\sqrt{2\pi}} \int_{\sqrt{n \ln 4(1-2^{1-n/3})}}^{\infty} \exp(-t^2/2) dt \\ &\leq \frac{2 \exp(-n \ln 2(1-2^{1-n/3}))}{\sqrt{2\pi n \ln 4(1-2^{1-n/3})}} = o(2^{-n}), \\ \mathbf{P}(\eta \in G^* \setminus G^{**}) &\leq \sum_I \mathbf{P}(|\eta_I| > 2^{|I|} \sqrt{(n+1)n \ln 4}) = o(n^k/2^n). \end{aligned}$$

Учитывая, что

$$\det((1-2^{1-n/3})Q) = (1-2^{1-n/3})^M \det Q = (1+o(1)) \det Q,$$

получаем оценку

$$|J_2| = \sqrt{(2\pi)^M / \det Q} O(n^k/2^n). \quad (6)$$

Согласно (4),

$$J_3 = J_4 - J_5 + J_6,$$

где аналогично оценке J_2

$$\begin{aligned} J_4 &= \int_{R^M} \exp\left(-\frac{1}{2}x^T Q x\right) \exp(-i(x, z)) dx = \sqrt{(2\pi)^M / \det Q} \exp\left(-\frac{1}{2}z^T Q^{-1}z\right), \\ J_5 &= \int_{R^M \setminus G^{**}} \exp\left(-\frac{1}{2}x^T Q x\right) \exp(-i(x, z)) dx = \sqrt{(2\pi)^M / \det Q} O(n^k/2^n) \end{aligned}$$

и

$$J_6 = \int_{G^{**}} \exp\left(-\frac{1}{2}x^T Q x\right) O(n^{5k+4}/2^n) dx = \sqrt{(2\pi)^M / \det Q} O(n^{5k+4}/2^n).$$

Из этих оценок, формул (1), (5), (6) и леммы 4 находим, что

$$\begin{aligned} (\pi 2^{n/2})^M \mathbf{P}(\xi = z 2^{n/2-1}) &= \sqrt{(2\pi)^M / \det Q} \left(\exp\left(-\frac{1}{2}z^T Q^{-1}z\right) \right. \\ &\quad \left. + O(n^k/2^n) + O(n^{5k+4}/2^n) \right) + (\pi 2^{n/2})^M \exp(-2^{n/4}) \\ &= \frac{\exp(-(1/2)\bar{z}^T Q^{-1}\bar{z}) + O(n^{5k+4}/2^n)}{\exp_2\left(\binom{n}{k}(n-k)/2 - nM/2 - M/2 \log_2 2\pi\right)}. \end{aligned}$$

Теорема 1 доказана.

Согласно формуле (1) работы [1], критерием принадлежности функции f классу $K(n, k)$ является условие

$$\exists r \in \{-2^{n-k-1}, \dots, 2^{n-k-1}\}: \forall 0 \leq |I| \leq k \quad w_I = \mathbf{E}w_I + r 2^{k-|I|}. \quad (7)$$

Поэтому

$$\frac{|R(n, k)|}{|B_n|} = \mathbf{P}\{f \in R(n, k)\} = \mathbf{P}\{\bar{w} = \mathbf{E}\bar{w}\}$$

и справедлива следующая асимптотическая формула для числа $(n, 1, k)$ -устойчивых функций.

Следствие 1. Если $n \rightarrow \infty$ и $k(n) = o(\sqrt{n})$, то

$$|R(n, k)| \sim \exp_2 \left(2^n - \frac{n-k}{2} \binom{n}{k} - M(n, k) \log_2 \sqrt{\pi/2} \right).$$

Согласно (7)

$$\mathbf{P}\{f \in K(n, k)\} = \sum_{r=-2^{n-k-1}}^{2^{n-k-1}} \mathbf{P}\{\bar{w} = r\bar{z}2^{n/2-1}\}, \quad (8)$$

где \bar{z} — вектор с компонентами $z_I = 2^{k-|I|-n/2+1}$, $0 \leq |I| \leq k$.

Для числа корреляционно-иммунных порядка k функций от n переменных справедливо следующее утверждение.

Следствие 2. Если $n \rightarrow \infty$ и $k(n) = o(\sqrt{n})$, то

$$\begin{aligned} |K(n, k)| &\sim \frac{|R(n, k)| \sqrt{\pi/2} 2^{n/2-k}}{\left(1 + \sum_{i=2}^k (i-1)^2 \binom{n}{i}\right)^{1/2}} \\ &\sim \frac{\exp_2 \left(2^n - \binom{n}{k} (n-k)/2 - (M(n, k) - 1) \log_2 \sqrt{\pi/2} + n/2 - k \right)}{\left(1 + \sum_{i=2}^k (i-1)^2 \binom{n}{i}\right)^{1/2}}. \end{aligned}$$

Доказательство. Из (8) и теоремы 1 следует, что

$$\begin{aligned} \frac{|K(n, k)|}{|B_n|} &= \sum_{r=-2^{n-k-1}}^{2^{n-k-1}} \frac{|R(n, k)|}{|B_n|} \left(\exp \left(-\frac{r^2}{2} \bar{z}^T Q^{-1} \bar{z} \right) + O(n^{5k+4}/2^n) \right), \\ \bar{z}^T Q^{-1} \bar{z} &= 2^{-n+2} \sum_I \left(2^{|I|} 2^{k-|I|} - \sum_{i \in I} 2^{|I|-1} 2^{k-|I|-1} \right)^2 \\ &= 2^{-n+2} \sum_I (2^k - |I| 2^k)^2 = 2^{2k-n+2} \sum_{i=0}^k \binom{n}{i} (1-i)^2 = 2^{2k-n+2}, \end{aligned}$$

где

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

Тогда

$$|K(n, k)| = |R(n, k)| \left(\frac{2^{n/2-k-1}}{\sqrt{S}} \sum_r \exp(-x_r^2/2) (x_{r+1} - x_r) + o(1) \right),$$

где $x_r = r\sqrt{S}/2^{n/2-k-1}$. Сумма в скобках есть интеграл от непрерывной функции по ступенчатой функции в пределах от $-2^{n/2}/\sqrt{S}$ до $2^{n/2}/\sqrt{S}$, который при $n \rightarrow \infty$ сходится к интегралу

$$\int_{-\infty}^{\infty} \exp(-t^2/2) dt = \sqrt{2\pi}.$$

Следствие доказано.

В следующей таблице приведены точные значения $|R(n, k)|$, $|K(n, k)|$ и приближенные значения, вычисленные по формулам

$$\begin{aligned} |R(n, 1)|^* &= \pi^{-(n+1)/2} \exp_2 \left(2^n - \frac{n^2 - 2n - 1}{2} \right), \\ |R(n, 2)|^* &= \pi^{-(n^2+n)/4} \exp_2 \left(2^n - \frac{n^3 - 4n^2 + n - 2}{4} \right), \\ |K(n, 1)|^* &= \pi^{-n/2} \exp_2 \left(2^n - \frac{n^2 - 3n + 2}{2} \right), \\ |K(n, 2)|^* &= \pi^{-\frac{n^2+n}{4}} \exp_2 \left(2^n - \frac{n^3 - 4n^2 - n + 8}{4} \right) / \sqrt{n(n+1)/2}, \end{aligned}$$

а также относительные погрешности $(x^* - x)/x$ в процентах.

n	k	$ R(n, k) $	$ R(n, k) ^*$	%	$ K(n, k) $	$ K(n, k) ^*$	%
4	1	222	331,13	50	648	830,02	28,1%
4	2	10	85,44	754,4	12	33,86	182,2%
5	1	807980	$1.08 \cdot 10^6$	33,9	314062	$3,84 \cdot 10^6$	22,2%
5	2	552	3536,31	540,6	1058	1618,38	53%

Из таблицы видно, что для $k = 1$ формулы дают правильный порядок уже при $n = 4, 5$. Для $k = 2$ и данных значений n величина отношения k^2/n велика и, видимо, этим в первую очередь объясняется большая величина погрешности.

Заметим, что, используя формулу условной вероятности, мы можем теперь оценивать распределение вектора $\bar{w}(f, n, k)$ при равновероятном выборе f не из всего B_n , а из множества

$$\{f \in B_n : \bar{w}(f, n, l) = \bar{w}_0\}$$

при любых $0 \leq l < k$ и $\bar{w}_0 \in Z^{M(n,l)}$. Так, при $l = 0$ и $\bar{w}_0 = (w)$ получаем при $n \rightarrow \infty$ предельное распределение \bar{w} при случайном выборе f из функций веса $w = w(n)$. Для иллюстрации сформулируем еще одно следствие.

Следствие 3. Если $n \rightarrow \infty$ и $k(n) = o(\sqrt{n})$, то

$$\begin{aligned} \mathbf{P}\{f \in R(n, k+1) \mid f \in R(n, k)\} &= \frac{|R(n, k+1)|}{|R(n, k)|} \\ &\sim \exp_2 \left(-\frac{n-k-1}{2} \binom{n}{k+1} + \frac{n-k}{2} \binom{n}{k} - \binom{n}{k+1} \log_2 \sqrt{\pi/2} \right) \\ &= \exp_2 \left(-\frac{1}{2} \binom{n}{k+1} \left(n-k-1-k-1 + \log_2 \frac{\pi}{2} \right) \right) \\ &= \exp_2 \left(-\frac{1}{2} \binom{n}{k+1} \left(n-2k - \log_2 \frac{8}{\pi} \right) \right). \end{aligned}$$

3. ЛПТ для распределения части спектра

Многие важные характеристики двоичных функций определяются частью спектра. В работе [7] доказано, что $f \in K(n, k)$ в том и только том случае, когда $F_I = 0$ для всех I , $1 \leq |I| \leq k$. Следовательно, $f \in R(n, k)$ в том и только том случае, когда

$F_I = 0$ для всех I , $0 \leq |I| \leq k$. В статье [8] этот критерий обобщен для функций $f: GF(q)^r \rightarrow GF(q)^m$.

В двоичном случае этот факт вытекает из однозначной связи векторов $\bar{w}(f, n, k)$ и $\bar{F}(f, n, k)$, которая, в свою очередь следует из известных формул связи весов подфункций функции и ее спектральных коэффициентов. Дадим простое доказательство формулы связи. Заметим, что $(-1)^a = 1 - 2a$ для $a = 0, 1$ и

$$\begin{aligned} a_1 \oplus \dots \oplus a_m &= \frac{1}{2} (1 - (-1)^{a_1 + \dots + a_m}) = \frac{1}{2} \left(1 - \prod_{j=1}^m (1 - 2a_j) \right) \\ &= \frac{1}{2} \left(1 - \sum_{J \subset \{1, \dots, m\}} (-2)^{|J|} a_{j_1} \dots a_{j_{|J|}} \right) \\ &= \sum_{\emptyset \neq J \subset \{1, \dots, m\}} (-2)^{|J|-1} a_{j_1} \dots a_{j_{|J|}}. \end{aligned} \tag{9}$$

Отсюда следует, что

$$\begin{aligned} &\|f(x_1, \dots, x_n) \oplus x_{i_1} \dots \oplus x_{i_{|I|}}\| \\ &= \sum_{x \in V_n} \left(\sum_{\emptyset \neq J \subset I} (-2)^{|J|-1} x_{j_1} \dots x_{j_{|J|}} + \sum_{J \subset I} (-2)^{|J|} x_{j_1} \dots x_{j_{|J|}} f(x) \right) \\ &= \sum_{\emptyset \neq J \subset I} (-2)^{|J|-1} 2^{n-|J|} + \sum_{J \subset I} (-2)^{|J|} \sum_{x \in V_n} x_{j_1} \dots x_{j_{|J|}} f(x) \\ &= 2^{n-1} \sum_{\emptyset \neq J \subset I} ((-1)^{|J|-1} - 1 + 1) + \sum_{J \subset I} (-2)^{|J|} w_J \\ &= 2^{n-1} + \sum_{J \subset I} (-2)^{|J|} w_J, \\ F_I &= - \sum_{J \subset I} (-2)^{|J|} w_J = \sum_{J \subset I} (-1)^{|J|} (2^{n-1} - 2^{|J|} w_J). \end{aligned} \tag{10}$$

Тогда по формуле обращения Мебиуса

$$2^{n-1} - 2^{|I|} w_I = \sum_{J \subset I} (-1)^{|J|} F_J w_I - 2^{n-|I|-1} = 2^{-|I|} \sum_{J \subset I} (-1)^{|J|+1} F_J. \tag{11}$$

Из (11) легко получить отношение сравнимости для спектральных коэффициентов, именно, для всех $1 \leq |I| \leq k$

$$F_I \equiv \sum_{J \subset I, J \neq I} (-1)^{|I \setminus J|-1} F_J \pmod{2^{|I|}}. \tag{12}$$

При $k = 1$ это сравнение равносильно одинаковости четности компонент \bar{F} . Таким образом, из теоремы 1 и формул связи (10)–(11) векторов \bar{w} и \bar{F} можно вывести асимптотическую формулу для вероятностей $\mathbf{P}(\bar{F} = \bar{a})$ для целочисленных векторов \bar{a} длины $M(n, k)$, удовлетворяющих условиям (12).

Теорема 2. Пусть $n \rightarrow \infty$ и $k(n) = o(\sqrt{n})$. Тогда равномерно относительно целочисленных векторов \bar{a} длины $M(n, k)$, удовлетворяющих условиям (12) сравнимости компонент a_I , справедливо представление

$$\mathbf{P}\{\bar{F} = \bar{a}\} = \frac{\exp(-U_k(\bar{a})/2^{n-1}) + O(n^{5k+4}/2^n)}{\exp_2 \left(\binom{n}{k} (n-k)/2 + M(n, k) \log_2 \sqrt{\pi/2} \right)},$$

где

$$U_k(\bar{a}) = \sum_{0 \leq |I| \leq k} \left(\sum_{J \subset I} (-1)^{|J|} (|I| - |J| - 1) a_J \right)^2.$$

В частности,

$$U_1(\bar{a}) = \sum_{|I| \leq 1} a_I^2,$$

$$U_2(\bar{a}) = \sum_{|I| \leq 1} a_I^2 + \sum_{|I|=2} (a_\emptyset - a_I)^2,$$

$$U_3(\bar{a}) = \sum_{|I| \leq 1} a_I^2 + \sum_{|I|=2} (a_\emptyset - a_I)^2 + \sum_{|I|=3} (2a_\emptyset - a_{\{i_1\}} - a_{\{i_2\}} - a_{\{i_3\}} + a_{\{i_1, i_2, i_3\}})^2.$$

Доказательство. Из теоремы 1 и формул (10)–(11) получаем, что

$$\mathbf{P}\{\bar{F} = \bar{a}\} = \mathbf{P}\{\bar{w} - \mathbf{E}\bar{w} = \bar{z}(\bar{a})\} = \frac{\exp \left(-(1/2) \bar{z}^T(\bar{a}) Q(n, k)^{-1} \bar{z}(\bar{a}) / 2^{n-2} \right) + O(n^{5k+4} / 2^n)}{\exp_2 \left(\binom{n}{k} (n-k) / 2 + M(n, k) \log_2 \sqrt{\pi/2} \right)}$$

равномерно относительно \bar{a} таких, что вектор $\bar{z}(\bar{a})$ с компонентами

$$z_I(\bar{a}) = 2^{-|I|} \sum_{J \subset I, J \neq \emptyset} (-1)^{|J|+1} a_J$$

целочисленный, что равносильно условию (12). Остается заметить, что

$$\bar{z}^T(\bar{a}) Q(n, k)^{-1} \bar{z}(\bar{a}) = U_k(\bar{a}),$$

поскольку (см. лемму 4)

$$\begin{aligned} 2^{|I|} z_{|I|} - \sum_{i \in I} 2^{|I|-1} z_{I \setminus \{i\}} &= \sum_{J \subset I} (-1)^{|J|+1} a_J - \sum_{K \subset I, |K|=|I|-1} \sum_{J \subset K} (-1)^{|J|+1} a_J \\ &= \sum_{J \subset I} (-1)^{|J|+1} a_J (1 - |\{K: J \subset K \subset I, |K|=|I|-1\}|) \\ &= \sum_{J \subset I} (-1)^{|J|} (|I \setminus J| - 1) a_J. \end{aligned}$$

Теорема доказана.

В работе Б.В. Рязанова [4] была доказана (а в [5] обобщена) следующая ЛПТ для распределения части спектра. Согласно формуле (17) из [4] при любом фиксированном $r \geq 1$ и $n \rightarrow \infty$ асимптотическое равенство

$$\mathbf{P}\{F_{I_j} = a_j, 1 \leq j \leq r\} = \frac{\exp \left(- \sum_{j=1}^r a_j^2 / 2^{n-1} \right) + O(2^{-n/2})}{\exp_2(nr/2 - r + 1 + r \log_2 \sqrt{\pi/2})} \tag{13}$$

выполняется равномерно по всем точкам $\bar{a} = (a_1, \dots, a_r)$ некоторой целочисленной решетки и наборам (I_1, \dots, I_r) таким, что соответствующие им векторы e_{I_1}, \dots, e_{I_r} (I — множество единичных координат вектора $e_I \in V_n$) линейно независимы.

Теорема 2 и ЛПТ из [4] характеризуют поведение непересекающихся множеств наборов спектральных коэффициентов. Тем не менее, если рассматривать предельное распределение первых $M(n, 1)$ спектральных коэффициентов, то главные члены в теореме 2 и формуле (13) при $r = n + 1$ одинаковы. Но на этом сходство оканчивается: при всех $k \geq 2$ и квадратичная форма $U_k(\bar{a})$, и выражение в знаменателе отличаются от соответствующих выражений в (13).

Автор благодарен А.С. Амбросимову за постановку задачи и внимание к работе.

Список литературы

1. Денисов О.В., Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций. *Дискретная математика* (1991) **3**, №2, 25–46.
2. Зуев Ю.А., Комбинаторно-вероятностные и геометрические методы в пороговой логике. *Дискретная математика* (1991) **3**, №2, 47–57.
3. Кузнецов Ю.В., Шкарин С.А., Коды Рида–Маллера (обзор публикаций). *Матем. вопросы кибернетики* (1996), №6, 51–80.
4. Рязанов Б.В., О распределении спектральной сложности булевых функций. *Дискретная математика* (1994) **6**, №2, 111–129.
5. Рязанов Б.В., Чечета С.И., О приближении случайной булевой функции множеством квадратичных форм. *Дискретная математика* (1995) **7**, №3, 129–145.
6. Chow C.K., On the characterization of threshold functions. *Minimization of Boolean Functions and Logical Design. Switching Circuit Theory and Logical Design. AIEE Special Publication* (1961) **134**, 34–38.
7. Guo-Zhen X., Massey J.L., A spectral characterization of correlation-immune combining functions. *IEEE Trans. Information Theory* (1988) **34**, 569–571.
8. Gopalakrishnan K., Stinson D.R., Three characterization of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography* (1995) **5**, 241–251.

Статья поступила 09.11.1999.