

ОЦЕНКИ СКОРОСТИ СХОДИМОСТИ В ПРЕДЕЛЬНЫХ ТЕОРЕМАХ ДЛЯ СОВМЕСТНЫХ РАСПРЕДЕЛЕНИЙ ЧАСТИ ХАРАКТЕРИСТИК СЛУЧАЙНЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

*Московский государственный технический университет радиотехники, электроники
и автоматики, г. Москва, Россия*

E-mail: k.n.pankov@gmail.com

Исследуется предельное распределение векторов, состоящих из части спектральных и автокорреляционных коэффициентов и весов подфункций линейных комбинаций координатных функций случайной двоичной вектор-функции. Получены теоремы об асимптотической нормальности этих векторов с оценкой скорости сходимости. Получены сравнения, которым должны удовлетворять координаты этих векторов.

Ключевые слова: случайное двоичное отображение, локальная предельная теорема, закон больших чисел, автокорреляционные коэффициенты, спектральные коэффициенты, веса подфункций.

Введение

Согласно [1], в устойчивости современных блочных и поточных шифрсистем к различным методам анализа значительную роль играют свойства используемых в них двоичных вектор-функций или S-box'ов. В работе [2] доказано, что многие важные свойства двоичного отображения f , такие, как максимальная нелинейность, корреляционная иммунность, устойчивость, сводятся к обладанию этими свойствами всеми ненулевыми линейными комбинациями координатных функций f , называемых в [3] компонентными функциями или компонентами. Свойства же компонент могут быть выражены в терминах их коэффициентов Фурье — Уолша — Адамара (спектральных коэффициентов), весов подфункций и автокорреляций.

Для произвольных подмножества $I = \{i_1, \dots, i_{|I|}\}$ множества $\{1, \dots, n\}$ и непустого подмножества $J = \{j_1, \dots, j_{|J|}\}$ множества $\{1, \dots, m\}$ через $w_I^J(f)$ обозначим вес $\|(f^J)_{i_1, \dots, i_{|I|}}^{1, \dots, 1}\|$ подфункции $(f^J)_{i_1, \dots, i_{|I|}}^{1, \dots, 1}$ компоненты $f^J = f_{j_1} \oplus \dots \oplus f_{j_{|J|}}$ отображения $f = (f_1, \dots, f_m) \in B_n^m$, получаемой, если у аргумента функции f^J значения координат с номерами $i_1, \dots, i_{|I|}$ положить равными единице. Под $|I|$ понимается мощность множества I .

В таких же условиях для компоненты f^J можно определить спектральный коэффициент Фурье — Уолша — Адамара

$$F_I^J(f) = \frac{1}{2} \sum_{x \in V_n} (-1)^{f^J(x) \oplus x_{i_1} \oplus \dots \oplus x_{i_{|I|}}}$$

и автокорреляционный коэффициент (автокорреляционную функцию, автокорреляцию)

$$r_I^J(f) = \sum_{x \in V_n} (-1)^{f^J(x) \oplus f^J(x \oplus e_I)},$$

где $e_I \in V_n$ — двоичный вектор веса $|I|$, в котором единицы стоят на $i_1, \dots, i_{|I|}$ местах, $I \neq \emptyset$.

Многие свойства двоичных отображений зависят от того, чему равен вектор, состоящий из части определённых выше характеристик всех компонент или их части. В частности, двоичное отображение является корреляционно-иммунным порядка k , если вектор

$$(w_I^J(f) - 2^{n-|I|-1} : J \subset \{1, \dots, m\}, J \neq \emptyset, I \subset \{1, \dots, n\}, 1 \leq |I| \leq k)$$

или вектор

$$(F_I^J(f) : J \subset \{1, \dots, m\}, J \neq \emptyset, I \subset \{1, \dots, n\}, 1 \leq |I| \leq k)$$

состоят из одних нулей [4]. Кроме того, отображение подчиняется строгому лавинному критерию или критерию распространения степени 1, если состоит из нулей вектор $(r_{\{i\}}^{\{j\}}(f) : j \in \{1, \dots, m\}, i \in \{1, \dots, n\})$ [1].

Изучению подобных векторов в случае одной компоненты или булевой функции посвящены работы [4–6]. Подробный обзор публикаций, в том числе и по этой тематике, содержится в [1].

Пусть функция f выбирается случайно и равновероятно из множества B_n^m всех m -мерных двоичных функций от n переменных. Это эквивалентно независимому равновероятному выбору её значений $f(\alpha)$ из множества V_m двоичных векторов размерности m для всех α из множества V_n . Можно рассматривать значение функции f как вектор длины m , состоящий из значений её координатных двоичных функций от n переменных:

$$f(\alpha) = (f_1(\alpha), f_2(\alpha), \dots, f_m(\alpha)) : V_n \rightarrow V_m,$$

где $f_i(\alpha) : V_n \rightarrow \{0, 1\}$ для всех $i \in \{1, \dots, m\}$.

Тогда значения $f_i(\alpha)$ выбираются независимо и равновероятно из множества $\{0, 1\}$ для всех α из множества V_n и для всех $i \in \{1, \dots, m\}$.

В случае случайного выбора f векторы, состоящие из части характеристик компонент отображения, также являются случайными, и возникает вопрос об их распределении, в том числе и предельном.

В п. 1 данной работы доказаны отношения сравнимости, которым должны удовлетворять координаты векторов части характеристик. В п. 2 получены результаты о характере и скорости сходимости к нулю нормы вектора части спектральных коэффициентов компонент случайного двоичного отображения, а также показана асимптотическая нормальность этого вектора с оценкой скорости сходимости. В п. 3 и 4 при введении дополнительных условий аналогичные результаты получены для векторов части весов подфункций компонент и автокорреляционных коэффициентов.

Везде далее $E\xi$ обозначает математическое ожидание случайной величины ξ .

1. Сравнения для характеристик компонент двоичного отображения

Для произвольного или случайного отображения f будем записывать далее

$$F_I^J(f) = F_I^J, \quad w_I^J(f) = w_I^J, \quad r_I^J(f) = r_I^J.$$

Формулы связи между спектральными и автокорреляционными коэффициентами широко известны (к примеру, теорема 65 в [7]).

В работе [4] доказаны формулы связи весов подфункций и спектральных коэффициентов для любых булевых функций:

$$F_I^J = \sum_{L \subset I} (-1)^{|L|} (2^{n-1} - 2^{|L|} w_L^J),$$

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

Последнее равенство, опубликованное О. В. Денисовым в начале 2000 г., является аналогом равенства Саркара для коэффициентов Уолша $W_I^J = 2F_I^J$, названного так в [8]. Из него легко выводится отношение сравнимости для спектральных коэффициентов, также представленное в [4]:

$$F_I^J \equiv \sum_{\substack{L \subset I, \\ L \neq I}} (-1)^{|I \setminus L|+1} F_L^J \pmod{2^{|I|}}.$$

Но это отношение верно для части спектральных коэффициентов, относящихся только к одной компоненте f^J функции f . Докажем следующее

Утверждение 1. Для любого непустого подмножества $J = \{j_1, \dots, j_{|J|}\}$ множества $\{1, \dots, m\}$ и произвольного подмножества $I = \{i_1, \dots, i_{|I|}\}$ множества $\{1, \dots, n\}$ имеет место

$$\sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} w_I^S = 2^{|J|-1} \left\| \left(f_{j_1} \cdot \dots \cdot f_{j_{|J|}} \right)_{i_1, \dots, i_{|I|}}^{1, \dots, 1} \right\|.$$

Доказательство. Очевидно, что $w_I^J = \sum_{\alpha \in V_n} \beta_I(\alpha) f^J(\alpha)$, где $\beta_I(\alpha) = \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{|I|}}$ (при $I = \emptyset$ считаем, что $\beta_I(\alpha) \equiv 1$). Получим

$$\begin{aligned} \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} w_I^S &= \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} \sum_{\alpha \in V_n} \beta_I(\alpha) f^S(\alpha) = \\ &= \sum_{\alpha \in V_n} \beta_I(\alpha) \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} (f_{s_1} \oplus \dots \oplus f_{s_{|S|}}). \end{aligned}$$

Известно, что $f_{j_1} \oplus \dots \oplus f_{j_{|J|}} = \sum_{\emptyset \neq K \subset J} (-2)^{|K|-1} f_{k_1} \dots f_{k_{|K|}}$, следовательно,

$$\begin{aligned} \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} (f_{s_1} \oplus \dots \oplus f_{s_{|S|}}) &= \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} \sum_{\emptyset \neq K \subset S} (-2)^{|K|-1} f_{k_1} \dots f_{k_{|K|}} = \\ &= \sum_{\emptyset \neq K \subset J} (-2)^{|K|-1} f_{k_1} \dots f_{k_{|K|}} \sum_{S: K \subset S \subset J} (-1)^{|S|+1} = \\ &= \sum_{\emptyset \neq K \subset J} 2^{|K|-1} f_{k_1} \dots f_{k_{|K|}} I\{K = J\} = 2^{|J|-1} f_{j_1} \dots f_{j_{|J|}}, \end{aligned}$$

где $I\{K = J\}$ — индикатор того, что множество K равно множеству J .

В итоге получаем

$$\begin{aligned} \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} w_I^S &= \sum_{\alpha \in V_n} \beta_I(\alpha) \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} (f_{s_1} \oplus \dots \oplus f_{s_{|S|}}) = \\ &= 2^{|J|-1} \sum_{\alpha \in V_n} \beta_I(\alpha) f_{j_1} \dots f_{j_{|J|}}. \end{aligned}$$

Утверждение доказано. ■

Из последнего равенства легко выводится сравнение для весов подфункций.

Следствие 1. В условиях утверждения 1 выполняется сравнение

$$\sum_{\emptyset \neq S \subset J} (-1)^{|S|} w_I^S \equiv 0 \pmod{2^{|J|-1}}.$$

К отношению же из [4] добавляется новое сравнение для спектральных коэффициентов.

Следствие 2. В условиях утверждения 1 выполняются сравнения

$$\begin{aligned} \sum_{L \subset I} (-1)^{|L|} F_L^J &\equiv 0 \pmod{2^{|I|}}, \\ \sum_{\substack{\emptyset \neq S \subset J, \\ L \subset I}} (-1)^{|L|+|S|} F_L^S &\equiv 0 \pmod{2^{|I|+|J|-1}}. \end{aligned}$$

Доказательство. Первое сравнение очевидно. Рассмотрим

$$\begin{aligned} \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} (w_I^S - 2^{n-|I|-1}) &= \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} \left(2^{-|I|} \cdot \sum_{L \subset I} (-1)^{|L|+1} F_L^S \right), \\ \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} (w_I^S - 2^{n-|I|-1}) &= \left(\sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} w_I^S \right) - 2^{n-|I|-1} = \\ &= 2^{|J|-1} \left\| \left(f_{j_1} \cdot \dots \cdot f_{j_{|J|}} \right)_{i_1, \dots, i_{|J|}}^{1, \dots, 1} \right\| - 2^{n-|I|-1}, \\ \sum_{\emptyset \neq S \subset J} (-1)^{|S|+1} \left(2^{-|I|} \cdot \sum_{L \subset I} (-1)^{|L|+1} F_L^S \right) &= 2^{-|I|} \sum_{\emptyset \neq S \subset J} \sum_{L \subset I} (-1)^{|L|+|S|} F_L^S. \end{aligned}$$

Следовательно, $2^{-|I|-|J|+1} \sum_{\emptyset \neq S \subset J} \sum_{L \subset I} (-1)^{|L|+|S|} F_L^S = \left\| \left(f_{j_1} \cdot \dots \cdot f_{j_{|J|}} \right)_{i_1, \dots, i_{|J|}}^{1, \dots, 1} \right\| - 2^{n-|I|-|J|}$. ■

Теперь докажем два свойства, общих для автокорреляционных коэффициентов всех двоичных отображений.

Утверждение 2. Пусть $n \in \mathbb{N}$, $n \geq 2$, $f(x) \in B_n^m$ — произвольная функция, $I \subset \{1, \dots, n\}$ и $J \subset \{1, \dots, m\}$, где $I, J \neq \emptyset$. Тогда

$$r_I^J(f) \equiv 0 \pmod{4}.$$

Доказательство. Пусть без ограничения общности $J = \{1\}$, $I = \{n - |I| + 1, \dots, n\}$. Обозначим $\bar{1}_n \in V_n$ двоичный вектор веса $|I|$, состоящий из единиц. Получим

$$\begin{aligned} r_I^J(f) &= \sum_{x \in V_n} (-1)^{f^J(x) \oplus f^J(x \oplus e_I)} = \sum_{\alpha \in V_{n-|I|}} \sum_{\beta \in V_{|I|}} \left((-1)^{f_1(\alpha, \beta) \oplus f_1(\alpha, \beta \oplus \bar{1}_{|I|})} \right) = \\ &= \sum_{\alpha \in V_{n-|I|}} 2 \sum_{\gamma \in V_{|I|-1}} \left((-1)^{f_1(\alpha, 0, \gamma) \oplus f_1(\alpha, 1, \gamma \oplus \bar{e}_{|I|-1})} \right) = \\ &= 2 \sum_{\alpha \in V_{n-|I|}} \sum_{\gamma \in V_{|I|-1}} (1 - 2(I \{f_1(\alpha, 0, \gamma) \oplus f_1(\alpha, 1, \gamma \oplus \bar{e}_{|I|-1}) = 1\})) = \\ &= 4 \left(2^{n-2} - \sum_{\alpha \in V_{n-|I|}} \left(\sum_{\gamma \in V_{|I|-1}} I \{f_1(\alpha, 0, \gamma) \oplus f_1(\alpha, 1, \gamma \oplus \bar{e}_{|I|-1}) = 1\} \right) \right). \end{aligned}$$

Утверждение доказано. ■

Утверждение 3. Пусть $I_1, I_2 \subset \{1, \dots, n\}$ и $J \subset \{1, \dots, m\}$, где $I_1, I_2, J \neq \emptyset$. Тогда

$$r_{I_1}^J - r_{I_2}^J \equiv 0 \pmod{8}.$$

Доказательство. Если $I_1 = I_2$, то утверждение очевидно. Без ограничения общности считаем, что $J = \{1\}$, $I_1 \neq I_2$. Обозначим $e_{I_1} = \alpha$, $e_{I_2} = \beta$, $\alpha \neq \beta$. Тогда

$$r_{I_1}^J - r_{I_2}^J = \sum_{x \in V_n} (-1)^{f_1(x)} \left((-1)^{f_1(x \oplus \alpha)} - (-1)^{f_1(x \oplus \beta)} \right).$$

Будем говорить, что $y \in V_n$ эквивалентен $x \in V_n$, если $y = x \oplus \delta_1 \alpha \oplus \delta_2 \beta$ для некоторых $\delta_1, \delta_2 \in \{0, 1\}$. Очевидно, что отношение эквивалентности введено корректно. Разобьём V_n на классы эквивалентности $V_n / \equiv$ по этому отношению и преобразуем разность $r_{I_1}^J(f) - r_{I_2}^J(f)$:

$$\begin{aligned} r_{I_1}^J(f) - r_{I_2}^J(f) &= \sum_{x \in V_n / \equiv} \left(2(-1)^{f_1(x \oplus \alpha) \oplus f_1(x)} + 2(-1)^{f_1(x \oplus \alpha \oplus \beta) \oplus f_1(x \oplus \alpha)} - \right. \\ &\quad \left. - 2(-1)^{f_1(x \oplus \beta) \oplus f_1(x)} - 2(-1)^{f_1(x \oplus \alpha \oplus \beta) \oplus f_1(x \oplus \beta)} \right) = \\ &= 2 \sum_{x \in V_n / \equiv} \left((-1)^{f_1(x \oplus \alpha)} - (-1)^{f_1(x \oplus \beta)} \right) \left((-1)^{f_1(x)} + (-1)^{f_1(x \oplus \alpha \oplus \beta)} \right). \end{aligned}$$

Осталось заметить, что в сумме каждый из двух сомножителей делится на 2. ■

Полученные сравнения позволяют уточнить вопрос о возможных значениях, которые могут принимать координаты векторов, состоящие из части характеристик компонент случайного двоичного отображения.

2. Предельные теоремы для вектора, состоящего из части спектральных коэффициентов компонент случайного двоичного отображения

Пусть f — случайная функция из B_n^m . Рассмотрим вектор

$$S(f) = (F_{I_s}^{J_s}(f) : I_s \subset \{1, \dots, n\}, \emptyset \neq J_s \subset \{1, \dots, m\}, s \in \{1, \dots, r\}),$$

состоящий из r коэффициентов Фурье — Уолша — Адамара, где r — некоторое натуральное число, не превышающее $2^{n+m} - 2^n$, и наборы множеств $(J_1, I_1), \dots, (J_r, I_r)$ попарно различны.

Из определения спектральных коэффициентов легко видеть, что этот вектор равен сумме 2^n векторов

$$S(f) = \frac{1}{2} \sum_{\alpha \in V_n} \chi(\alpha) = \frac{1}{2} \sum_{\alpha \in V_n} \left((-1)^{f^{J_s}(\alpha) \oplus \alpha_{i_1} \oplus \dots \oplus \alpha_{i_{|I_s|}}} : s \in \{1, \dots, r\} \right).$$

Рассмотрим набор из 2^n независимых и одинаково распределённых случайных векторов $\chi(\alpha) = (\chi_1(\alpha), \dots, \chi_r(\alpha))$, $\alpha \in V_n$, координаты которых имеют математическое ожидание

$$E\chi_s(\alpha) = E(-1)^{f^{J_s}(\alpha) \oplus \alpha_{i_1} \oplus \dots \oplus \alpha_{i_{|I_s|}}} = 0$$

для всех $s \in \{1, \dots, r\}$.

Очевидно, что для любых $k, s \in \{1, \dots, r\}$ ковариация координат равна

$$\text{cov}(\chi_s(\alpha), \chi_k(\alpha)) = E(-1)^{f^{J_s}(\alpha) \oplus \alpha_{i_1} \oplus \dots \oplus \alpha_{i_{|I_s|}} \oplus f^{J_k}(\alpha) \oplus \alpha_{i_1} \oplus \dots \oplus \alpha_{i_{|I_k|}}} = I\{k = s\}.$$

Следовательно, $\chi(\alpha)$, $\alpha \in V_n$, — независимые одинаково распределённые в $\mathbb{R}^r$ случайные векторы с единичной ковариационной матрицей и нулевым средним.

Сумма векторов $\sum_{\alpha \in V_n} \chi(\alpha)$ лежит в множестве $\mathbb{R}^r$, которое является евклидовым пространством со скалярным произведением $(\vec{x}, \vec{y}) = \sum_{i=1}^r x_i y_i$, где $\vec{x} = (x_1 \dots x_r) \in \mathbb{R}^r$, $\vec{y} = (y_1 \dots y_r) \in \mathbb{R}^r$, и нормой $\|\vec{x}\| = \sqrt{(\vec{x}, \vec{x})}$.

Как легко видеть, $\|\chi(\alpha)\| = \sqrt{r}$, следовательно, верно, что $E\left(\|\chi(\alpha)\|^\beta\right) = r^{\beta/2} < \infty$ при всех вещественных $\beta \in (0, 2)$. Таким образом, мы попадаем в условия основной теоремы [9], из которой следует, что верно

Утверждение 4. Пусть $n \rightarrow \infty$, m — произвольное натуральное число, $\beta \in (0, 2)$ — вещественное число. Тогда для любых попарно различных наборов множеств $(J_1, I_1), \dots, (J_r, I_r)$, где $I_s \subset \{1, \dots, n\}$, $\emptyset \neq J_s \subset \{1, \dots, m\}$ для всех $s \in \{1, \dots, r\}$, $r \in \mathbb{N}$, верно, что норма вектора $2^{-n/\beta} S(f)$ сходится к нулю с вероятностью 1.

Данное утверждение при $\beta = 1$ является формулировкой усиленного закона больших чисел для случайных векторов $\chi(\alpha)$, $\alpha \in V_n$.

Очевидно, что выполняется и обычный закон больших чисел для случайных векторов, и возникает вопрос о скорости сходимости нормы вектора $2^{-n/\beta} S(f)$ к нулю.

Для случайных векторов с нулевыми математическими ожиданиями выполняется теорема 1 [10, с. 47], из которой следует

Утверждение 5. Пусть n, m — произвольные натуральные числа, $\beta \in (0, 2)$ — вещественное число. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, где $I_s \subset \{1, \dots, n\}$, $\emptyset \neq J_s \subset \{1, \dots, m\}$ для всех $s \in \{1, \dots, r\}$, $r \in \mathbb{N}$, для любого $\varepsilon > 0$ верно неравенство

$$P\left\{\|2^{-n/\beta} S(f)\| \geq \varepsilon\right\} \leq \frac{4r}{\varepsilon^2} 2^{(\beta-2)n/\beta}.$$

Докажем теперь теорему о скорости сходимости распределения P_n вектора $2^{1-n/2} S(f)$ к распределению Φ стандартного r -мерного нормального закона.

Теорема 1. Пусть n, m — произвольные натуральные числа. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, где $I_s \subset \{1, \dots, n\}$, $\emptyset \neq J_s \subset \{1, \dots, m\}$ для всех $s \in \{1, \dots, r\}$, $r \in \mathbb{N}$, и для любого выпуклого борелевского множества B справедливо неравенство $|P_n(B) - \Phi(B)| \leq 400r^{7/4} 2^{-n/2}$.

Доказательство. Согласно основному результату [11], если $\xi^{(1)}, \xi^{(2)}, \dots$ — независимые одинаково распределённые в $\mathbb{R}^r$ случайные величины с единичной ковариационной матрицей и нулевым средним, μ — случайная величина со стандартным r -мерным нормальным распределением, $S_N = N^{-1/2} \sum_{j=1}^N \xi^{(j)}$, то $\delta_N = \sup_{A \in L} |P(S_N \in A) - P(\mu \in A)| \leq 400r^{1/4} E\|\xi^{(1)}\|^3 N^{-1/2}$, где L — класс выпуклых борелевских подмножеств $\mathbb{R}^r$.

Для векторов $\chi(\alpha)$, $\alpha \in V_n$, попадаем в условия этого результата при $E\|\chi(\alpha)\|^3 = r^{3/2}$ и $N = 2^n$. ■

Данная теорема предлагает равномерные по r оценки расстояния между распределением вектора $2^{1-n/2} S(f)$ и многомерным стандартным нормальным распределением в обобщённой метрике полной вариации по классу выпуклых борелевских множеств и, следовательно, в равномерной метрике в терминах [12]. При $n \rightarrow \infty$ из этой тео-

ремы следует асимптотическая нормальность вектора и, следовательно, интегральная предельная теорема.

3. Предельные теоремы для вектора, состоящего из части весов подфункций компонент случайного двоичного отображения

Теперь рассмотрим вектор $W(f) = (2^{1+(|I_s|/2)} (w_{I_s}^{J_s}(f) - 2^{n-|I_s|-1}) : I_s \subset \{1, \dots, n\}, \emptyset \neq J_s \subset \{1, \dots, m\}, s \in \{1, \dots, r\})$, состоящий из r весов подфункций, где r — некоторое натуральное число, не превышающее $2^{n+m} - 2^n$, а пары множеств $(J_1, I_1), \dots, (J_r, I_r)$ — любые попарно различные.

Из определения $w_I^J(f)$ легко видеть, что этот вектор равен сумме векторов

$$W(f) = \sum_{\alpha \in V_n} \left(2^{\frac{|I_s|}{2}} \beta_{I_s}(\alpha) (-1)^{f^{J_s}(\alpha) \oplus 1} : s \in \{1, \dots, r\} \right) = \sum_{\alpha \in V_n} \tau(\alpha),$$

где $\beta_I(\alpha) = \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_{|I|}}$ (при $I = \emptyset$ считаем, что $\beta_I(\alpha) \equiv 1$).

Рассмотрим набор из 2^n независимых случайных векторов $\tau(\alpha)$, для всех координат которого $\tau_s(\alpha)$ верно равенство

$$\mathbb{E} \tau_s(\alpha) = 2^{\frac{|I_s|}{2}} \beta_{I_s}(\alpha) \mathbb{E}(-1)^{f^{J_s}(\alpha) \oplus 1} = 0.$$

Следовательно, $\tau(\alpha)$, $\alpha \in V_n$ — независимые не одинаково распределенные в $\mathbb{R}^r$ случайные величины с нулевым средним. Сумма векторов $\sum_{\alpha \in V_n} \tau(\alpha)$ лежит в $\mathbb{R}^r$. Введём

Условия 1. Пусть выполняется следующее:

- 1) Зафиксировано некоторое натуральное $r \in \{1, \dots, 2^m - 1\}$.
- 2) Зафиксирован набор непустых попарно различных подмножеств $J_1, \dots, J_r$ множества $\{1, \dots, m\}$.
- 3) Для любого $s \in \{1, \dots, r\}$ зафиксировано произвольное подмножество I_s множества $\{1, \dots, n\}$.

Обозначим $\delta = \sum_{s=1}^r 2^{|I_s|}$.

Пусть выполняются условия 1. Тогда при фиксированном m выполняется неравенство $\mathbb{E} \|\tau(\alpha)\|^2 \leq \delta < +\infty$. Следовательно, попадаем в условия теоремы 4.2.1 [13], согласно которой верно следующее

Утверждение 6. Пусть $n \rightarrow \infty$, m — произвольное натуральное число. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, удовлетворяющих условиям 1, норма вектора $2^{-n} W(f)$ сходится к нулю с вероятностью 1.

Данное утверждение является формулировкой усиленного закона больших чисел для случайных векторов $\tau(\alpha)$, $\alpha \in V_n$.

Рассмотрим вопрос о скорости сходимости нормы вектора $2^{-n} W(f)$ к нулю. Аналогично утверждению 5 можно легко доказать, что верно

Утверждение 7. Пусть n, m — произвольные натуральные числа. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$ и для любого $\varepsilon > 0$ верно неравенство

$$\mathbb{P} \{ \|2^{-n} W(f)\| \geq \varepsilon \} \leq \varepsilon^{-2} 2^{-n} \sum_{s=1}^r 2^{|I_s|}.$$

Определение 1 [14]. Пусть $\xi^{(1)}, \dots, \xi^{(N)}$ есть N независимых не обязательно одинаково распределённых случайных векторов в $\mathbb{R}^r$ с ковариационными матрицами $\text{cov}(\xi^{(j)})$, $j \in \{1, \dots, N\}$. Тогда средней ковариационной матрицей случайных векторов $\xi^{(1)}, \dots, \xi^{(N)}$ называется матрица $V = \frac{1}{N} \sum_{j=1}^N \text{cov}(\xi^{(j)})$.

Теперь оценим скорость сходимости характеристической функции специальным образом преобразованного вектора, составленного из весов подфункций, к характеристической функции стандартного многомерного нормального закона соответствующей размерности.

Утверждение 8. Пусть n, m — произвольные натуральные числа. Дано случайное отображение $f = (f_1, f_2, \dots, f_m) \in B_n^m$ и выполняются условия 1. Тогда для всех $t \in \mathbb{R}^r$, таких, что $\|t\| \leq 2^{n/4-1} \delta^{-1/2}$, для характеристической функции $\varphi_{w_r}(t)$ случайного вектора

$$w_r = \left(2^{\frac{|I_s|}{2} + 1 - \frac{n}{2}} (w_{I_s}^{J_s}(f) - 2^{n-|I_s|-1}) : I_s \subset \{1, \dots, n\}, \emptyset \neq J_s \subset \{1, \dots, m\}, s \in \{1, \dots, r\} \right)$$

верно неравенство

$$\left| \varphi_{w_r}(t) - e^{-\frac{1}{2}\|t\|^2} \right| \leq 2^{-n-2} \|t\|^4 \delta^2 \left(\frac{7}{10} e^{-\frac{1}{2}\|t\|^4} + \delta \|t\|^2 \left(\frac{9}{125} 2^{-n} \delta \|t\|^2 + \frac{1}{9} \right) e^{-\frac{383}{1000}\|t\|^2} \right).$$

Доказательство. Пусть f — случайная функция из B_n^m . Рассмотрим вектор

$$w_r = \left(2^{\frac{|I_s|}{2} + 1 - \frac{n}{2}} (w_{I_s}^{J_s}(f) - \mathbb{E} w_{I_s}^{J_s}(f)) : s \in \{1, \dots, r\} \right),$$

где $\mathbb{E} w_{I_s}^{J_s}(f) = 2^{n-|I_s|-1}$. Очевидно, что $w_r = 2^{-n/2} \sum_{\alpha \in V_n} \tau(\alpha)$.

Рассмотрим набор из 2^n независимых случайных векторов $\tau(\alpha)$, для всех координат которого $\tau_s(\alpha)$ выполняется свойство $\mathbb{E} \tau_s(\alpha) = 0$.

Для любых $k, s \in \{1, \dots, r\}$ верно равенство

$$\text{cov}(\tau_s(\alpha), \tau_k(\alpha)) = 2^{\frac{|I_s|}{2} + \frac{|I_k|}{2}} \beta_{I_s}(\alpha) \beta_{I_k}(\alpha) \mathbb{E}(-1)^{f^{J_s}(\alpha) \oplus f^{J_k}(\alpha)} = 2^{|I_s|} \beta_{I_s}(\alpha) I\{k = s\}.$$

Следовательно, средняя ковариационная матрица V , за исключением главной диагонали, заполнена нулями, а элементы главной диагонали равны

$$\frac{1}{2^n} \sum_{\alpha \in V_n} 2^{|I_s|} \beta_{I_s}(\alpha) = 1.$$

Получили, что $\tau(\alpha)$, $\alpha \in V_n$ — независимые неодинаково распределённые в $\mathbb{R}^r$ случайные векторы с единичной средней ковариационной матрицей и нулевым средним.

Рассмотрим ляпуновскую дробь $l_{s,2^n}$, определённую по формуле

$$l_{s,2^n} = \sup_{\|t\|=1, t \in \mathbb{R}^r} \frac{\sum_{\alpha \in V_n} \mathbb{E}(|(t, \tau(\alpha))|^s)}{\left(\sum_{\alpha \in V_n} \mathbb{E}((t, \tau(\alpha))^2) \right)^{s/2}}.$$

Во введённых обозначениях выполняется теорема 8.6 из [14], согласно которой, если каждый вектор $\tau(\alpha)$ имеет конечный четвёртый абсолютный момент $\rho_4(\tau(\alpha)) =$

$= E\|\tau(\alpha)\|^4$ и ляпуновская дробь $l_{4,2^n}$ не превосходит единицы, то для всех $t \in \mathbb{R}^r$, таких, что $\|t\| \leq \frac{1}{2}l_{4,2^n}^{-1/4}$, справедливо неравенство

$$\begin{aligned} & \left| \varphi_{w_r}(t) - e^{-\frac{1}{2}\|t\|^2} (1 + i^6 2^{-n/2} \mu_3(t)) \right| \leq \\ & \leq \frac{7}{40} l_{4,2^n} \|t\|^4 e^{-\frac{1}{2}\|t\|^4} + \left(\frac{9}{500} l_{4,2^n}^2 \|t\|^8 + \frac{1}{36} l_{3,2^n}^2 \|t\|^6 \right) e^{-\frac{383}{1000}\|t\|^2}, \end{aligned}$$

где $\mu_3(t) = 2^{-n} \sum_{\alpha \in V_n} E((t, \tau(\alpha))^3)$. Легко видеть, что

$$\rho_4(\tau(\alpha)) = \left(\sum_{s=1}^r \left(2^{\frac{|I_s|}{2}} \beta_{I_s}(\alpha) \right)^2 \right)^2 = \left(\sum_{s=1}^r 2^{|I_s|} \beta_{I_s}(\alpha) \right)^2 \leq \delta^2.$$

В обозначениях (8.11) в [14] $\rho_4 = 2^{-n} \sum_{\alpha \in V_n} \rho_4(\tau(\alpha))$.

Очевидно, что $\rho_4 \leq \delta^2$, $E((t, \tau(\alpha))^3) = 0$ и $\mu_3(t) = 0$.

В силу неравенства (8.12) из [14] $l_{4,2^n} \leq 2^{-n}\delta^2$, $l_{3,2^n} \leq 2^{-n/2}\delta^{3/2}$. Следовательно, для всех $t \in \mathbb{R}^r$, таких, что $\|t\| \leq 2^{n/4-1}\delta^{-1/2} \leq 2^{n/4-1}(\rho_4)^{-1/4} \leq \frac{1}{2}l_{4,2^n}^{-1/4}$, выполняется утверждение теоремы. ■

Теперь, используя утверждение 8, докажем теорему о скорости сходимости распределения w_r к распределению Φ стандартного r -мерного нормального закона.

Теорема 2. Пусть m, n — произвольные натуральные числа, L — множество борелевских выпуклых подмножеств $\mathbb{R}^r$, выполняется набор условий 1 и дано случайное отображение $f = (f_1, f_2, \dots, f_m) \in B_n^m$. Пусть для n выполняется

$$n > \max \left\{ \delta^2 - 1, 12 + 2\log_2(9\delta(r+2)^2) \right\}.$$

Тогда для случайного вектора w_r из формулировки утверждения 8 с распределением Q_n верно следующее неравенство:

$$\begin{aligned} \sup_{C \in \mathcal{C}} |Q_n(C) - \Phi(C)| & \leq \frac{4}{3} \left(b_1(r) 2^{-n/2} + b_2(r) 2^{-n/2} n^{-1/2} + b_3(r) 2^{-n} n^{r/2} + \right. \\ & + b_4(r) 2^{-3n/2} n^{-3/2} + b_5(r) 2^{-2n} n^{r/2} + b_6(r) e^{-\frac{2^{n/2}}{280\sqrt{\delta}}} 2^{-n/4} n^{r/2} + \\ & \left. + b_7(r) e^{-\frac{2^{n/2}}{16\sqrt{\delta}}} 2^{-n/4} n^{r/2} + b_8(r) e^{-\frac{2^{n/2}}{16\sqrt{\delta}}} 2^{-3n/4} n^{r/2} \right), \end{aligned}$$

где Φ — распределение случайной величины со стандартным r -мерным нормальным распределением,

$$\begin{aligned} b_1(r) & = \frac{2^5 r^{4/3} \delta^{3/2} \Gamma((r+1)/2)}{3\pi^{1/3} \Gamma(r/2)} + \frac{11r\delta^{3/2}}{2} + \\ & + \frac{(4 + e^{3/2}) \delta^{3/2}}{6e^{3/2} \sqrt{2\pi}} + \frac{(r-1) \delta^{3/2}}{2r^{1/2} \pi e^{1/2}} + \frac{2^{1/2} \delta^{3/2} (r^{3/2} - 3r^{1/2} + 2)}{\pi^{3/2}}, \\ b_3(r) & = \frac{2^{(r-1)/2} r^{(r-2)/2} (\ln 2)^{r/2} \delta^2}{(\Gamma(r/2))^2} \left(\frac{7}{20} 2^{\frac{r}{4}} \Gamma\left(\frac{r+4}{4}\right) + \frac{\delta}{18} \left(\frac{1000}{383}\right)^{\frac{r+6}{2}} \Gamma\left(\frac{r+6}{2}\right) \right), \end{aligned}$$

$$b_4(r) = \frac{2^3 r^{5/2} \delta^3}{\pi (\log 2)^{3/2}}, b_5(r) = \frac{9 \cdot 2^{(r-3)/2} r^{(r-2)/2} (\ln 2)^{r/2} \delta^4 \left(\frac{1000}{383}\right)^{\frac{r+8}{2}} \Gamma\left(\frac{r+8}{2}\right)}{125 (\Gamma(r/2))^2},$$

$$b_2(r) = \frac{r}{(\pi \ln 2)^{1/2}}, b_6(r) = \frac{2^{r+3} \delta^{1/2} r^{(r-2)/2} (\ln 2)^{r/2}}{(\Gamma(r/2))^2} \left(\frac{3}{3-2\sqrt{2}}\right)^{(1+r)/2},$$

$$b_7(r) = \frac{\delta^{1/2} 2^{r+3} r^{(r-2)/2} (\ln 2)^{r/2}}{(\Gamma(r/2))^2}, b_8(r) = \frac{\delta^2 2^{r+7/2} r^{(r-2)/2} (\ln 2)^{r/2}}{3 (\Gamma(r/2))^2}.$$

Здесь $\Gamma(x)$ — значение гамма-функции Эйлера в точке x .

Доказательство. Верно следующее равенство:

$$|\mathbf{P}(w_r \in C) - \Phi(C)| = \left| \int_{\mathbb{R}^r} I_C d(Q_n - \Phi) \right|,$$

где I_C — индикатор множества C .

Рассмотрим случайный вектор K со значениями в $\mathbb{R}^r$ с плотностью

$$p_K(x_1 \dots x_r) = \left(\frac{3a}{2\pi}\right)^r \prod_{s=1}^r \left(\frac{\sin ax_s}{ax_s}\right)^4,$$

где $a = 2\pi^{-1/3} r^{5/6}$. Сглаживающая вероятностная мера, порождённая этим вектором, активно используется в [14].

Рассмотрим случайный вектор εK с распределением K_ε . Согласно неравенству (13.12) из [14],

$$\mathbf{P}(\varepsilon K \in \mathbb{R}^r \setminus B(0 : \varepsilon)) \leq \mathbf{P}(K \in \mathbb{R}^r \setminus B(0 : 1)) \leq \frac{1}{8},$$

где $B(x : \varepsilon)$ — открытый шар в $\mathbb{R}^r$ радиуса ε с центром в x . Тогда

$$\mathbf{P}(\varepsilon K \in B(0 : \varepsilon)) \geq \frac{7}{8} > \frac{1}{2}.$$

Следовательно, попадаем в условия следствия 11.5 в [14]:

$$\left| \int_{\mathbb{R}^r} I_C d(Q_n - \Phi) \right| \leq \frac{4}{3} \left(\frac{1}{2} w_{I_C}(\mathbb{R}^r) \|(Q_n - \Phi) * K_\varepsilon\| + w_{I_C}^*(2\varepsilon : \Phi) \right),$$

где $*$ — внутренняя операция свёртки (композиции) двух конечных обобщённых мер; $w_{I_C}(S) = \sup_{x, y \in S} |I_C(x) - I_C(y)|$ — колебание функции I_C на множестве S ; вариационная норма [14] на классе всех конечных обобщённых мер, равная полной вариации меры, обозначена как $\|(Q_n - \Phi) * K_\varepsilon\|$,

$$w_{I_C}^*(2\varepsilon : \Phi) = \sup_{y \in \mathbb{R}^r} \int_{\mathbb{R}^r} w_{I_C}(B(x - y : 2\varepsilon)) \Phi(dx).$$

Очевидно, что $w_{I_C}(\mathbb{R}^r) = 1$, а, согласно неравенству (13.42) из [14],

$$w_{I_C}^*(2\varepsilon : \Phi) \leq \frac{2^{5/2} \Gamma((r+1)/2)}{3 \Gamma(r/2)} \varepsilon.$$

Теперь рассмотрим поведение величины $\|(Q_n - \Phi) * K_\varepsilon\|$. Из определения вариационной нормы следует, что

$$\|(Q_n - \Phi) * K_\varepsilon\| = 2 \sup_{B \in B^r} |(Q_n - \Phi) * K_\varepsilon(B)|,$$

где B^r — борелевская сигма-алгебра подмножеств из $\mathbb{R}^r$.

Для каждого борелевского множества B и $k > 0$ определим множества

$$B_1 = B \cap B(0 : k), \quad B_2 = B \setminus B_1.$$

Оценим $|(Q_n - \Phi) * K_\varepsilon(B_i)|$, $i \in \{1, 2\}$.

Рассмотрим конечную обобщённую меру $P_1(\alpha)$ с плотностью

$$\begin{aligned} \varphi(x_1 \dots x_r) \times & \left[\frac{1}{6} (\chi_{(3,0,\dots,0)}(x_1^3 - 3x_1) + \dots + \chi_{(0,0,\dots,3)}(x_r^3 - 3x_r)) + \right. \\ & + \frac{1}{2} (\chi_{(2,1,\dots,0)}(x_1^2 x_2 - x_2) + \chi_{(0,\dots,1,2)}(x_r^2 x_{r-1} - x_{r-1})) + \\ & \left. + \chi_{(1,1,1,0,\dots,0)} x_1 x_2 x_3 + \dots + \chi_{(0,\dots,1,1,1)} x_{r-2} x_{r-1} x_r \right] = p_1^\alpha(x_1 \dots x_r), \end{aligned}$$

где $\chi_{(\gamma_1, \dots, \gamma_k)} = \chi_\gamma$ — семиинварианты (кумулянты) вероятностной меры, порождённой случайным вектором $\tau(\alpha)$, порядка γ ; $\varphi(x_1 \dots x_r)$ — плотность распределения случайного вектора со стандартным r -мерным нормальным распределением.

Согласно равенству (7.22) из [14], $\int_{\mathbb{R}^r} p_1^\alpha(x_1 \dots x_r) dx = 0$. Пусть $P_1 = 2^{-n} \sum_{\alpha \in V_n} p_1^\alpha(x_1 \dots x_r)$.

Данная мера введена в равенстве (2.10) в [15]. Имеем

$$|(Q_n - \Phi) * K_\varepsilon(B_1)| \leq |H_n * K_\varepsilon(B_1)| + 2^{-n/2} |P_1 * K_\varepsilon(B_1)|,$$

где $H_n = Q_n - \Phi - 2^{-n/2} P_1$.

Обозначим через $\widehat{H}_n = \int_{\mathbb{R}^r} e^{i(t,x)} H_n(dx)$ преобразование Фурье обобщённой меры H_n .

Согласно неравенству (13.22) из [14], получим

$$|H_n * K_\varepsilon(B_1)| \leq (2\pi)^{-r} \lambda_r(B_1) \int_{\mathbb{R}^r} |\widehat{H}_n(t) \widehat{K}_\varepsilon(t)| dx,$$

где λ_r — мера Лебега на $\mathbb{R}^r$.

С учётом вычисленного в [14] преобразования Фурье для P_1 получаем, что верно равенство

$$\begin{aligned} \widehat{H}_n &= \int_{\mathbb{R}^r} e^{i(t,x)} H_n(dx) = \int_{\mathbb{R}^r} e^{i(t,x)} (Q_n - \Phi - n^{-1/2} P_1)(dx) = \\ &= \widehat{Q}_n - e^{-\frac{1}{2}\|t\|^2} \left(1 + \frac{i^3}{6} n^{-1/2} \mu_3(t) \right), \quad \text{где } \mu_3(t) = 2^{-n} \sum_{\alpha \in V_n} E((t, \tau(\alpha))^3). \end{aligned}$$

Легко показать, что $E((t, \tau(\alpha))^3) = 0$.

Возьмем в качестве ε величину $ar^{1/2} \rho_3 2^{-(n-3)/2}$, где $\rho_3 = 2^{-n} \sum_{\alpha \in V_n} \rho_3(\tau(\alpha))$,

$\rho_3(\tau(\alpha)) = E\|\tau(\alpha)\|^3$. Очевидно, что $\rho_3 \leq \delta^{3/2}$.

Согласно соотношению (13.36) в [14], верно неравенство

$$\begin{aligned} & \int_{\mathbb{R}^r} \left| \widehat{H}_n(t) \widehat{K}_\varepsilon(t) \right| dt \leq \int_{\|t\| < 2^{(n+1)/2}(\rho_3)^{-1}} \left| \widehat{H}_n(t) \right| dt = \\ & = \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \left| \widehat{H}_n(t) \right| dt + \int_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}} < \|t\| < 2^{(n+1)/2}(\rho_3)^{-1}} \left| \widehat{H}_n(t) \right| dt, \end{aligned}$$

где ρ_4 введено в конце доказательства утверждения 8. Там же показано, что утверждение 8 верно при всех $\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}$. Следовательно,

$$\begin{aligned} & \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \left| \widehat{H}_n(t) \right| dt = \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \left| \widehat{Q}_n - e^{-\frac{1}{2}\|t\|^2} \right| dt \leq \\ & \leq \frac{7}{5} 2^{-n-3} \delta^2 \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \|t\|^4 e^{-\frac{1}{2}\|t\|^4} dt + \frac{9}{125} 2^{-2n-2} \delta^4 \times \\ & \times \dots \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \|t\|^8 e^{-\frac{383}{1000}\|t\|^2} dt + \frac{2^{-n-2}}{9} \delta^3 \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \|t\|^6 e^{-\frac{383}{1000}\|t\|^2} dt. \end{aligned}$$

Легко можно показать, что верны следующие неравенства:

$$\begin{aligned} & \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{2}}} \|t\|^4 e^{-\frac{1}{2}\|t\|^4} dt \leq \int_{\mathbb{R}^r} \|t\|^4 e^{-\frac{1}{2}\|t\|^4} dt = \frac{2\pi^{r/2}}{\Gamma(r/2)} \int_0^{+\infty} x^{r+3} e^{-\frac{1}{2}x^4} dx, \\ & \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{2}}} \|t\|^8 e^{-\frac{383}{1000}\|t\|^2} dt \leq \frac{2\pi^{r/2}}{\Gamma(r/2)} \int_0^{+\infty} x^{r+7} e^{-\frac{383}{1000}x^2} dx, \\ & \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{2}}} \|t\|^6 e^{-\frac{383}{1000}\|t\|^2} dt \leq \frac{2\pi^{r/2}}{\Gamma(r/2)} \int_0^{+\infty} x^{r+5} e^{-\frac{383}{1000}x^2} dx. \end{aligned}$$

Из равенства $\int_0^{+\infty} x^m e^{-ax^n} dx = a^{-(m+1)/n} \frac{1}{n} \Gamma((m+1)/n)$ следует, что

$$\begin{aligned} & \int_{\|t\| \leq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \left| \widehat{H}_n(t) \right| dt \leq \frac{\pi^{r/2}}{\Gamma(r/2)} \delta^2 2^{-n-1} \left(\frac{7}{20} 2^{r/4} \Gamma\left(\frac{r+4}{4}\right) + \right. \\ & \left. + \frac{9\delta^2}{250} 2^{-n} \left(\frac{1000}{383} \right)^{(r+8)/2} \Gamma\left(\frac{r+8}{2}\right) + \frac{\delta}{18} \left(\frac{1000}{383} \right)^{(r+6)/2} \Gamma\left(\frac{r+6}{2}\right) \right). \end{aligned}$$

Согласно оценке (13.39) в [14], при $n \geq \delta^2 \geq \rho_4$ верно неравенство

$$\begin{aligned} & \int_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}} < \|t\| < 2^{(n+1)/2}(\rho_3)^{-1}} \left| \widehat{H}_n(t) \right| dt \leq \int_{\|t\| \geq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} e^{\|t\|^2(2\sqrt{2}-3)/6} dt + \\ & + \int_{\|t\| \geq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} e^{-\frac{1}{2}\|t\|^2} dt + \frac{1}{6} \rho_3 2^{-n/2} \int_{\|t\| \geq 2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}}} \|t\|^3 e^{-\frac{1}{2}\|t\|^2} dt. \end{aligned}$$

Следовательно,

$$\begin{aligned} & \int_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}} < \|t\| < 2^{(n+1)/2}(\rho_3)^{-1}} \left| \widehat{H}_n(t) \right| dt \leq \\ & \leq \frac{2\pi^{r/2}}{\Gamma(r/2)} \left(\left(\frac{6}{3-2\sqrt{2}} \right)^{r/2} \int_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}} \sqrt{\frac{3-2\sqrt{2}}{6}}}^{+\infty} x^{r-1} e^{-x^2} dx + \right. \\ & \left. + 2^{r/2} \int_{2^{\frac{n}{4}-\frac{3}{2}}(\rho_4)^{-\frac{1}{4}}}^{+\infty} x^{r-1} e^{-x^2} dx + \frac{1}{3} \rho_3 2^{(r+1-n)/2} \int_{2^{\frac{n}{4}-\frac{3}{2}}(\rho_4)^{-\frac{1}{4}}}^{+\infty} x^{r+2} e^{-x^2} dx \right). \end{aligned}$$

Для всех $n > 12 + 2\log_2(9\delta(r+2)^2)$ подынтегральные функции можно ограничить функцией $e^{-x^2}/2$ и, используя известное неравенство, получить

$$\begin{aligned} & \int_{2^{\frac{n}{4}-1}(\rho_4)^{-\frac{1}{4}} < \|t\| < 2^{(n+1)/2}(\rho_3)^{-1}} \left| \widehat{H}_n(t) \right| dt \leq \frac{4\pi^{r/2}\delta^{1/2}}{\Gamma(r/2)} \times \\ & \times \left(\left(\frac{6}{3-2\sqrt{2}} \right)^{(1+r)/2} 2^{-n/4} e^{-\frac{2n/2}{280\sqrt{\delta}}} + \left(2^{r/2} + \frac{\delta^{3/2}}{3} 2^{(r+1-n)/2} \right) e^{-\frac{2n/2}{16\sqrt{\delta}}} 2^{(2-n)/4} \right). \end{aligned}$$

Применяя лемму 13.1 из [14] и учитывая, что $\rho_3 \leq \delta^{3/2}$, получаем

$$\begin{aligned} & 2^{-n/2} |P_1 * K_\varepsilon(B_1)| \leq 2^{-(n+2)/2} \|P_1\| \leq \\ & \leq \left(\frac{4 + e^{3/2}}{6e^{3/2}\sqrt{2\pi}} + \frac{(r-1)}{2r^{1/2}\pi e^{1/2}} + \frac{2^{1/2}(r^{3/2} - 3r^{1/2} + 2)}{\pi^{3/2}} \right) \delta^{3/2} 2^{-n/2}. \end{aligned}$$

Собирая все оценки воедино, с учётом того, что $\lambda_r(B_1) \leq \frac{2\pi^{r/2}}{r\Gamma(r/2)} k^r$, получаем, что верно неравенство

$$\begin{aligned} & |(Q_n - \Phi) * K_\varepsilon(B_1)| \leq \frac{2k^r}{r2^r(\Gamma(r/2))^2} \left(\left(\delta^2 2^{-n-1} \left(\frac{7}{20} 2^{\frac{r}{4}} \Gamma\left(\frac{r+4}{4}\right) + \right. \right. \right. \\ & \left. \left. + \frac{9\delta^2}{250} 2^{-n} \left(\frac{1000}{383} \right)^{\frac{r+8}{2}} \Gamma\left(\frac{r+8}{2}\right) + \frac{\delta}{18} \left(\frac{1000}{383} \right)^{\frac{r+6}{2}} \Gamma\left(\frac{r+6}{2}\right) \right) + \right. \\ & \left. + 4\delta^{1/2} \left(\left(\frac{6}{3-2\sqrt{2}} \right)^{(1+r)/2} 2^{-n/4} e^{-\frac{2n/2}{280\sqrt{\delta}}} + \left(2^{r/2} + \frac{\delta^{3/2}}{3} 2^{(r+1-n)/2} \right) e^{-\frac{2n/2}{16\sqrt{\delta}}} 2^{(2-n)/4} \right) \right) + \\ & + \left(\frac{4 + e^{3/2}}{6e^{3/2}\sqrt{2\pi}} + \frac{(r-1)}{2r^{1/2}\pi e^{1/2}} + \frac{2^{1/2}(r^{3/2} - 3r^{1/2} + 2)}{\pi^{3/2}} \right) \delta^{3/2} 2^{-n/2}. \end{aligned}$$

Теперь рассмотрим $|(Q_n - \Phi) * K_\varepsilon(B_2)|$. Согласно оценкам (13.27) и (13.28) в [14], верны следующие неравенства:

$$\begin{aligned} & |(Q_n - \Phi) * K_\varepsilon(B_2)| \leq \max \left\{ P \left(\left\| 2^{-\frac{n}{2}} \sum_{\alpha \in V_n} \tau(\alpha) \right\| \geq k/2 \right), \frac{2^{3/2} r^{3/2} e^{-k^2/8r}}{k\pi^{1/2}} \right\} + \\ & + \frac{2^{-(3n-15)/2} r^4 (\rho_3)^2}{\pi k^3}, \end{aligned}$$

$$P \left(\left\| 2^{-\frac{n}{2}} \sum_{\alpha \in V_n} \tau(\alpha) \right\| \geq k/2 \right) \leq \sum_{s=1}^r P \left(\left| 2^{-\frac{n}{2}} \sum_{\alpha \in V_n} \tau_s(\alpha) \right| \geq \frac{k}{2\sqrt{r}} \right),$$

где $\tau_s(\alpha)$ — s -е координаты случайных векторов $\tau(\alpha)$.

Согласно теореме Берри — Эссена для независимых разнораспределённых случайных величин [14], верно неравенство

$$\begin{aligned} \sum_{s=1}^r P \left(\left| 2^{-n/2} \sum_{\alpha \in V_n} \tau_s(\alpha) \right| \geq \frac{k}{2\sqrt{r}} \right) &\leq \frac{11}{2} \rho_3 r 2^{-n/2} + r \int_{|t| \geq k/2} \varphi(t) dt \leq \\ &\leq \frac{11}{2} \delta^{3/2} r 2^{-n/2} + \frac{2^{3/2} r^{3/2} e^{-\frac{k^2}{8r}}}{k \pi^{1/2}}, \end{aligned}$$

где $\varphi(t)$ — плотность стандартного нормального распределения

Если принять $k = (8rn \log 2)^{1/2}$, то, собрав все неравенства вместе, получим утверждение теоремы. ■

В теореме 2 получена оценка расстояния между распределением случайного вектора $2^{-n/\beta} W(f)$ и r -мерным стандартным нормальным распределением в обобщённой метрике полной вариации [12] по классу всех выпуклых борелевских множеств, из которой при $n \rightarrow \infty$ следует асимптотическая нормальность и локальная предельная теорема.

В отличие от следствия теоремы 13.3 из [14], где показано, что

$$|Q_n(B) - \Phi(C)| \leq C(r) \rho_4 2^{-n/2},$$

в теореме 2 удалось найти зависимость оценки скорости сходимости к нормальному закону от размерности вектора.

4. Предельные теоремы для вектора, состоящего из части автокорреляционных коэффициентов компонент случайного двоичного отображения

Рассмотрим вектор

$$A(f) = (r_{I_s}^{J_s}(f) : I_s \subset \{1, \dots, n\}; J_s \subset \{1, \dots, m\}; I_s \neq \emptyset, J_s \neq \emptyset; s \in \{1, \dots, r\}),$$

состоящий из r аддитивных автокорреляционных коэффициентов, где r — некоторое натуральное число и наборы множеств $(J_1, I_1), \dots, (J_r, I_r)$ удовлетворяют таким условиям:

Условия 2. Пусть выполняется следующее:

- 1) Зафиксирован набор непустых попарно различных подмножеств $J_1^*, \dots, J_p^*$ множества $\{1, \dots, m\}$, $p \in \{1, \dots, 2^m - 1\}$.
- 2) Для каждого $q \in \{1, \dots, p\}$ зафиксированы натуральное $d_q \in \{1, \dots, 2^n\}$ и набор произвольных попарно неравных непустых подмножеств $I_{q,1}, \dots, I_{q,d_q}$ множества $\{1, \dots, n\}$.

Обозначим $r = \sum_{q=1}^p d_q$, $k = \left| \bigcup_{q=1}^p \left(\bigcup_{j=1}^{d_q} I_{q,j} \right) \right|$, а пары множеств $(J_1^*, I_{1,1}), \dots, (J_1^*, I_{1,d_1}), (J_2^*, I_{2,1}), \dots, (J_p^*, I_{p,d_p})$ — через $(J_1, I_1), \dots, (J_d, I_d)$.

Обозначим распределение случайного вектора $2^{-(n+1)/2} A(f)$ через R_n и найдём расстояние между ним и r -мерным стандартным нормальным распределением в обобщённой метрике полной вариации [12] по классу всех выпуклых борелевских множеств.

Теорема 3. Дано случайное отображение $f = (f_1, f_2, \dots, f_m) \in B_n^m$ и выполняется набор условий 2. Тогда для любого выпуклого борелевского множества B выполняется неравенство

$$|R_n(B) - \Phi(B)| \leq 100r^{7/4}2^{2k-n/2}.$$

Доказательство. Пусть, без ограничения общности, $\bigcup_{q=1}^p \left(\bigcup_{j=1}^{d_q} I_{q,j} \right) = \{1, \dots, k\}$.

Обозначим $e_{I_{q,j}} \in V_n$, $j \in \{1, \dots, d_q\}$, $q \in \{1, \dots, p\}$, через $\gamma_1, \dots, \gamma_r$, где $e_I \in V_n$ введено при определении r_I^J .

Пусть $f^{J_i}(\beta) = \rho_i(\beta)$ для любых $i \in \{1, \dots, r\}$. Запишем

$$\begin{pmatrix} \|\rho_1(\beta) \oplus \rho_1(\beta \oplus \gamma_1)\| \\ \dots \\ \|\rho_r(\beta) \oplus \rho_r(\beta \oplus \gamma_r)\| \end{pmatrix} = \sum_{\beta \in V_n} \begin{pmatrix} \rho_1(\beta) \oplus \rho_1(\beta \oplus \gamma_1) \\ \dots \\ \rho_r(\beta) \oplus \rho_r(\beta \oplus \gamma_r) \end{pmatrix}.$$

Разобьём в получившейся сумме область суммирования на 2^{n-k} областей, соответствующих векторам β с одинаковыми последними $n-k$ координатами, набор которых обозначим α . Очевидно, что

$$\rho_{1+\sum_{i=1}^{q-1} d_i}(\beta) = \dots = \rho_{\sum_{i=1}^q d_i}(\beta) = g_q(\beta),$$

где g_q , $q \in \{1, \dots, p\}$, — попарно независимые случайные величины. Тогда

$$\sum_{\beta \in V_n} \begin{pmatrix} \rho_1(\beta) \oplus \rho_1(\beta \oplus \gamma_1) \\ \dots \\ \rho_r(\beta) \oplus \rho_r(\beta \oplus \gamma_r) \end{pmatrix} = \sum_{\alpha \in V_{n-k}} 2(\eta_\alpha^{q,i}, q \in \{1, \dots, p\}, i \in \{1, \dots, d_q\})^T = \sum_{\alpha \in V_{n-k}} \eta_\alpha,$$

где $\eta_\alpha^{q,i} = \frac{1}{2} \sum_{t \in V_k} (g_q(t\alpha) \oplus g_q(t\alpha \oplus \gamma_{q,i}))$.

Каждая компонента $\eta_\alpha^{q,i}$, $i \in \{1, \dots, d_q\}$, $q \in \{1, \dots, p\}$, имеет биномиальное распределение с параметрами $(2^{k-1}, 1/2)$. Следовательно, математическое ожидание каждой компоненты равно $E\eta_\alpha^{q,i} = 2^{k-2}$, а дисперсия $D\eta_\alpha^{q,i} = 2^{k-3}$.

Аналогично доказательству основной теоремы в [5], можно показать, что ковариационная матрица вектора η_α равна $2^{k-3}E_r$, где E_r — единичная матрица соответствующего размера.

Пусть f — случайная функция из B_n^m . Рассмотрим вектор $a(f) = 2^{-(n+1)/2} A(f)$.

Из определения автокорреляционных коэффициентов следует, что

$$a(f) = 2^{-\frac{n-k}{2}} \sum_{\alpha \in V_{n-k}} \left(2^{\frac{3-k}{2}} (2^{k-2} - \eta_\alpha^{q,i}), q \in \{1, \dots, p\}, i \in \{1, \dots, d_q\} \right)^T = 2^{-\frac{n-k}{2}} \sum_{\alpha \in V_n} \xi(\alpha).$$

Рассмотрим набор из 2^{n-k} величин $\xi(\alpha)$, $\alpha \in V_{n-k}$, — независимых одинаково распределённых в $\mathbb{R}^r$ случайных векторов с единичной ковариационной матрицей и нулевым средним. В этих условиях, как и в теореме 1, выполняется результат из [11]. Несложно показать, что

$$E(\xi(\alpha))^3 \leq r^{\frac{3}{2}} 2^{\frac{3k-3}{2}}.$$

Следовательно, выполняется неравенство $|R_n(B) - \Phi(B)| \leq 400r^{1/4}r^{3/2}2^{(3k-3)/2}2^{-(n-k)/2}$. Теорема доказана. ■

Из этой теоремы следует равномерная по r оценка расстояния между распределением вектора $2^{-(n+1)/2} A(f)$ и многомерным стандартным нормальным распределением в равномерной метрике, стремящаяся к нулю, т. е. опять получаются асимптотическая нормальность и интегральная предельная теорема.

Из доказательства теоремы 3 следует равенство

$$(r_{I_s}^{J_s}(f) : s \in \{1, \dots, r\}) = \sum_{\alpha \in V_n} \xi(\alpha) = \sum_{\alpha \in V_{n-k}} (4(2^{k-2} - \eta_{\alpha}^{q,i}), q \in \{1, \dots, p\}, i \in \{1, \dots, d_q\})^T,$$

где случайные величины $\eta_{\alpha}^{q,i}$ введены при доказательстве теоремы 3.

Рассмотрим набор из 2^{n-k} величин $\xi(\alpha)$, $\alpha \in V_{n-k}$, — независимых одинаково распределённых в $\mathbb{R}^r$ случайных векторов с ковариационной матрицей $2^{k+1}E_r$ и нулевым средним.

Легко показать, что $\|\xi(\alpha)\| \leq \sqrt{r}2^k$ и $E(\|\xi(\alpha)\|^\beta) \leq r^{\beta/2}2^{k\beta} < \infty$ при всех вещественных $\beta \in (0, 2)$. Таким образом, попадаем в условия основной теоремы из [9], согласно которой верно

Утверждение 9. Пусть $n \rightarrow \infty$, m — произвольное натуральное число, $\beta \in (0, 2)$ — вещественное число. Тогда для любых попарно различных наборов множеств $(J_1, I_1), \dots, (J_r, I_r)$, удовлетворяющих условиям 2, норма вектора $2^{-n/\beta} A(f)$ сходится к нулю с вероятностью 1.

Данное утверждение при $\beta = 1$ является формулировкой усиленного закона больших чисел для случайных векторов $\xi(\alpha)$, $\alpha \in V_n$.

Теперь рассмотрим вопрос о скорости сходимости к нулю нормы вектора $2^{-n/\beta} A(f)$. Так как $\|\xi(\alpha)\| \leq \sqrt{r}2^k$ и $E(\|\xi(\alpha)\|^2) \leq r2^{2k}$, то при всех $n - k \geq \log_2 r$ попадаем в условия основной теоремы из [16], из которой следует

Утверждение 10. Пусть n, m — произвольные натуральные числа, $\beta \in (0, 2)$ — вещественное число. Тогда для любых попарно различных $(J_1, I_1), \dots, (J_r, I_r)$, удовлетворяющих условиям 2, таких, что $n - k \geq \log_2 r$, и для любого $\varepsilon > 0$ верно

$$P\{\|2^{-n/\beta} A(f)\| \geq \varepsilon\} \leq \left(1 + \frac{e^{5/12}}{\sqrt{2\pi}}\right) \exp\left\{-\frac{\varepsilon^2}{re^2} 2^{\frac{(2-\beta)n}{\beta} - k - 3}\right\}.$$

Заключение

В данной работе удалось доказать асимптотическую нормальность совместного распределения части автокорреляционных и спектральных коэффициентов и весов подфункций компонент двоичных вектор-функций. Следующий этап в изучении векторов из части этих характеристик, в том числе и растущей размерности, — это построение локальных предельных теорем, полезных для изучения криптографических свойств функций. В частности, стоят задачи обобщения на m -мерный случай результатов [4, 6] и усиления фактически доказанной в [5] локальной предельной теоремы для вектора, состоящего из части автокорреляционных коэффициентов одной компоненты с I , мощность которых равна 1.

ЛИТЕРАТУРА

1. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 472 с.
2. Яценко В. В. Свойства булевых отображений, сводимые к свойствам их координатных функций // Вестник МГУ. Сер. Математика. 1997. Т. 33. № 1. С. 11–13.

3. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. New York: Cambridge University Press, 2010. P. 398–472.
4. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. Т. 12. № 1. С. 82–95.
5. *Панков К. Н.* Верхняя граница для числа функций, удовлетворяющих строгому лавинному критерию // Дискретная математика. 2005. Т. 17. № 2. С. 95–101.
6. *Рязанов Б. В.* О распределении спектральной сложности булевых функций // Дискретная математика. 1994. Т. 6. № 2. С. 111–129.
7. *Таранников Ю. В.* Комбинаторные свойства дискретных структур и приложения к криптологии. М.: МЦНМО, 2011. 152 с.
8. *Халевин А. В.* Оценка нелинейности корреляционно-иммунных булевых функций // Прикладная дискретная математика. 2011. № 1. С. 34–69.
9. *Азларов Т. А., Володин Н. А.* Законы больших чисел для одинаково распределенных базисовых значений случайных величин // Теория вероятностей и её применения. 1981. Т. 26. № 3. С. 584–590.
10. *Кахан Ж.-П.* Случайные функциональные ряды. М.: Мир, 1973. 304 с.
11. *Bentkus V.* On the dependence of the Berry-Esseen bound on dimension // J. Stat. Plan. Infer. 2003. V. 113. No. 2. P. 385–402.
12. *Золотарев В. М.* О свойствах и связях некоторых типов метрик // Записки научных семинаров ЛОМИ. 1979. Т. 87. С. 18–35.
13. *Padgett W. J. and Taylor R. L.* Laws of Large Numbers for Normed Linear Spaces and Certain Frechet Spaces. New York: Springer, 1973. 117 p.
14. *Бхаттачария Р. Н., Ранга Р.* Аппроксимация нормальным распределением и асимптотические разложения. М.: Наука, 1982. 288 с.
15. *Bhattacharya R. N.* Rates of weak convergence for the multidimensional central limit theorem // Теория вероятностей и её применения. 1970. Т. 15. № 1. С. 69–85.
16. *Прохоров Ю. В.* Распространение неравенств С. Н. Бернштейна на многомерный случай // Теория вероятностей и её применения. 1968. Т. 13. № 2. С. 266–274.