

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.214

ОБ АСИМПТОТИЧЕСКОЙ НОРМАЛЬНОСТИ ЧАСТОТ ЗНАКОВ В МУЛЬТИЦИКЛИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Н. М. Меженная*, В. Г. Михайлов**

*Московский государственный технический университет им. Н. Э. Баумана,
г. Москва, Россия

**Математический институт им. В. А. Стеклова РАН, г. Москва, Россия

Доказана многомерная центральная предельная теорема для частот знаков в мультициклической последовательности, образованной сложением знаков из $r \geq 2$ независимых в совокупности векторов взаимно простых длин $n_1, \dots, n_r$ из независимых случайных величин, распределённых равномерно на некотором конечном алфавите, когда длины регистров $n_1, \dots, n_r \rightarrow \infty$, а размер алфавита фиксирован. Получена оценка скорости сходимости в равномерной метрике одномерного закона распределения любой из частот знаков (при подходящей нормировке) к стандартному нормальному закону.

Ключевые слова: мультициклическая последовательность, центральная предельная теорема, частоты знаков, метод Янсона.

DOI 10.17223/20710410/48/1

ON THE ASYMPTOTIC NORMALITY OF THE FREQUENCIES OF LETTERS IN A MULTICYCLIC SEQUENCE

N. M. Mezhenaya*, V. G. Mikhailov**

*Bauman Moscow State Technical University, Moscow, Russia

**Steklov Mathematical Institute of Russian Academy of Sciences, Moscow, Russia

E-mail: natalia.mezhenaya@gmail.com, mikhail@mi-ras.ru

The paper presents a multidimensional central limit theorem for frequencies $\xi_{y,T}$ of letters y , $y \in \{0, 1, \dots, N-1\}$, $N \geq 2$, in a multicyclic sequence of length T formed by addition letters from r , $r \geq 2$, independent vectors of coprime lengths $n_1, \dots, n_r$ consisted of independent random variables distributed uniformly on the set $\{0, 1, \dots, N-1\}$: if the lengths of the registers $n_1, \dots, n_r \rightarrow \infty$, the size of the alphabet N is fixed, and $T \left(\sum_{k=1}^r n_k^{-1} \right)^{2(1-1/m)} \rightarrow 0$ for some natural number $m \geq 3$, then the random vector $(T/N)^{-1/2}(\xi_{0,T} - T/N, \dots, \xi_{N-2,T} - T/N)$ converge in distribution to the $(N-1)$ -dimensional normal law with zero mean and non-degenerate covariance matrix. We also obtain an estimate for the rate of convergence in the uniform metric of the one-dimensional distribution function of any of the frequencies $\xi_{y,T}$ to the

distribution function of the standard normal law Φ of the form

$$\left| \mathbb{P} \left\{ \xi_{y,T} < \frac{T}{N} + \frac{x}{N} \sqrt{T(N-1)} \right\} - \Phi(x) \right| \leq CT^{3/4} \left(\sum_{k=1}^r n_k^{-1} \right)$$

for any $y \in \mathcal{A}_N$, $x \in \mathbb{R}$, where $C > 0$ is known constant.

Keywords: *multicyclic sequence, central limit theorem, frequencies of letters, Jan-son's method.*

Введение

Пусть заданы $r \geq 2$ независимых (в совокупности) наборов $(X_l^{(k)}, l = 0, \dots, n_j - 1)$, $k = 1, \dots, r$, взаимно простых длин $n_1, \dots, n_r \geq 2$ из независимых случайных величин, распределённых равномерно на множестве $\mathcal{A}_N = \{0, 1, \dots, N - 1\}$, $N \geq 2$. В работе рассматривается простейшая мультициклическая случайная последовательность [1], которая строится по правилу

$$Z_t = \bigoplus_{k=1}^r X_{t(n_k)}^{(k)}, \quad t = 0, 1, 2, \dots, n_1 \dots n_r - 1, \quad (1)$$

где $\oplus$ — операция сложения по модулю N , $t(n_k) = t \bmod n_k$.

Впервые свойства мультициклической последовательности (1) при $N = 2$ описаны Питером Полем (Peter Pohl) в диссертации [2] (её основные результаты опубликованы в [1]) в связи с изучением свойств генератора случайных чисел специального вида. В российской литературе этот генератор носит название *генератор Пола* (или *двоичный генератор Пола*).

Мультициклическая последовательность (1) является чисто периодической и имеет период (возможно, не минимальный) длины $L = n_1 n_2 \dots n_r$. Поэтому при исследовании числа единиц рассматривается отрезок выходной последовательности $(Z_0, \dots, Z_{L-1})$, называемый *циклом*. Для определения всех L значений знаков Z_t нужно сгенерировать $n_1 + \dots + n_r$ двоичных случайных знаков.

Известно, что любые двойки, тройки и пятёрки знаков последовательности (1), лежащие в цикле длины L , состоят из независимых между собой случайных величин [1, теорема 4]. Четвёрки знаков могут быть зависимы, только если расстояние между знаками в ней не меньше $2\sqrt{L}$ [1, теорема 5]. В теореме 7 [1] также отмечено, что при длине последовательности (1) меньше $2\sqrt{L}$ четвёрки знаков ведут себя как независимые случайные величины. Приведённые свойства мультициклической последовательности позволяют сделать вывод о том, что она может быть использована для построения последовательности псевдослучайных чисел, например, вместо линейного конгруэнтного метода [3]. Для вывода этих теорем в [1] использованы свойства соответствующего характеристического многочлена.

Аналогичные исследования выходной последовательности фильтрующего и комбинирующего генераторов проведены в [4] и [5, 6] соответственно. Свойства таких генераторов подробно описаны в [7–10].

В [1] приведена постановка задачи о выполнении центральной предельной теоремы для величин, строящихся из наборов по ω последовательных элементов двоичной мультициклической последовательности, используемых для генерации целых чисел из диапазона $\{0, \dots, 2^\omega - 1\}$. В настоящей работе рассматривается другая постановка: изучаются свойства распределения вектора частот знаков $y \in \mathcal{A}_N$ в отрезке мультициклической случайной последовательности длины $T < L$ над произвольным конечным алфавитом.

Рассмотрим набор случайных величин

$$\xi_{y,T} = \sum_{t=0}^{T-1} I\{Z_t = y\}, \quad y \in \mathcal{A}_N, \quad (2)$$

равных числам знаков y среди первых T знаков мультициклической последовательности (1).

В работе изучены свойства предельных распределений частот знаков $\xi_{0,T}, \dots, \xi_{N-1,T}$ в мультициклической последовательности (1) длины $T < L$. В частности, показано, что совместное предельное распределение частот знаков в мультициклической последовательности длины T при определённых ограничениях на величину T сходится к многомерному нормальному распределению.

1. Предельные теоремы

Величины в наборе (2) для любого $T \geq 1$ связаны равенством

$$\sum_{y \in \mathcal{A}_N} \xi_{y,T} = T,$$

поэтому далее будем рассматривать $(N-1)$ -мерный случайный вектор

$$\xi_T = (\xi_{0,T}, \dots, \xi_{N-2,T}). \quad (3)$$

Обозначим E_n единичную матрицу размера $n \times n$, $\mathbf{1}_{n \times n}$ — матрицу размера $n \times n$, все элементы которой равны единице,

$$\begin{aligned} \xi_{y,T}^* &= \frac{\xi_{y,T} - T/N}{\sqrt{T/N}}, \quad y \in \mathcal{A}_N, \\ \xi_T^* &= (\xi_{0,T}^*, \dots, \xi_{N-2,T}^*). \end{aligned}$$

Теорема 1. Пусть параметры $N, r \geq 2$, целые числа $n_1, \dots, n_r \geq 2$ взаимно просты, $X_l^{(k)}$, $l = 0, \dots, n_k - 1$, $k = 1, \dots, r$, — независимые в совокупности случайные величины, распределённые равномерно на $\mathcal{A}_N$, $1 \leq T \leq L-1$. Пусть $T, n_1, \dots, n_r \rightarrow \infty$, число N фиксировано и параметр r меняется так, что существует натуральное число $m \geq 3$, такое, что

$$T \left(\sum_{k=1}^r \frac{1}{n_k} \right)^{2(1-1/m)} \rightarrow 0. \quad (4)$$

Тогда закон распределения случайного вектора $\xi_T^* = (\xi_{0,T}^*, \dots, \xi_{N-2,T}^*)$ сходится к $(N-1)$ -мерному нормальному закону с нулевым средним и ковариационной матрицей $\Sigma_{\xi_T^*} = E_{N-1} - \frac{1}{N} \mathbf{1}_{(N-1) \times (N-1)}$.

Замечание 1. Пусть $r \geq 2$ и $2 \leq n_1 < \dots < n_r$. Тогда $\sum_{k=1}^r \frac{1}{n_k} \leq \frac{r}{n_1}$. Поэтому условие (4) теоремы 1 принимает вид $T = o(n_1^{2(1-1/m)})$, $n_1 \rightarrow \infty$.

Замечание 2. Для выполнения условия (4) достаточно, чтобы

$$T = o \left(\left(\sum_{k=1}^r \frac{1}{n_k} \right)^{-2+\varepsilon} \right), \quad n_1, \dots, n_r \rightarrow \infty,$$

при сколь угодно малом $\varepsilon > 0$.

Замечание 3. Пусть $r = 2$ и $n_1, n_2 \rightarrow \infty$. Тогда условие (4) эквивалентно тому, что $T = o((n_1 + n_2)^{2-\varepsilon})$ при сколь угодно малом $\varepsilon > 0$.

Для каждой компоненты вектора ξ_T^* можно получить явную оценку скорости сходимости её функции распределения к функции распределения нормального закона Φ в равномерной метрике.

Теорема 2. Пусть параметры $N, r \geq 2$, целые числа $n_1, \dots, n_r \geq 2$ взаимно просты, $X_l^{(k)}, l = 0, \dots, n_k - 1, k = 1, \dots, r$, — независимые в совокупности случайные величины, распределённые равномерно на $\mathcal{A}_N$, $1 \leq T \leq L - 1$. Тогда для любого $y \in \mathcal{A}_N$ и $x \in \mathbb{R}$

$$\left| \mathbb{P} \left\{ \xi_{y,T} < \frac{T}{N} + \frac{x}{N} \sqrt{T(N-1)} \right\} - \Phi(x) \right| \leq CT^{3/4} \left(\sum_{k=1}^r \frac{1}{n_k} \right), \quad (5)$$

где $C = 32(1 + \sqrt{6}) \left(\frac{N}{\sqrt{N-1}} \right)^{3/2}$.

Замечание 4. Правая часть оценки (5) стремится к нулю при $T, n_1, \dots, n_r \rightarrow \infty$, если $T = o \left(\left(\sum_{k=1}^r \frac{1}{n_k} \right)^{4/3} \right)$, что соответствует выполнению условия (4) при $m = 3$.

Теорема 3 [11, теорема 1]. Пусть параметр $r \geq 2$ остаётся фиксированным, целые числа $n_1, \dots, n_r \geq 2$ взаимно просты, $X_l^{(k)}, l = 0, \dots, n_k - 1, k = 1, \dots, r$, — независимые в совокупности случайные величины, распределённые равномерно на $\{0, \dots, 3\}$. Тогда закон распределения случайного вектора $\xi_L^* = (\xi_{0,L}^*, \dots, \xi_{3,L}^*)$ сходится при $n_1, \dots, n_r \rightarrow \infty$ к закону распределения случайного вектора

$$(\eta_r + 2^{1-r/2} \rho_r \cos \phi, -\eta_r + 2^{1-r/2} \rho_r \cos \phi, \eta_r - 2^{1-r/2} \rho_r \cos \phi, -\eta_r - 2^{1-r/2} \rho_r \cos \phi).$$

Здесь η_r, ρ_r и ϕ — независимые (в совокупности) случайные величины, где η_r распределена как произведение r независимых (в совокупности) стандартных нормальных случайных величин, ρ_r — как произведение r независимых (в совокупности) случайных величин, каждая из которых распределена по закону Рэлея с плотностью $f(x) = xe^{-x^2/2}$, $x \geq 0$, а ϕ имеет равномерное распределение на единичной окружности.

Таким образом, совместное предельное распределение частот знаков в мультициклической последовательности при существенно больших, чем в теореме 1, значениях T может существенно отличаться от приведённого в теореме 1.

Замечание 5. Для двоичной мультициклической последовательности в [12] выведена формула, связывающая число единиц $\xi_{1,L}$ с числами единиц в наборах $(X_l^{(k)}, l = 0, \dots, n_k - 1), k = 1, \dots, r$. С помощью этой формулы получена оценка скорости сходимости в равномерной метрике функции распределения центрированного и нормированного числа единиц $\xi_{1,L}^*$ к функции распределения Φ_r произведения r независимых (в совокупности) стандартных нормальных случайных величин, когда числа $n_1, \dots, n_r$ нечётны и взаимно просты, случайные величины $X_l^{(k)}, l = 0, \dots, n_k - 1, k = 1, \dots, r$, независимы в совокупности и распределены равномерно на $\{0, 1\}$, следующего вида:

$$|\mathbb{P} \{ \xi_{1,L}^* < x \} - \Phi_r(x)| \leq C_{\text{BE}} \sum_{k=1}^r \frac{1}{\sqrt{n_k}},$$

где C_{BE} — константа из неравенства Берри — Эссеена [13, теорема 1]. Из этой оценки следует, что при выполнении указанных условий для центрированного и нормированного числа единиц $\xi_{1,L}^*$ при фиксированном $r \geq 2$ предельной при $n_1, \dots, n_r \rightarrow \infty$

функцией распределения будет Φ_r . Этот результат существенно отличается от предельного закона в теореме 2.

Аналогичные исследования последовательности вида (1) при $N = 2$ и 4 с неравновероятными заполнениями регистров проведены в [14] и [15] соответственно. В частности, показано, что при определённых предположениях предельным распределением для частот знаков будет нормальное распределение.

2. Доказательства

2.1. Доказательство теоремы 1

Согласно теореме Крамера — Уолда [16, теорема 7.7, с. 76], достаточно показать, что для любого $\alpha = (\alpha_0, \dots, \alpha_{N-1}) \in \mathbb{R}^{N-1}$, $\alpha \neq (0, \dots, 0)$, линейная комбинация $\langle \alpha, \xi_T \rangle$ имеет в пределе нормальное распределение (здесь и далее через $\langle \cdot, \cdot \rangle$ обозначено скалярное произведение). Для доказательства этой сходимости воспользуемся следующим результатом работы [17].

Пусть $\{\eta_v, v \in V_n\}$ — семейство случайных величин, где V_n — произвольное множество, возможно зависящее от параметра n . Напомним (см. [17]), что граф зависимостей $\Gamma_n = (V_n, E_n)$ для семейства $\{\eta_v, v \in V_n\}$ — это граф с множеством вершин V_n , который обладает следующим свойством: для любых множеств $V_1, V_2 \subset V_n$, $V_1 \cap V_2 = \emptyset$, таких, что между ними нет рёбер Γ_n , наборы случайных величин $\{\eta_v, v \in V_1\}$ и $\{\eta_v, v \in V_2\}$ независимы.

Теорема 4 [17, Theorem 2]. Пусть $\{\eta_v, v \in V_n\}$ — семейство случайных величин с графом зависимостей $\Gamma_n = (V_n, E_n)$, M_n — максимальная степень вершины в графе Γ_n и существует константа A_n , такая, что $|\eta_v| \leq A_n$ почти наверное для всех $v \in V_n$. Пусть $W_n = \sum_{v \in V_n} \eta_v$ и $\sigma_n^2 = \text{DW}_n$. Тогда если существует такое натуральное число m , что при $n \rightarrow \infty$

$$\frac{|V_n|}{M_n} \left(\frac{M_n A_n}{\sigma_n} \right)^m \rightarrow 0, \quad (6)$$

то при $n \rightarrow \infty$

$$\mathbb{P} \left\{ \frac{W_n - \mathbb{E}W_n}{\sigma_n} < x \right\} \rightarrow \Phi(x)$$

при всех $x \in \mathbb{R}$.

Перейдём к доказательству теоремы 1. При $n_1 \leq t \leq n_1 \dots n_r - 1$ каждому значению t соответствует единственный набор индексов $\mathbf{i}_t = (i_{1,t}, \dots, i_{r,t})$, $i_{k,t} = t(n_k)$, $k = 1, \dots, r$. Будем использовать обозначение $t_{\mathbf{i}}$ для значения t , которому соответствует набор индексов $\mathbf{i}_t = (i_{1,t}, \dots, i_{r,t})$. Тогда

$$\xi_{y,T} = \sum_{\mathbf{i}_t: t=0, \dots, T-1} I\{Z_{\mathbf{i}_t} = y\}, \quad y \in \mathcal{A}_{N-1}.$$

Рассмотрим набор случайных величин

$$\left\{ w_{y,t} = \alpha_y I\{Z_{\mathbf{i}_t} = y\} : t = 0, \dots, T-1, y \in \mathcal{A}_{N-1} \right\}. \quad (7)$$

Тогда $\langle \alpha, \xi_T \rangle = \sum_{t=0}^{T-1} \sum_{y \in \mathcal{A}_{N-1}} w_{y,t}$.

Построим для набора (7) граф зависимостей $\Gamma_T = (V_T, E_T)$, в котором множество вершин $V_T = \{(y, t) : t = 0, 1, \dots, T-1, y \in \mathcal{A}_{N-1}\}$, а множество рёбер определяется следующими правилами:

- 1) есть петли при всех вершинах;
- 2) вершины (y_1, t_1) и (y_2, t_2) связаны ребром, если наборы $\mathbf{i}_{t_1}$ и $\mathbf{i}_{t_2}$ таковы, что существует номер $k \in \{1, \dots, r\}$, для которого $i_{k,t_1} = i_{k,t_2}$.

Таким образом, граф $\Gamma_T = (V_T, E_T)$ является графом зависимостей и удовлетворяет требованиям теоремы 4. Тогда

$$|V_T| = (N - 1)T. \quad (8)$$

Обозначим M_T максимальную степень вершины в графе Γ_T . Пусть зафиксировано значение t_1 и, следовательно, $\mathbf{i}_{t_1}$. Вычислим максимальное число вершин в Γ_T , с которыми (y_1, t_1) связана ребрами. Начнём с вершин (y_2, t_2) , для которых $i_{1,t_1} = i_{1,t_2}$, а остальные элементы $i_{2,t_2}, \dots, i_{r,t_2}$ любые. Всего таких вершин не более $(N - 1)[T/n_1]$. Аналогично для других наборов совпадающих индексов. Тогда

$$M_T \leq (N - 1) \sum_{k=1}^r [T/n_k]. \quad (9)$$

Воспользуемся также следующим утверждением, которое доказано далее в п. 2.3.

Лемма 1. Пусть выполнены условия теоремы 2. Тогда для всех $y, z \in A_N, y \neq z$,

$$E\xi_{y,T} = \frac{T}{N}, \quad D\xi_{y,T} = \frac{T}{N} \left(1 - \frac{1}{N}\right); \quad (10)$$

$$\text{cov}(\xi_{y,T}, \xi_{z,T}) = -\frac{T}{N^2}. \quad (11)$$

Из (10) и (11) следует, что

$$E\langle \alpha, \xi_T \rangle = \langle \alpha, E\xi_T \rangle = \frac{T}{N} \langle \alpha, \mathbf{1}_{n \times 1} \rangle = \frac{T}{N} \sum_{y \in A_{N-1}} \alpha_y,$$

$$D\langle \alpha, \xi_T \rangle = \langle \alpha, \Sigma_{\xi_T} \alpha \rangle,$$

где Σ_{ξ_T} — ковариационная матрица вектора ξ_T , в которой все диагональные элементы одинаковы между собой и определяются формулой (10), а остальные элементы также одинаковы между собой и определяются формулой (11). Тогда

$$\begin{aligned} D\langle \alpha, \xi_T \rangle &= \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 D\xi_{y,T} + \sum_{\substack{y, z \in \mathcal{A}_{N-1}: \\ y \neq z}} \alpha_y \alpha_z \text{cov}(\xi_{y,T}, \xi_{z,T}) = \\ &= \frac{T}{N^2} \left((N - 1) \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 - \sum_{\substack{y, z \in \mathcal{A}_{N-1}: \\ y \neq z}} \alpha_y \alpha_z \right) \end{aligned} \quad (12)$$

(в последней формуле считается, что сумма по пустому множеству равна 0). Заметим, что в (12) $D\langle \alpha, \xi_T \rangle > 0$ при $\alpha \neq (0, \dots, 0)$. Действительно,

$$(N - 1) \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 + \sum_{\substack{y, z \in \mathcal{A}_{N-1}: \\ y \neq z}} \alpha_y \alpha_z = (N - 1) \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 > 0,$$

если $N = 2$. При $N \geq 3$ в силу неравенства Йенсена [18, с. 336], согласно которому

$$(N - 1) \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 - \left(\sum_{y \in \mathcal{A}_{N-1}} \alpha_y \right)^2 \geq 0,$$

причём последнее неравенство выполняется в форме равенства, только если $\alpha_0 = \alpha_1 = \dots = \alpha_{N-1}$, имеем

$$(N-1) \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 - \sum_{\substack{y, z \in \mathcal{A}_{N-1}: \\ y \neq z}} \alpha_y \alpha_z = N \sum_{y \in \mathcal{A}_{N-1}} \alpha_y^2 - \left(\sum_{y \in \mathcal{A}_{N-1}} \alpha_y \right)^2 > 0,$$

так как $\alpha \neq (0, \dots, 0)$. Значит, в условиях теоремы $\sigma_T^2 = D\langle \alpha, \xi_T \rangle \asymp T$. Здесь и далее запись $A_n \asymp B_n$ при $n \rightarrow \infty$ означает, что существует $\lim_{n \rightarrow \infty} \frac{A_n}{B_n} = c \in (0; \infty)$.

Воспользуемся оценкой (6). Учитывая, что $A_T = \max\{|\alpha_y|, y \in \mathcal{A}_{N-1}\}$, из (6) и (9) имеем

$$\frac{|V_T|}{M_T} \left(\frac{M_T A_T}{\sigma_T} \right)^m \asymp T^{m/2} \left(\sum_{k=1}^r \frac{1}{n_k} \right)^{m-1}.$$

Правая часть последнего соотношения стремится к нулю при выполнении условия (4) теоремы 1. Значит, согласно теореме 4, случайная величина

$$\frac{\langle \alpha, \xi_T \rangle - E\langle \alpha, \xi_T \rangle}{\sigma_T}$$

распределена в пределе при $T, n_1, \dots, n_r \rightarrow \infty$ по стандартному нормальному закону. Так как вектор α был выбран произвольно, то по теореме Крамера — Уолда [16, теорема 7.7, с. 76] получаем, что вектор ξ_T и связанный с ним линейным преобразованием вектор ξ_T^* (при подходящей нормировке) имеют в пределе $(N-1)$ -мерные нормальные законы распределения.

Остаётся заметить, что из формул (10) следует, что для каждой компоненты $\xi_{y,T}^* = \frac{\xi_{y,T} - T/N}{\sqrt{T/N}}$ вектора ξ_T^* , определённого формулой (3), имеет место

$$E\xi_{y,T}^* = 0, \quad D\xi_{y,T}^* = 1 - \frac{1}{N}, \quad y \in \mathcal{A}_N,$$

а из (11) получаем

$$\text{cov}(\xi_{y,T}^*, \xi_{z,T}^*) = -\frac{1}{N}, \quad y, z \in \mathcal{A}_N, \quad y \neq z.$$

Значит, $E\xi_T^* = (0, \dots, 0)$ и $\Sigma_{\xi_T^*} = E_{N-1} - \frac{1}{N} \mathbf{1}_{(N-1) \times (N-1)}$. ■

2.2. Доказательство теоремы 2

Воспользуемся следующим результатом.

Теорема 5 [19, Corollary 2]. В условиях теоремы 4

$$\left| P \left\{ \frac{W_n - EW_n}{\sigma_n} < x \right\} - \Phi(x) \right| \leq 32(1 + \sqrt{6})Q^{1/2}, \quad (13)$$

$$Q = \frac{|V_n| M_n^2 A_n^3}{\sigma_n^3},$$

при всех $x \in \mathbb{R}$.

Так как закон распределения случайных величин $\xi_{y,T}$ одинаков для всех $y \in \mathcal{A}_N$, достаточно доказать утверждение теоремы при $y = 0$. Для этого воспользуемся результатами, полученными при доказательстве теоремы 1.

Набору случайных индикаторов $\{I\{Z_t = 0\}, t = 0, \dots, T-1\}$ соответствует часть графа зависимостей $\Gamma_T = (V_T, E_T)$ с вершинами $\{(0, t) : t = 0, \dots, T-1\}$ и рёбрами, соединяющими вершины $(0, t_1)$ и $(0, t_2)$. Такой граф также является графом зависимостей и удовлетворяет требованиям теорем 4 и 5. В нём число вершин и максимальная степень вершины описываются формулами (8) и (9) соответственно при $N = 2$.

В силу определения (2) имеем $A_T = 1$. Тогда с учётом (10) получим

$$Q \leq \frac{T \left(\sum_{k=1}^r \frac{T}{n_k} \right)^2}{\left(\frac{T}{N} \left(1 - \frac{1}{N} \right) \right)^{3/2}} = T^{3/2} \left(\frac{N}{\sqrt{N-1}} \right)^3 \left(\sum_{k=1}^r \frac{1}{n_k} \right)^2.$$

Тогда, согласно (10) и (13),

$$\begin{aligned} & \left| \mathbb{P} \left\{ \xi_{y,T} < \frac{T}{N} + \frac{x}{N} \sqrt{T(N-1)} \right\} - \Phi(x) \right| = \\ & = \left| \mathbb{P} \left\{ \left(\frac{T}{N} \left(1 - \frac{1}{N} \right) \right)^{-1/2} \left(\xi_{y,T} - \frac{T}{N} \right) < x \right\} - \Phi(x) \right| \leq 32(1 + \sqrt{6})Q^{1/2} = CT^{3/4} \left(\sum_{k=1}^r \frac{1}{n_k} \right). \end{aligned}$$

Значит, имеет место оценка (5). ■

2.3. Доказательство леммы 1

Начнём с вычисления математического ожидания. Так как $\mathbb{P}\{Z_t = y\} = 1/N$, $y \in \mathcal{A}_N$, то

$$\mathbb{E}I\{Z_t = y\} = \frac{1}{N}, \quad \mathbb{D}I\{Z_t = y\} = \frac{1}{N} \left(1 - \frac{1}{N} \right), \quad \mathbb{E}\xi_{y,T} = \sum_{t=0}^{T-1} \mathbb{P}\{Z_t = 1\} = \frac{T}{N}.$$

Вычислим вероятность $\mathbb{P}\{Z_{t_1} = y, Z_{t_2} = z\}$ при $0 \leq t_1 < t_2 \leq T, y, z \in \mathcal{A}_N$. Так как длины регистров $n_1, \dots, n_r$ взаимно просты, при любых $0 \leq t_1 < t_2 \leq T$ наборы $\mathbf{i}_{t_1}$ и $\mathbf{i}_{t_2}$ имеют не более $r-1$ одинаковых элементов на одних и тех же местах.

Пусть наборы $\mathbf{i}_{t_1}$ и $\mathbf{i}_{t_2}$ имеют ровно l , $1 \leq l \leq r-1$, общих элементов на одних и тех же местах $1 \leq k_1 < \dots < k_l \leq r$: $i_{u,t_1} = i_{u,t_2}, u \in \{k_1, \dots, k_l\}$, и $i_{u,t_1} \neq i_{u,t_2}, u \in \{1, \dots, r\} \setminus \{k_1, \dots, k_l\}$. Тогда

$$\begin{aligned} \mathbb{P}\{Z_{t_1} = y, Z_{t_2} = z\} &= \mathbb{P} \left\{ \bigoplus_{u=1}^r X_{i_{u,t_1}}^{(u)} = y, \bigoplus_{u=1}^r X_{i_{u,t_2}}^{(u)} = z \right\} = \\ &= \sum_{a \in \mathcal{A}_N} \mathbb{P} \left\{ \bigoplus_{u \in \{k_1, \dots, k_l\}} X_{i_{u,t_1}}^{(u)} = a, \bigoplus_{u \in \{1, \dots, r\} \setminus \{k_1, \dots, k_l\}} X_{i_{u,t_1}}^{(u)} = y \oplus a, \right. \\ & \quad \left. \bigoplus_{u \in \{1, \dots, r\} \setminus \{k_1, \dots, k_l\}} X_{i_{u,t_2}}^{(u)} = z \oplus a \right\} = \\ &= \sum_{a \in \mathcal{A}_N} \mathbb{P} \left\{ \bigoplus_{u \in \{k_1, \dots, k_l\}} X_{i_{u,t_1}}^{(u)} = a \right\} \mathbb{P} \left\{ \bigoplus_{u \in \{1, \dots, r\} \setminus \{k_1, \dots, k_l\}} X_{i_{u,t_1}}^{(u)} = y \oplus a \right\} \times \\ & \times \mathbb{P} \left\{ \bigoplus_{u \in \{1, \dots, r\} \setminus \{k_1, \dots, k_l\}} X_{i_{u,t_2}}^{(u)} = z \oplus a \right\} = N \cdot \frac{1}{N^3} = \frac{1}{N^2} = \mathbb{P}\{Z_{t_1} = y\} \mathbb{P}\{Z_{t_2} = z\}. \end{aligned}$$

Таким образом, Z_{t_1} и Z_{t_2} попарно независимы при $0 \leq t_1 < t_2 \leq T$. Тогда

$$D\xi_{y,T} = \sum_{t=0}^{T-1} DI\{Z_t = y\} = \frac{T}{N} \left(1 - \frac{1}{N}\right), \quad y \in \mathcal{A}_N.$$

Тем самым формулы (10) доказаны.

Перейдём к вычислению ковариации. Так как при $y, z \in \mathcal{A}_N$, $y \neq z$, $\text{cov}(I\{Z_{t_1} = y\}, I\{Z_{t_2} = z\}) = 0$, если $t_1 \neq t_2$, и

$$\text{cov}(I\{Z_{t_1} = y\}, I\{Z_{t_1} = z\}) = P\{Z_{t_1} = y, Z_{t_1} = z\} - P\{Z_{t_1} = y\}P\{Z_{t_1} = z\} = -\frac{1}{N^2},$$

то, согласно определению (2), при $y, z \in \mathcal{A}_N$, $y \neq z$,

$$\begin{aligned} \text{cov}(\xi_{y,T}, \xi_{z,T}) &= \sum_{t_1=0}^{T-1} \sum_{t_2=0}^{T-1} \text{cov}(I\{Z_{t_1} = y\}, I\{Z_{t_2} = z\}) = \\ &= \sum_{t_1=0}^{T-1} \text{cov}(I\{Z_{t_1} = y\}, I\{Z_{t_1} = z\}) = -\frac{T}{N^2}. \end{aligned}$$

Лемма доказана. ■

Заключение

Доказана многомерная центральная предельная теорема для частот знаков в отрезке мультициклической последовательности длиной много меньше длины периода с оценками скорости сходимости в равномерной метрике для отдельных компонент в предположении, что знаки, формирующие последовательность, независимы в совокупности и распределены равномерно на конечном алфавите.

Авторы выражают признательность рецензенту за полезные замечания и внимание к работе.

ЛИТЕРАТУРА

1. Pohl P. Description of MCV, a pseudo-random number generator // Scand. Actuar. J. 1976. V. 1. P. 1–14.
2. Pohl P. MCV — a Fast Pseudo-Random Number Generator with Extremely Good Statistical Properties. PhD Dissertation. University of Stockholm, Stockholm, 1975. 34 p.
3. Lehmer D. H. Mathematical methods in large-scale computing units // Proc. Second Symp. Large-Scale Digital Calculating Machinery, Cambridge (Mass.). Harvard University Press, 1951. P. 141–146.
4. Камловский О. В. Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. № 3(21). С. 11–25.
5. Биляк И. Б., Камловский О. В. Частотные характеристики циклов выходных последовательностей комбинирующих генераторов над полем из двух элементов // Прикладная дискретная математика. 2015. № 3(29). С. 17–31.
6. Камловский О. В. Количество появлений векторов на циклах выходных последовательностей двоичных комбинирующих генераторов // Проблемы передачи информации. 2017. Т. 53. № 1. С. 92–100.
7. Агibalов Г. П. Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. № 2. С. 43–73.

8. *Dai Z. D., Feng X. N., Liu M. L., and Wan Z. X.* Some statistical properties of feedforward sequences (I) // *Science in China (Ser. A)*. 1994. V.37. No.1. P.34–41.
9. *Dai Z. D., Feng X. N., Liu M. L., and Wan Z. X.* Some statistical properties of feedforward sequences (II) // *Science in China (Ser. A)*. 1994. V.37. No.2. P.129–136.
10. *Niederreiter H.* Distribution properties of feedback shift register sequences // *Probl. Control and Inform. Theory*. 1986. V.15. No.1. P.19–34.
11. *Меженная Н. М., Михайлов В. Г.* О числе появлений знаков в мультициклической случайной последовательности по модулю 4 // *Дискретная математика*. 2014. Т.26. №4. С.51–58.
12. *Меженная Н. М., Михайлов В. Г.* О распределении числа единиц в выходной последовательности генератора Пола над полем $GF(2)$ // *Математические вопросы криптографии*. 2013. Т.4. №4. С.95–107.
13. *Тюрин И. С.* Уточнения остаточного члена в теореме Ляпунова // *Теория вероятностей и ее применения*. 2011. Т.56. №3. С.808–811.
14. *Меженная Н. М.* О распределении числа единиц в двоичной мультициклической последовательности // *Прикладная дискретная математика*. 2015. №1(27). С.69–77.
15. *Меженная Н. М., Михайлов В. Г.* Об асимптотической нормальности чисел появлений знаков в неравновероятной мультициклической случайной последовательности по модулю 4 // *Математические вопросы криптографии*. 2016. Т.7. №4. С.81–94.
16. *Биллингсли П.* Сходимость вероятностных мер. М.: Наука, 1977. 352 с.
17. *Janson S.* Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs // *Ann. Probab.* 1988. V.16. No.1. P.305–312.
18. *Физтенгольц Г. М.* Курс дифференциального и интегрального исчисления. 8-е изд. М.: Физматлит, 2003. Т.1. 680 с.
19. *Baldi P. and Rinott Y.* On normal approximations of distributions in terms of dependency graphs // *Ann. Probab.* 1989. V.17. No.4. P.1646–1650.

REFERENCES

1. *Pohl P.* Description of MCV, a pseudo-random number generator. *Scand. Actuar. J.*, 1976, vol.1, pp.1–14.
2. *Pohl P.* MCV — a fast pseudo-random number generator with extremely good statistical properties. PhD Dissertation, University of Stockholm, Stockholm, 1975, 34 p.
3. *Lehmer D. H.* Mathematical methods in large-scale computing units. *Proc. Second Symp. Large-Scale Digital Calculating Machinery*, 1951, Harvard University Press, Cambridge, Mass., pp.141–146.
4. *Kamlovskii O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. *Prikladnaya Diskretnaya Matematika*, 2013, no.3(21), pp.11–25. (in Russian)
5. *Bilyak I. B. and Kamlovskii O. V.* Chastotnyye kharakteristiki tsiklov vykhodnykh posledovatel'nostey kombiniruyushchikh generatorov nad polem iz dvukh elementov [Frequency characteristics of cycles in output sequences generated by combining generators over the field of two elements]. *Prikladnaya Diskretnaya Matematika*, 2015, vol.3, no.3(29), pp.17–31. (in Russian)
6. *Kamlovskii O. V.* Occurrence numbers for vectors in cycles of output sequences of binary combining generators. *Problems Inform. Transmission*, 2017, vol.53, no.1, pp.84–91.
7. *Agibalov G. P.* Konechnyye avtomaty v kriptografii [Finite automata in cryptography]. *Prikladnaya Diskretnaya Matematika. Prilozhenie*, 2009, no.2, pp.43–73. (in Russian)

8. Dai Z. D., Feng X. N., Liu M. L., and Wan Z. X. Some statistical properties of feedforward sequences (I). Science in China (Ser. A), 1994, vol. 37, no. 1, pp. 34–41.
9. Dai Z. D., Feng X. N., Liu M. L., and Wan Z. X. Some statistical properties of feedforward sequences (II). Science in China (Ser. A), 1994, vol. 37, no. 2, pp. 129–136.
10. Niederreiter H. Distribution properties of feedback shift register sequences. Probl. Control and Inform. Theory, 1986, vol. 15, no. 1, pp. 19–34.
11. Mezhenayaya N. M. and Mikhailov V. G. On frequencies of elements in multicyclic random sequence modulo 4. Discrete Math. Appl., 2015, vol. 25, no. 6, pp. 359–365.
12. Mezhenayaya N. M. and Mikhailov V. G. O raspredelenii chisla edinit v vykhodnoy posledovatel'nosti generatora Pola nad polem GF(2) [On the distribution of the number of ones in the output sequence of the MCV-generator over GF(2)]. Matematicheskie Voprosy Kriptografii, 2013, vol. 4, no. 4, pp. 95–107. (in Russian)
13. Tyurin I. S. An improvement of the residual in the Lyapunov theorem. Theory Probab. Appl., 2011, vol. 56, no. 3, pp. 693–696.
14. Mezhenayaya N. M. O raspredelenii chisla edinit v dvoichnoy mul'titsiklicheskoj posledovatel'nosti [On distribution of number of ones in binary multicycle sequence]. Prikladnaya Diskretnaya Matematika, 2015, no. 1(27), pp. 69–77. (in Russian)
15. Mezhenayaya N. M. and Mikhailov V. G. Ob asimptoticheskoy normal'nosti chisel poyavleniy znakov v neravnoveroyatnoy mul'titsiklicheskoj sluchaynoy posledovatel'nosti po modulyu 4 [On the asymptotic normality of frequencies of values in the non-equiprobable multi-cyclic random sequence modulo 4]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 81–94. (in Russian)
16. Billingsley P. Convergence of Probability Measures, 2nd ed. New-York, Wiley, 1999. 296 p.
17. Janson S. Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs. Ann. Probab., 1988, vol. 16, no. 1, pp. 305–312.
18. Fikhtengol'ts G. M. Kurs differentsial'nogo i integral'nogo ischisleniya. 8-e izd. [Differential and Integral Calculus Course. 8th ed.] Moscow, Fizmatlit Publ., 2003, vol. 1. 680 p. (in Russian)
19. Baldi P. and Rinott Y. On normal approximations of distributions in terms of dependency graphs. Ann. Probab., 1989, vol. 17, no. 4, pp. 1646–1650.