Math-Net.Ru

Общероссийский математический портал

Н. М. Меженная, В. Г. Михайлов, О числе появлений знаков в мультициклической случайной последовательности по модулю 4, *Дискрет. матем.*, 2014, том 26, выпуск 4, 51–58

DOI: <https://doi.org/10.4213/dm1304>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.197.130.99

26 апреля 2023 г., 17:00:13

О числе появлений знаков в мультициклической случайной последовательности по модулю 4

© 2014 г. Н. М. Меженная*, В. Г. Михайлов**

Указаны достаточные условия сходимости совместного распределения чисел появлений знаков на цикле мультициклической случайной последовательности по модулю 4 к предельному распределению. Указан вид этого распределения и описаны некоторые его свойства.

Ключевые слова: мультициклическая последовательность, генератор Пола, предельные теоремы.

1. Введение

Пусть $n_1, \dots, n_r \geq 2$ — взаимно простые натуральные числа. Мультициклическая случайная последовательность $\{Z_t\}_{t \geq 0}$ со значениями в $\{0, 1, \dots, M-1\}$ образуется по правилу

$$Z_t = \sum_{i=1}^r X_{t(n_i)}^{(i)} \bmod M, \quad t = 0, 1, \dots, \quad (1)$$

где $(X_0^{(i)}, \dots, X_{n_i-1}^{(i)})$, $i = 1, \dots, r$, — наборы независимых в совокупности случайных величин, распределенных равномерно на множестве неотрицательных вычетов по модулю M , а $t(n_i) = t - [t/n_i]n_i$. Эта последовательность используется в качестве теоретико-вероятностной модели выходной последовательности генератора Пола (см. [1]) при изучении статистических свойств последней. Напомним, что генератор Пола вырабатывает выходную последовательность по правилу (1), в котором в качестве $(X_0^{(i)}, \dots, X_{n_i-1}^{(i)})$, $i = 1, \dots, r$, используются заданные наборы чисел, называемые заполнениями регистров.

Нас интересует случай $M = 4$. Отрезок $Z = (Z_0, Z_1, \dots, Z_{n_1 \dots n_r - 1})$ будем называть *циклом* мультициклической последовательности $\{Z_t\}$. Целью работы является изучение асимптотического поведения при $n_1, \dots, n_r \rightarrow \infty$ совместного распределения случайных величин $\kappa_{a_2 a_1}$ — количеств чисел в Z , имеющих двоичную запись $a_2 a_1$, $a_1, a_2 \in \{0, 1\}$. Аналогичные задачи для случая $M = 2$ рассматривались в работах [2] и [3].

*Место работы: МГТУ им. Н. Э. Баумана, e-mail: natalia.mezhennaya@gmail.com

**Место работы: Математический институт им. В.А. Стеклова РАН,
e-mail: mikhail@mi.ras.ru

2. Основные определения и результаты

Положим

$$\tilde{K} = \left(\frac{4\kappa_{00} - n_1 \dots n_r}{\sqrt{n_1 \dots n_r}}, \frac{4\kappa_{01} - n_1 \dots n_r}{\sqrt{n_1 \dots n_r}}, \frac{4\kappa_{10} - n_1 \dots n_r}{\sqrt{n_1 \dots n_r}}, \frac{4\kappa_{11} - n_1 \dots n_r}{\sqrt{n_1 \dots n_r}} \right).$$

Пусть случайные величины η_r , ϱ_r и ϕ независимы в совокупности, причем величина η_r распределена как произведение r независимых стандартных нормальных случайных величин, ϱ_r — как произведение r независимых случайных величин, имеющих распределение Рэлея с плотностью $f(x) = xe^{-x^2/2}$, $x \geq 0$, а ϕ имеет равномерное распределение на единичной окружности.

Теорема 1. Пусть $n_1, \dots, n_r \geq 2$ — взаимно простые натуральные числа, наборы $X^{(i)} = (X_0^{(i)}, \dots, X_{n_i-1}^{(i)})$, $i = 1, \dots, r$, образованы независимыми в совокупности случайными величинами, распределенными равномерно на множестве $\{0, \dots, 3\}$, и $n_1, \dots, n_r \rightarrow \infty$. Тогда распределение случайного вектора $\tilde{K}$ сходится к распределению вектора $(\tilde{N}_{00}, \tilde{N}_{01}, \tilde{N}_{10}, \tilde{N}_{11})$, где

$$\begin{aligned} \tilde{N}_{00} &= \eta_r + 2^{1-r/2} \varrho_r \cos \phi, & \tilde{N}_{01} &= -\eta_r + 2^{1-r/2} \varrho_r \sin \phi, \\ \tilde{N}_{10} &= \eta_r - 2^{1-r/2} \varrho_r \cos \phi, & \tilde{N}_{11} &= -\eta_r - 2^{1-r/2} \varrho_r \sin \phi. \end{aligned}$$

Под сходимостью распределений здесь и везде далее понимается слабая сходимость, а под асимптотической независимостью ниже понимается слабая сходимость распределения случайного вектора к распределению вектора из независимых компонент.

Пусть κ_{*0} — количество чисел в Z , имеющих в младшем разряде своей двоичной записи нуль, а κ_{0*} — количество чисел в Z , имеющих нуль в старшем разряде своей двоичной записи. Непосредственно из теоремы 1 вытекает следующее утверждение.

Следствие 1. Пусть выполнены условия теоремы 1. Тогда:

- 1) распределение случайной величины $(2\kappa_{*0} - n_1 \dots n_r)(n_1 \dots n_r)^{-1/2}$ сходится к распределению произведения r независимых стандартных нормальных случайных величин,
- 2) распределение случайной величины $(2\kappa_{0*} - n_1 \dots n_r)(n_1 \dots n_r)^{-1/2}$ сходится к распределению случайной величины $2^{1-r/2} \varrho_r (\cos \phi + \sin \phi)$.

Замечание 1. Утверждение 1) следствия 1 (в иной формулировке) было доказано в работе [3].

Замечание 2. Предельное распределение, указанное в теореме 1, имеет нулевой вектор математических ожиданий и матрицу ковариаций с числами 3 на главной диагонали и числами -1 в остальных позициях. Таким образом, указанные характеристики распределения частот исходов в полном цикле мультициклической последовательности по модулю 4 совпадают с аналогичными характеристиками для последовательности независимых равновероятных полиномиальных испытаний с четырьмя исходами.

Приведем основные идеи, на которых базируется доказательство теоремы 1. Введем обозначение $\nu_{a_2 a_1}^{(i)}$ для количества чисел в $X^{(i)} = (X_0^{(i)}, \dots, X_{n_i-1}^{(i)})$, имеющих в двоичной системе счисления запись $a_2 a_1$, и обозначение $\nu_{a_1}^{(i)}$ для количества чисел в $X^{(i)}$, двоичная запись которых заканчивается числом a_1 . Введем величины

$$\delta^{(i)} = \nu_0^{(i)} - \nu_1^{(i)}, \quad \delta_a^{(i)} = \nu_{0a}^{(i)} - \nu_{1a}^{(i)}, \quad a \in \{0, 1\}, i = 1, \dots, r. \quad (2)$$

Тогда

$$\nu_{a_2 a_1}^{(i)} = \frac{1}{4} \left(n_i + (-1)^{a_1} \delta^{(i)} + 2(-1)^{a_2} \delta_{a_1}^{(i)} \right), \quad a_1, a_2 \in \{0, 1\}, \quad i = 1, \dots, r. \quad (3)$$

Лемма 1. При $r = 2$

$$\kappa_{a_2 a_1} = \frac{1}{4} \left(n_1 n_2 + (-1)^{a_1} \beta + 2(-1)^{a_2} \beta_{a_1} \right), \quad a_1, a_2 \in \{0, 1\}, \quad (4)$$

где $\beta = \delta^{(1)} \delta^{(2)}$, а величины β_a определяются равенством

$$\begin{pmatrix} \beta_0 & -\beta_1 \\ \beta_1 & \beta_0 \end{pmatrix} = \begin{pmatrix} \delta_0^{(1)} & -\delta_1^{(1)} \\ \delta_1^{(1)} & \delta_0^{(1)} \end{pmatrix} \begin{pmatrix} \delta_0^{(2)} & -\delta_1^{(2)} \\ \delta_1^{(2)} & \delta_0^{(2)} \end{pmatrix}.$$

Доказательство леммы 1 проводится непосредственным вычислением, поэтому оно здесь не приводится.

Полезно заметить, что

$$\beta = \kappa_0 - \kappa_1, \quad \beta_a = \kappa_{0a} - \kappa_{1a}, \quad a \in \{0, 1\}. \quad (5)$$

Замечание 3. Распределение любой случайной величины η со значениями в конечной абелевой группе G можно записать в виде

$$\mathbf{P}\{\eta = h\} = \frac{1}{|G|} \sum_{g \in G} \Delta_g \chi_g(h), \quad h \in G,$$

где

$$\Delta_g = \sum_{h \in G} \mathbf{P}\{\eta = h\} \bar{\chi}_g(h),$$

в частности, $\Delta_0 = 1$. Здесь $\chi_g(h)$, $g \in G$, — характеры группы G , а $\bar{z}$ — комплексное число, сопряженное с z . Пусть случайные величины η' и η'' независимы, $\eta = \eta' + \eta''$, а Δ_g , Δ'_g , Δ''_g соответствуют η , η' , η'' . Тогда при всех $g \in G$ выполнено равенство $\Delta_g = \Delta'_g \Delta''_g$ (см. [4]). Величины $\delta^{(i)}$, $\delta_0^{(i)}$ и $\delta_1^{(i)}$ в (3) с точностью до числового множителя представляют собой преобладания Δ_g , $g \neq 0$, соответствующие распределению на группе вычетов по модулю 4 с вероятностями $\left(\frac{\nu_{0,0}^{(i)}}{n_i}, \frac{\nu_{0,1}^{(i)}}{n_i}, \frac{\nu_{1,0}^{(i)}}{n_i}, \frac{\nu_{1,1}^{(i)}}{n_i} \right)$, а утверждение леммы 1 выражает указанное свойство этих преобладаний.

Для обобщения леммы 1 на случай произвольного $r \geq 2$ воспользуемся интерпретацией мультициклической последовательности как выходной последовательности генератора Пола. Генератор Пола с r регистрами можно рассматривать как генератор с двумя регистрами, заполнение первого из которых представляет собой всю выходную последовательность генератора Пола с первыми $r - 1$ регистрами исходного генератора, а заполнение второго — заполнение последнего r -го регистра исходного генератора. Потому утверждение леммы 1 обобщается следующим образом.

Лемма 2. Пусть $r \geq 2$. Тогда выполнена формула

$$\kappa_{a_2 a_1} = \frac{1}{4} \left(n_1 \dots n_r + (-1)^{a_1} \beta + 2(-1)^{a_2} \beta_{a_1} \right),$$

где

$$\beta = \delta^{(1, \dots, r)} = \delta^{(1)} \cdot \dots \cdot \delta^{(r)}, \quad (6)$$

$\beta_{a_1} = \delta_{a_1}^{(1, \dots, r)}$, а величины $\delta_0^{(1, \dots, r)}$, $\delta_0^{(1, \dots, r)}$ вычисляются по рекуррентным формулам

$$\begin{pmatrix} \delta_0^{(1, \dots, k)} & -\delta_1^{(1, \dots, k)} \\ \delta_1^{(1, \dots, k)} & \delta_0^{(1, \dots, k)} \end{pmatrix} = \begin{pmatrix} \delta_0^{(1, \dots, k-1)} & -\delta_1^{(1, \dots, k-1)} \\ \delta_1^{(1, \dots, k-1)} & \delta_0^{(1, \dots, k-1)} \end{pmatrix} \begin{pmatrix} \delta_0^{(k)} & -\delta_1^{(k)} \\ \delta_1^{(k)} & \delta_0^{(k)} \end{pmatrix}, \quad (7)$$

$k = 2, \dots, r$.

Используя лемму 2, мы изучим свойства распределения случайных величин $\kappa_{a_2 a_1}$, сведя его к изучению свойств совместного распределения случайных величин $\delta^{(1, \dots, r)}$, $\delta_0^{(1, \dots, r)}$, $\delta_1^{(1, \dots, r)}$. Положим

$$\xi_r = \frac{\delta^{(1, \dots, r)}}{\sqrt{n_1 \dots n_r}}, \quad \xi_{r,0} = \sqrt{\frac{2^r}{n_1 \dots n_r}} \cdot \delta_0^{(1, \dots, r)}, \quad \xi_{r,1} = \sqrt{\frac{2^r}{n_1 \dots n_r}} \cdot \delta_1^{(1, \dots, r)}.$$

Теорема 2. Пусть выполнены условия теоремы 1. Тогда случайная величина ξ_r и случайный вектор $(\xi_{r,0}, \xi_{r,1})$ асимптотически независимы и:

- 1) распределение величины ξ_r сходится к распределению случайной величины η_r ,
- 2) распределение вектора $(\xi_{r,0}, \xi_{r,1})$ сходится к распределению вектора $(\varrho_r \cos \phi, \varrho_r \sin \phi)$.

Нетрудно проверить, что из теоремы 2 и леммы 2 вытекает утверждение теоремы 1.

3. Доказательства

Сначала рассмотрим отдельно i -й регистр. Для простоты записи индекс i в обозначениях величин будем пока опускать. В данных обозначениях $X^{(i)} = (X_1, \dots, X_n)$, $\nu_{a_2 a_1} = \nu_{a_2 a_1}(n)$ — количество чисел в $X_1, \dots, X_n$, имеющих двоичную запись $a_2 a_1$, и $\nu_{a_1} = \nu_{a_1}(n)$ — количество тех элементов последовательности $X_1, \dots, X_n$, двоичная запись которых заканчивается числом a_1 .

Рассмотрим вектор $\nu(n) = (\nu_{00}(n) - \nu_{10}(n), \nu_{01}(n) - \nu_{11}(n), \nu_0(n))$.

Лемма 3. Пусть $0 \leq k \leq n$, $0 \leq l_0 \leq k$, $0 \leq l_1 \leq n - k$. Тогда при целых $(l_0 + k)/2$ и $(l_1 + n - k)/2$

$$\begin{aligned} \mathbf{P}\{\nu_{00}(n) - \nu_{10}(n) = l_0, \nu_{01}(n) - \nu_{11}(n) = l_1, \nu_0(n) = k\} = \\ = \frac{1}{2^{2n}} C_n^k C_k^{(l_0+k)/2} C_{n-k}^{(l_1+n-k)/2}. \end{aligned} \quad (8)$$

В остальных случаях эта вероятность равна нулю.

Замечание 4. Утверждение леммы не связано с понятием мультициклической последовательности. Под $X_1, \dots, X_n$ можно понимать последовательность независимых в совокупности случайных величин, распределенных равномерно на множестве вычетов по модулю 4.

Доказательство леммы 3. Из независимости в совокупности отдельных разрядов всех чисел $X_1, \dots, X_n$ следует, что

$$\mathbf{P}\{\nu_{00}(n) - \nu_{10}(n) = l_0 | \nu_0(n) = k\} = \mathbf{P}\{\nu_0(k) - \nu_1(k) = l_0\},$$

$$\mathbf{P}\{\nu_{01}(n) - \nu_{11}(n) = l_1 | \nu_1(n) = n - k\} = \mathbf{P}\{\nu_0(n - k) - \nu_1(n - k) = l_1\}.$$

Разумеется, $\{\nu_1(n) = n - k\} = \{\nu_0(n) = k\}$, и при выполнении любого из этих равенств события $\{\nu_{00}(n) - \nu_{10}(n) = l_0\}$ и $\{\nu_{01}(n) - \nu_{11}(n) = l_1\}$ независимы. Кроме того,

$$\begin{aligned} \mathbf{P}\{\nu_1(n) = n - k\} &= \mathbf{P}\{\nu_0(n) = k\} = \frac{1}{2^n} C_n^k, \\ \mathbf{P}\{\nu_0(k) - \nu_1(k) = l\} &= \mathbf{P}\{2\nu_0(k) - k = l\} = \\ &= \mathbf{P}\{2\nu_0(k) = l + k\} = \frac{1}{2^k} C_k^{(l+k)/2} \end{aligned}$$

при всех l , для которых число $(l + k)/2$ целое. В остальных случаях эта вероятность равна нулю.

Поэтому

$$\begin{aligned} &\mathbf{P}\{\nu_{00}(n) - \nu_{10}(n) = l_0, \nu_{01}(n) - \nu_{11}(n) = l_1, \nu_0(n) = k\} = \\ &= \frac{1}{2^n} C_n^k \mathbf{P}\{\nu_{00}(n) - \nu_{10}(n) = l_0 | \nu_0(n) = k\} \mathbf{P}\{\nu_{01}(n) - \nu_{11}(n) = l_1 | \nu_1(n) = n - k\} = \\ &= \frac{1}{2^n} C_n^k \mathbf{P}\{\nu_0(k) - \nu_1(k) = l_0\} \mathbf{P}\{\nu_0(n - k) - \nu_1(n - k) = l_1\}, \end{aligned}$$

и при целых $(l_0 + k)/2$ и $(l_1 + n - k)/2$ получаем (8). Второе утверждение леммы очевидно. Лемма 3 доказана.

Лемма 4. *Характеристическая функция вектора $\nu(n)$ имеет вид*

$$g(t_1, t_2, t_3) = \frac{1}{2^{2n}} \left(\frac{1 + e^{2it_2}}{e^{it_2}} \right)^n \left(e^{it_3} \frac{1 + e^{2it_1}}{e^{it_1}} \frac{e^{it_2}}{1 + e^{2it_2}} + 1 \right)^n. \quad (9)$$

Доказательство леммы 4. Пользуясь определением характеристической функции и леммой 3, получаем

$$\begin{aligned} g(t_1, t_2, t_3) &= \mathbf{E} e^{it_1(\nu_{00}(n) - \nu_{10}(n))} e^{it_2(\nu_{01}(n) - \nu_{11}(n))} e^{it_3\nu_0(n)} = \\ &= \frac{1}{2^{2n}} \sum_{k=0}^n \sum_{l_0=-k}^k \sum_{l_1=-(n-k)}^{n-k} C_n^k C_k^{(l_0+k)/2} C_{n-k}^{(l_1+n-k)/2} e^{it_1 l_0} e^{it_2 l_1} e^{it_3 k} = \\ &= \frac{1}{2^{2n}} \sum_{k=0}^n C_n^k e^{it_3 k} \sum_{l_0=-k}^k C_k^{(l_0+k)/2} e^{it_1 l_0} \sum_{l_1=-(n-k)}^{n-k} C_{n-k}^{(l_1+n-k)/2} e^{it_2 l_1} \quad (10) \end{aligned}$$

(здесь считается, что величины C_k^m с дробным показателем m равны нулю). Произведя во внутренних суммах выражения в правой части (10) замены $m = \frac{l_0+k}{2}$ и $m = \frac{l_1+n-k}{2}$ соответственно, получим

$$\begin{aligned} \sum_{l_0=-k}^k C_k^{(l_0+k)/2} x^{l_0} &= \sum_{m=0}^k C_k^m x^{2m-k} = x^{-k} (1 + x^2)^k = \left(\frac{1 + x^2}{x} \right)^k, \\ \sum_{l_1=-(n-k)}^{n-k} C_{n-k}^{(l_1+n-k)/2} y^{l_1} &= \sum_{m=0}^{n-k} C_{n-k}^m y^{2m-n+k} = y^{-n+k} (1 + y^2)^{n-k} = \left(\frac{1 + y^2}{y} \right)^{n-k}. \end{aligned}$$

Поэтому из (10) при $x = e^{it_1}$, $y = e^{it_2}$ следует, что

$$g(t_1, t_2, t_3) = \frac{1}{2^{2n}} \sum_{k=0}^n C_n^k e^{it_3 k} \left(\frac{1 + e^{2it_1}}{e^{it_1}} \right)^k \left(\frac{1 + e^{2it_2}}{e^{it_2}} \right)^{n-k} =$$

$$= \frac{1}{2^{2n}} \left(e^{it_3} \frac{1 + e^{2it_1}}{e^{it_1}} + \frac{1 + e^{2it_2}}{e^{it_2}} \right)^n = \frac{1}{2^{2n}} \left(\frac{1 + e^{2it_2}}{e^{it_2}} \right)^n \left(e^{it_3} \frac{1 + e^{2it_1}}{e^{it_1}} \frac{e^{it_2}}{1 + e^{2it_2}} + 1 \right)^n.$$

Лемма 4 доказана.

Пользуясь леммой 4, найдем вектор математических ожиданий $\mathbf{E}\nu(n)$ и ковариационную матрицу Σ вектора $\nu(n)$ (для этого вычисляем первые и вторые производные функции (9) в точке $(0,0,0)$). Имеем

$$\mathbf{E}\nu(n) = \left(0, 0, \frac{n}{2} \right), \quad \Sigma = \begin{pmatrix} \frac{n}{2} & 0 & 0 \\ 0 & \frac{n}{2} & 0 \\ 0 & 0 & \frac{n}{4} \end{pmatrix}.$$

Рассмотрим теперь вектор

$$\tilde{\nu}(n) = \left(\frac{\nu_{00}(n) - \nu_{10}(n)}{\sqrt{n/2}}, \frac{\nu_{01}(n) - \nu_{11}(n)}{\sqrt{n/2}}, \frac{\nu_0(n) - n/2}{\sqrt{n/4}} \right).$$

Лемма 5. При $n \rightarrow \infty$ распределение случайного вектора $\tilde{\nu}(n)$ сходится к трехмерному нормальному закону с нулевым вектором средних и единичной ковариационной матрицей.

Из леммы 5 непосредственно вытекает следующее утверждение.

Следствие 2. Пусть $n \rightarrow \infty$. Тогда случайная величина $\frac{\nu_0(n) - n/2}{\sqrt{n/4}}$ и случайный вектор $\left(\frac{\nu_{00}(n) - \nu_{10}(n)}{\sqrt{n/2}}, \frac{\nu_{01}(n) - \nu_{11}(n)}{\sqrt{n/2}} \right)$ асимптотически независимы и:

1) распределение случайной величины $\frac{\nu_0(n) - n/2}{\sqrt{n/4}}$ сходится к стандартному нормальному распределению,

2) распределение случайного вектора $\left(\frac{\nu_{00}(n) - \nu_{10}(n)}{\sqrt{n/2}}, \frac{\nu_{01}(n) - \nu_{11}(n)}{\sqrt{n/2}} \right)$ сходится к распределению случайного вектора $(R \cos \phi, R \sin \phi)$, в котором случайные величины R и ϕ независимы, причем величина R имеет распределение Рэлея с плотностью $f(x) = xe^{-x^2/2}, x \geq 0$, а величина ϕ — равномерное распределение на единичной окружности.

Доказательство леммы 5. Используя лемму 4, запишем характеристическую функцию $h(t_1, t_2, t_3)$ вектора $\tilde{\nu}(n)$ в явном виде:

$$\begin{aligned} h(t_1, t_2, t_3) &= e^{-it_3\sqrt{n}} g(e^{it_1\sqrt{2/n}}, e^{it_2\sqrt{2/n}}, e^{2it_3/\sqrt{n}}) = \\ &= e^{-\sqrt{n}it_3} \left(\frac{e^{-it_2\sqrt{2/n}} + e^{it_2\sqrt{2/n}}}{2} \right)^n \tilde{h}(t_1, t_2, t_3)^n, \end{aligned} \quad (11)$$

$$\tilde{h}(t_1, t_2, t_3) = \left(1 + \frac{1}{2} \left(\frac{(e^{-it_1\sqrt{2/n}} + e^{it_1\sqrt{2/n}}) e^{it_2\sqrt{2/n}} e^{2it_3\sqrt{1/n}}}{1 + e^{2it_2\sqrt{2/n}}} - 1 \right) \right).$$

С помощью соотношений

$$\begin{aligned} e^u &= 1 + u + u^2/2 + O(u^3), \quad (e^{-u} + e^u)/2 = 1 + u^2/2 + O(u^4), \\ (1 + e^u)^{-1} &= 1 - u/4 + O(u^3) \end{aligned} \quad (12)$$

при $u \rightarrow 0$, получаем

$$\begin{aligned}
 \ln \left(\frac{e^{-it_2\sqrt{2/n}} + e^{it_2\sqrt{2/n}}}{2} \right)^n &= -t_2^2 + O(n^{-1}), \\
 \frac{\left(e^{-it_1\sqrt{2/n}} + e^{it_1\sqrt{2/n}} \right) e^{it_2\sqrt{2/n}} e^{2it_3\sqrt{1/n}}}{1 + e^{2it_2\sqrt{2/n}}} &= \\
 &= \left(1 - \frac{t_1^2}{n} + O(n^{-3/2}) \right) \left(1 + it_2\sqrt{\frac{2}{n}} - \frac{t_2^2}{n} + O(n^{-3/2}) \right) \times \\
 &\times \left(1 + 2it_3\sqrt{\frac{1}{n}} - \frac{2t_3^2}{n} + O(n^{-3/2}) \right) \left(1 - \frac{it_2\sqrt{2}}{\sqrt{n}} + O(n^{-3/2}) \right) = \\
 &= \left(1 - \frac{t_1^2}{n} \right) \left(1 + \frac{t_2^2}{n} \right) \left(1 + 2it_3\sqrt{\frac{1}{n}} - \frac{2t_3^2}{n} \right) + O(n^{-3/2}) = \\
 &= 1 - \frac{t_1^2}{n} + \frac{t_2^2}{n} + 2it_3\sqrt{\frac{1}{n}} - \frac{2t_3^2}{n} + O(n^{-3/2}),
 \end{aligned} \tag{13}$$

а значит,

$$\begin{aligned}
 \ln \tilde{h}(t_1, t_2, t_3) &= \frac{1}{2} \left(-\frac{t_1^2}{n} + \frac{t_2^2}{n} + 2it_3\sqrt{\frac{1}{n}} - \frac{2t_3^2}{n} \right) - \\
 &- \frac{1}{8} \left(-\frac{t_1^2}{n} + \frac{t_2^2}{n} + 2it_3\sqrt{\frac{1}{n}} - \frac{2t_3^2}{n} \right)^2 + O(n^{-3/2}) = \\
 &= -\frac{t_1^2}{2n} + \frac{t_2^2}{2n} + it_3\sqrt{\frac{1}{n}} - \frac{t_3^2}{n} - \frac{1}{8} \left(2it_3\sqrt{\frac{1}{n}} \right)^2 + O(n^{-3/2}) = \\
 &= -\frac{t_1^2}{2n} + \frac{t_2^2}{2n} + it_3\sqrt{\frac{1}{n}} - \frac{t_3^2}{2n} + O(n^{-3/2}).
 \end{aligned} \tag{14}$$

Логарифмируя формулу (11) и подставляя в слагаемые правой части полученной формулы разложения (12), (13) и (14), получаем

$$\begin{aligned}
 \ln h(t_1, t_2, t_3) &= -\sqrt{n}it_3 - n\frac{t_2^2}{n} + n \left(-\frac{t_1^2}{2n} + \frac{t_2^2}{2n} + it_3\sqrt{\frac{1}{n}} - \frac{t_3^2}{2n} \right) + O(n^{-1/2}) = \\
 &= -\frac{t_1^2}{2} - \frac{t_2^2}{2} - \frac{t_3^2}{2} + O\left(\frac{1}{\sqrt{n}}\right).
 \end{aligned}$$

Осталось воспользоваться теоремой о непрерывности для характеристических функций многомерных распределений (см., например, [5], гл. XY). Лемма 5 доказана.

Доказательство теоремы 2. Утверждение 1) теоремы вытекает из соотношений (2) и (6):

$$\xi_r = \frac{\delta^{(1)} \dots \delta^{(r)}}{\sqrt{n_1 \dots n_r}} = \prod_{i=1}^r \frac{\nu_0^{(i)} - \nu_1^{(i)}}{\sqrt{n_i}} = \prod_{i=1}^r \frac{\nu_0^{(i)} - n_i/2}{\sqrt{n_i/4}}. \tag{15}$$

Докажем утверждение 2). Из (5) и (7) следует, что

$$\left(\sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_0^{(1, \dots, r)} \quad -\sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_1^{(1, \dots, r)} \right) = \left(\sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_1^{(1, \dots, r)} \quad \sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_0^{(1, \dots, r)} \right)$$

$$= \prod_{i=1}^r \begin{pmatrix} \frac{\delta_0^{(i)}}{\sqrt{n_i/2}} & -\frac{\delta_1^{(i)}}{\sqrt{n_i/2}} \\ \frac{\delta_1^{(i)}}{\sqrt{n_i/2}} & \frac{\delta_0^{(i)}}{\sqrt{n_i/2}} \end{pmatrix} = \prod_{i=1}^r \begin{pmatrix} \frac{\nu_{00}^{(i)} - \nu_{10}^{(i)}}{\sqrt{n_i/2}} & -\frac{\nu_{01}^{(i)} - \nu_{11}^{(i)}}{\sqrt{n_i/2}} \\ \frac{\nu_{01}^{(i)} - \nu_{11}^{(i)}}{\sqrt{n_i/2}} & \frac{\nu_{00}^{(i)} - \nu_{10}^{(i)}}{\sqrt{n_i/2}} \end{pmatrix}. \quad (16)$$

Случайные матрицы, входящие в произведение матриц в правой части (16), независимы в совокупности, и согласно лемме 5 сходятся по распределению к случайным матрицам

$$\begin{pmatrix} R_i \cos \phi^{(i)} & -R_i \sin \phi^{(i)} \\ R_i \sin \phi^{(i)} & R_i \cos \phi^{(i)} \end{pmatrix}, \quad i = 1, \dots, r,$$

где случайные величины $R_1, \dots, R_r, \phi^{(1)}, \dots, \phi^{(r)}$ независимы в совокупности, первые r из них имеют распределение Рэлея, указанное в формулировке теоремы, а последние r распределены равномерно на единичной окружности. Поэтому случайная матрица

$$\begin{pmatrix} \sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_0^{(1, \dots, r)} & -\sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_1^{(1, \dots, r)} \\ \sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_1^{(1, \dots, r)} & \sqrt{\frac{2r}{n_1 \dots n_r}} \cdot \delta_0^{(1, \dots, r)} \end{pmatrix}$$

сходится по распределению к случайной матрице

$$\begin{aligned} \prod_{i=1}^r \begin{pmatrix} R_i \cos \phi_i & -R_i \sin \phi_i \\ R_i \sin \phi_i & R_i \cos \phi_i \end{pmatrix} &= \begin{pmatrix} R_1 \dots R_r \cos \phi & -R_1 \dots R_r \sin \phi \\ R_1 \dots R_r \sin \phi & R_1 \dots R_r \cos \phi \end{pmatrix} = \\ &= \begin{pmatrix} \varrho_r \cos \phi & -\varrho_r \sin \phi \\ \varrho_r \sin \phi & \varrho_r \cos \phi \end{pmatrix}, \end{aligned} \quad (17)$$

где величина $\phi = \phi_1 + \dots + \phi_r$ также распределена равномерно на единичной окружности и не зависит от величины ϱ_r . Утверждение 2) доказано.

Асимптотическая независимость величины ξ_r и вектора $(\xi_{r,0}, \xi_{r,1})$ вытекает из асимптотической независимости величин $\frac{\nu_0^{(i)} - n_1/2}{\sqrt{n_i/4}}$ и векторов $\left(\frac{\nu_{00}^{(i)} - \nu_{10}^{(i)}}{\sqrt{n/2}}, \frac{\nu_{01}^{(i)} - \nu_{11}^{(i)}}{\sqrt{n/2}} \right)$ при каждом $i = 1, \dots, r$ (она доказана в лемме 5) и независимости случайных векторов $X^{(i)} = (X_0^{(i)}, \dots, X_{n_i-1}^{(i)})$. Теорема 2 доказана.

Научные исследования Меженной Н.М. поддержаны грантом РФФИ 14-01-00318а.

Список литературы

1. Pohl P., "Description of MCV, a pseudo-random number generator", *Scand. Actuarial J*, **1** (1976), 1–14.
2. Меженная Н. М., Михайлов В. Г., "О распределении числа единиц в выходной последовательности генератора Пола над полем $\text{GF}(2)$ ", *Матем. вopr. криптогр.*, **4:4** (2013), 95–107.
3. Mezhenneya N. M., "Convergence rate estimators for the number of ones in outcome sequence of MCV generator with m -dependent registers items", *Сиб. электрон. матем. изв.*, **11** (2014), 18–25.
4. Севастьянов Б. А., "Условное распределение выхода автоматов без памяти при заданных характеристиках входа", *Дискретная математика*, **6:1** (1994), 34–39.
5. Феллер В., *Введение в теорию вероятностей и ее приложения*, т. 2, Мир, Москва, 1984, 738 с.