

УДК 519.214.5

**О РАСПРЕДЕЛЕНИИ ЧИСЛА ЕДИНИЦ В ДВОИЧНОЙ  
МУЛЬТИЦИКЛИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ<sup>1</sup>**

Н. М. Меженная

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

Работа посвящена исследованию устойчивости теоретико-вероятностной модели, описывающей генератор Пола. Для этого изучено распределение случайной величины, равной числу единиц в выходной последовательности мультициклического генератора над полем  $GF(2)$  в случае, когда двоичные случайные величины, заполняющие регистры, независимы, а вероятности появления единиц в регистрах отличны от  $1/2$  и могут меняться с ростом длин регистров. Получены точные выражения математического ожидания и дисперсии для этой случайной величины. В случае когда число регистров фиксировано, получены условия, при которых распределение нормированного числа единиц сходится к распределению произведения независимых случайных величин, каждая из которых распределена по стандартному нормальному закону. Доказана нормальная предельная теорема для нормированного числа единиц в случае, когда число регистров стремится к бесконечности. Результаты показывают, что нарушение свойства равновероятности распределения знаков в регистрах приводит к существенным изменениям свойств указанных предельных распределений по сравнению с равновероятным случаем.

**Ключевые слова:** мультициклическая последовательность, генератор Пола, центральная предельная теорема.

DOI 10.17223/20710410/27/7

**ON DISTRIBUTION OF NUMBER OF ONES IN BINARY  
MULTICYCLE SEQUENCE**

N. M. Mezhennaya

*Bauman Moscow State Technical University, Moscow, Russia***E-mail:** natalia.mezhennaya@gmail.com

The work is devoted to studying the stability of probability-theoretical model which describes Pohl generator. For the purpose, we investigate the distribution of random variable equalled to the number of ones in the outcome sequence of a multicycle generator over the field  $GF(2)$  in the case when binary random variables filling the registers are independent and the probabilities of one's occurrences in registers differ from  $1/2$  and can change with growing the registers lengths. The exact expressions for expectation and variance of the random variable are given. For the case when the number of registers is finite, we derive the conditions under which the distribution of normalized number of ones converges to the distribution of the product of independent

<sup>1</sup>Работа выполнена при финансовой поддержке Министерства образования и науки РФ (тема № 1.2640.2014).

random variables each of which is distributed by standard normal law. We prove the central limit theorem for normalized number of ones when the number of registers tends to infinity. It is shown that breaking the property of equiprobable distribution for binary characters in registers results in significant differences of properties of the limit distributions compared to equiprobable case.

**Keywords:** *multicycle sequence, Pohl generator, central limit theorem.*

### Введение

Пусть  $X^{(i)} = (X_0^{(i)}, \dots, X_{n_i-1}^{(i)})$ ,  $i = 1, \dots, r$ ;

$$\mathbf{P}\{X_j^{(i)} = 1\} = 1 - \mathbf{P}\{X_j^{(i)} = 0\} = p_i, \quad j = 0, \dots, n_i - 1, \quad (1)$$

случайные величины, образующие наборы  $X^{(1)}, \dots, X^{(r)}$ , независимы в совокупности. При этом знаки  $X_j^{(i)}$ ,  $j = 0, \dots, n_i - 1$ , представляют собой заполнения  $i$ -го регистра  $X^{(i)}$ ,  $i = 1, \dots, r$ . Обычно считается, что числа  $n_1, \dots, n_r$  попарно взаимно просты.

Пусть последовательность  $Z_t$ ,  $t = 0, \dots, n_1 \dots n_r - 1$ , образована по правилу

$$Z_t = \bigoplus_{i=1}^r X_{t(n_i)}^{(i)}, \quad (2)$$

где  $t(n) = t \bmod n$ . Последовательность  $Z_t$ , построенную по формуле (2), принято называть мультициклической [1, 2].

Если случайные величины, представляющие заполнения регистров, независимы в совокупности и распределены равномерно, то последовательность представляет собой естественную теоретико-вероятностную модель выходной последовательности мультициклического генератора с  $r$  регистрами (генератора Пола).

Свойства мультициклической последовательности  $Z_t$  при равномерном распределении знаков в наборах  $X^{(1)}, \dots, X^{(r)}$  изучены в работах [2–5]. В [2] отмечено, что если выходная последовательность  $Z_t$  имеет длину порядка  $\sqrt{n_1 \dots n_r}$  и менее, то она обладает свойствами, аналогичными свойствам последовательности из независимых равномерно распределённых двоичных случайных величин. Это позволяет использовать генератор Пола в качестве генератора псевдослучайных чисел с большой длиной цикла (примеры других генераторов с большой длиной цикла можно найти в [6, 7]).

В работах [3–5] изучен случай, когда длина выходной последовательности равна длине полного цикла  $n_1 \dots n_r$ . В [3] в предположении, что регистры заполнены равномерно вероятными независимыми случайными величинами, получены оценки точности аппроксимации распределения числа единиц в мультициклической случайной последовательности логнормальным распределением и распределением произведения  $r$  независимых нормальных случайных величин.

Интересным представляется вопрос, как изменится предельное распределение числа единиц в выходной последовательности при нарушении условий модели, связанных с независимостью случайных величин, представляющих заполнения регистров. В [5] показано, что замена условия независимости знаков, образующих заполнения регистров, на условие их конечной зависимости не меняет вид предельных распределений.

В настоящей работе проведено исследование устойчивости данной модели для случая, когда двоичные знаки, образующие наборы  $X^{(1)}, \dots, X^{(r)}$ , независимы, а их вероятности могут меняться с ростом длин регистров. Оказывается, что в этом случае предельные распределения числа единиц в выходной последовательности могут существенно отличаться от предельных распределений, приведённых в работах [3, 5].

## 1. Основные результаты

Обозначим

$$S_i = \sum_{j=0}^{n_i-1} X_j^{(i)}, i = 1, \dots, r, \quad \xi_r = \sum_{j=0}^{n_1 \dots n_r - 1} Z_j.$$

Известно [3], что

$$n_1 \dots n_r - 2\xi_r = (n_1 - 2S_1) \dots (n_r - 2S_r). \quad (3)$$

**Теорема 1.** Пусть случайные величины в наборах  $X^{(1)}, \dots, X^{(r)}$  независимы в совокупности и имеют распределения (1). Тогда

$$\mathbf{E}\xi_r = \frac{1}{2}n_1 \dots n_r \left(1 - \prod_{i=1}^r (1 - 2p_i)\right); \quad (4)$$

$$\mathbf{D}\xi_r = \frac{1}{4} \left( \prod_{i=1}^r (n_i^2(1 - 2p_i)^2 + 4n_i p_i(1 - p_i)) - \left( n_1 \dots n_r \prod_{i=1}^r (1 - 2p_i) \right)^2 \right). \quad (5)$$

**Доказательство.** Вычислим математическое ожидание случайной величины  $\xi_r$ . Из (3) следует, что

$$\begin{aligned} \mathbf{E}\xi_r &= \frac{1}{2} (n_1 \dots n_r - \mathbf{E}(n_1 - 2S_1) \dots (n_r - 2S_r)) = \\ &= \frac{1}{2} (n_1 \dots n_r - (n_1 - 2\mathbf{E}S_1) \dots (n_r - 2\mathbf{E}S_r)) = \\ &= \frac{1}{2} (n_1 \dots n_r - (n_1 - 2n_1 p_1) \dots (n_r - 2n_r p_r)) = \frac{1}{2} n_1 \dots n_r \left(1 - \prod_{i=1}^r (1 - 2p_i)\right). \end{aligned}$$

Теперь вычислим дисперсию. Из (3) получим

$$\begin{aligned} \mathbf{D}\xi_r &= \frac{1}{4} \mathbf{D}((n_1 - 2S_1) \dots (n_r - 2S_r)) = \\ &= \frac{1}{4} (\mathbf{E}((n_1 - 2S_1)^2 \dots (n_r - 2S_r)^2) - (\mathbf{E}(n_1 - 2S_1) \dots (n_r - 2S_r))^2) = \\ &= \frac{1}{4} (\mathbf{E}(n_1 - 2S_1)^2 \dots \mathbf{E}(n_r - 2S_r)^2 - ((n_1 - 2n_1 p_1) \dots (n_r - 2n_r p_r))^2). \end{aligned}$$

Так как

$$\begin{aligned} \mathbf{E}(n_i - 2S_i)^2 &= \mathbf{E}(n_i - 2n_i p_i + 2n_i p_i - 2S_i)^2 = (n_i - 2n_i p_i)^2 + 4\mathbf{E}(n_i p_i - S_i)^2 = \\ &= n_i^2(1 - 2p_i)^2 + 4\mathbf{D}S_i = n_i^2(1 - 2p_i)^2 + 4n_i p_i(1 - p_i), \end{aligned}$$

то

$$\mathbf{D}\xi_r = \frac{1}{4} \left( \prod_{i=1}^r (n_i^2(1 - 2p_i)^2 + 4n_i p_i(1 - p_i)) - \left( n_1 \dots n_r \prod_{i=1}^r (1 - 2p_i) \right)^2 \right).$$

Теорема доказана. ■

**Замечание 1.** При  $p_1 = \dots = p_r = 1/2$  формулы (4) и (5) совпадают с формулами (4) работы [3].

Пусть  $S_i^* = \frac{S_i - n_i p_i}{\sqrt{n_i p_i(1 - p_i)}}$ ,  $i = 1, \dots, r$ . Тогда

$$n_i - 2S_i = n_i(1 - 2p_i) - 2\sqrt{n_i p_i(1 - p_i)} S_i^* = 2\sqrt{n_i p_i(1 - p_i)} \left( \frac{n_i(1 - 2p_i)}{2\sqrt{n_i p_i(1 - p_i)}} - S_i^* \right).$$

Обозначим  $a_i = \frac{n_i(1-2p_i)}{2\sqrt{n_i p_i(1-p_i)}}$ ,  $\tilde{\xi}_r = \frac{n_1 \dots n_r - 2\xi_r}{2^r \left( \prod_{i=1}^r n_i p_i(1-p_i) \right)^{1/2}}$ . Из (3) следует, что

$$\tilde{\xi}_r = \prod_{i=1}^r (a_i - S_i^*). \quad (6)$$

Перенумеруем векторы  $X^{(1)}, \dots, X^{(r)}$  так, что  $|a_1| \leq |a_2| \leq \dots \leq |a_r|$ .

**Теорема 2.** Пусть случайные величины в наборах  $X^{(1)}, \dots, X^{(r)}$  независимы в совокупности и имеют распределения (1). Пусть  $n_1, \dots, n_r \rightarrow \infty$  и вероятности  $p_i = p_i(n_i)$ ,  $i = 1, \dots, r$ , меняются так, что  $n_i p_i(1-p_i) \rightarrow \infty$ ,  $i = 1, \dots, k$ . Тогда если

$$a_i \rightarrow c_i \in \mathbb{R}, \quad i = 1, \dots, k, \quad |a_i| \rightarrow +\infty, \quad i = k+1, \dots, r, \quad 1 \leq k \leq r-1,$$

то  $\frac{\tilde{\xi}_r}{a_{k+1} \dots a_r} \xrightarrow{d} \prod_{i=1}^k \eta_i$ , где случайные величины  $\eta_1, \dots, \eta_r$  независимы и имеют нормальный закон распределения со средними  $c_1, \dots, c_r$  соответственно и единичными дисперсиями.

**Доказательство.** Заметим, что при указанных условиях выполнены условия теоремы Муавра — Лапласа для случайных величин  $S_i^*$ ,  $i = 1, \dots, k$  [8, гл. I, § 6], значит, при  $k = r$  утверждение теоремы очевидно. Пусть  $k \leq r-1$ . Из (6) следует, что

$$\begin{aligned} \frac{\tilde{\xi}_r}{a_{k+1} \dots a_r} &= \frac{1}{a_{k+1} \dots a_r} \prod_{i=1}^r (a_i - S_i^*) = \\ &= (a_1 - S_1^*) \dots (a_k - S_k^*) \left(1 - \frac{1}{a_{k+1}} S_{k+1}^*\right) \dots \left(1 - \frac{1}{a_r} S_r^*\right). \end{aligned} \quad (7)$$

При  $i = k+1, \dots, r$  из неравенства Чебышева имеем

$$\mathbf{P} \left\{ \left| 1 - \frac{1}{a_i} S_i^* - 1 \right| > x \right\} = \mathbf{P} \{ |S_i^*| > |a_i| x \} \leq \frac{1}{(a_i x)^2} \mathbf{D} S_i^* = \frac{1}{(a_i x)^2}. \quad (8)$$

Так как правая часть в неравенстве (8) стремится к нулю в условиях теоремы, то из (7) и (8) следует, что

$$\begin{aligned} a_i - S_i^* &\xrightarrow{d} \eta_i, \quad a_i \rightarrow c_i, \quad i = 1, \dots, k, \\ 1 - \frac{1}{a_i} S_i^* &\xrightarrow{\mathbf{P}} 1, \quad |a_i| \rightarrow +\infty, \quad i = k+1, \dots, r. \end{aligned}$$

Тогда из (7) и независимости случайных величин  $S_1^*, \dots, S_r^*$  получаем утверждение теоремы. ■

**Замечание 2.** Условия теоремы 2 выполнены, если, например,

$$p_i = \frac{1}{2} - \frac{c_i}{\sqrt{n_i}}, \quad i = 1, \dots, k, \quad p_i = \frac{1}{2} - \frac{A_i}{\sqrt{n_i}}, \quad i = k+1, \dots, r,$$

где  $c_1, \dots, c_k$  — постоянные, а  $A_{k+1}, \dots, A_r$  — бесконечно большие величины, такие, что  $A_i/\sqrt{n_i} \rightarrow 0$  при  $n_1, \dots, n_r \rightarrow \infty$ . В этом случае главный член дисперсии случайной величины  $\xi_r$  (см. (5)) равен

$$4^r \sum_{i=k+1}^r \sqrt{n_i} A_i \prod_{\substack{j=k+1, \dots, r; \\ j \neq i}} n_j A_j^2 \prod_{l=1}^k n_l c_l^2.$$

**Следствие 1.** Пусть выполнены условия теоремы 2 и  $a_i \rightarrow 0 \in \mathbb{R}$ ,  $i = 1, \dots, r$ . Тогда  $\tilde{\xi}_r \xrightarrow{d} \prod_{i=1}^r \eta_i$ , где случайные величины  $\eta_1, \dots, \eta_r$  независимы и имеют стандартный нормальный закон распределения.

**Замечание 3.** Следствие 1 указывает условия на характер изменения вероятностей  $p_1, \dots, p_r$ , при выполнении которых сохраняет свой вид предельное распределение следствия 2 работы [3].

**Теорема 3.** Пусть случайные величины в наборах  $X^{(1)}, \dots, X^{(r)}$  независимы в совокупности и имеют распределения (1). Пусть при  $n_1, \dots, n_r \rightarrow +\infty$  вероятности  $p_i = p_i(n_i)$ ,  $i = 1, \dots, r$ , меняются так, что  $n_i p_i(1 - p_i) \rightarrow \infty$ . Если  $|a_i| \rightarrow +\infty$ ,  $i = 1, \dots, r$ , то закон распределения случайной величины  $\frac{\tilde{\xi}_r - a_1 \dots a_r}{a_1 \dots a_r \sqrt{\frac{1}{a_1^2} + \frac{1}{a_2^2} + \dots + \frac{1}{a_r^2}}}$  сходится к стандартному нормальному закону.

**Доказательство.** Из (6) имеем

$$\begin{aligned} \frac{\tilde{\xi}_r}{a_2 \dots a_r} &= \frac{1}{a_2 \dots a_r} \prod_{i=1}^r (a_i - S_i^*) = (a_1 - S_1^*) \left(1 - \frac{1}{a_2} S_2^*\right) \dots \left(1 - \frac{1}{a_r} S_r^*\right) = \\ &= a_1 \left(1 - \sum_{i=2}^r \frac{S_i^*}{a_i} + \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} (-1)^i \frac{S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}}\right) = \\ &= a_1 - \sum_{i=2}^r \frac{a_1 S_i^*}{a_i} + \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} (-1)^i \frac{a_1 S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}}. \end{aligned} \quad (9)$$

Заметим, что при  $x > 0$  в силу неравенства Чебышева

$$\begin{aligned} \mathbf{P} \left\{ \left| \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} (-1)^i \frac{a_1 S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}} \right| > x \right\} &\leq \frac{1}{x^2} \mathbf{D} \left( \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} (-1)^i \frac{a_1 S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}} \right) \leq \\ &\leq \frac{1}{x^2} \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \sum_{i'=2}^r \sum_{1 \leq k_1 < \dots < k_{i'} \leq r} (-1)^{i+i'} \text{cov} \left( \frac{a_1 S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}}, \frac{a_1 S_{k_1}^* \dots S_{k_{i'}}^*}{a_{k_1} \dots a_{k_{i'}}} \right) \leq \\ &\leq \frac{1}{x^2} \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \sum_{i'=2}^r \sum_{1 \leq k_1 < \dots < k_{i'} \leq r} \left| \frac{a_1}{a_{j_1} \dots a_{j_i}} \right| \left| \frac{a_1}{a_{k_1} \dots a_{k_{i'}}} \right| \left| \text{cov} (S_{j_1}^* \dots S_{j_i}^*, S_{k_1}^* \dots S_{k_{i'}}^*) \right|. \end{aligned} \quad (10)$$

Заметим, что

$$\mathbf{D} (S_{j_1}^* \dots S_{j_i}^*) = \mathbf{E} (S_{j_1}^* \dots S_{j_i}^*)^2 = \mathbf{E} (S_{j_1}^*)^2 \dots \mathbf{E} (S_{j_i}^*)^2 = \mathbf{D} S_{j_1}^* \dots \mathbf{D} S_{j_i}^* = 1.$$

Если существует  $l$ , для которого  $j_l \notin \{k_1, \dots, k_{i'}\}$ , то

$$\begin{aligned} \text{cov} (S_{j_1}^* \dots S_{j_i}^*, S_{k_1}^* \dots S_{k_{i'}}^*) &= \mathbf{E} (S_{j_1}^* \dots S_{j_i}^* S_{k_1}^* \dots S_{k_{i'}}^*) = \\ &= \mathbf{E} S_{j_l}^* \mathbf{E} (S_{j_1}^* \dots S_{j_{l-1}}^* S_{j_{l+1}}^* \dots S_{j_i}^* S_{k_1}^* \dots S_{k_{i'}}^*) = 0. \end{aligned}$$

Значит,  $\text{cov} (S_{j_1}^* \dots S_{j_i}^*, S_{k_1}^* \dots S_{k_{i'}}^*) \neq 0$  только при  $i = i'$ ,  $j_1 = k_1, \dots, j_i = k_{i'}$  и

$$\text{cov} (S_{j_1}^* \dots S_{j_i}^*, S_{j_1}^* \dots S_{j_i}^*) = \mathbf{D} (S_{j_1}^* \dots S_{j_i}^*) = 1.$$

Подставляя последнюю оценку в (10), получаем

$$\mathbf{P} \left\{ \left| \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} (-1)^i \frac{a_1 S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}} \right| > x \right\} \leq \frac{1}{x^2} \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \left( \frac{a_1}{a_{j_1} \dots a_{j_i}} \right)^2. \quad (11)$$

Так как  $\frac{a_1}{a_{j_1} \dots a_{j_i}} \rightarrow 0$  при любом  $i \geq 2$ , правая часть формулы (11) стремится к нулю. Значит,

$$\frac{\tilde{\xi}_r - a_1 \dots a_r}{a_1 \dots a_r \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}} = - \left( \sum_{i=1}^r \frac{S_i^*}{a_i \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}} + \frac{1}{a_1 \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}} \eta \right), \quad (12)$$

где

$$\eta = \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} (-1)^i \frac{a_1 S_{j_1}^* \dots S_{j_i}^*}{a_{j_1} \dots a_{j_i}} \xrightarrow{P} 0. \quad (13)$$

Далее из свойств нормального распределения, ограниченности коэффициентов  $\frac{1}{a_i \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}}$  при всех  $i = 1, \dots, r$  выражения  $\sum_{i=1}^r \frac{S_i^*}{a_i \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}}$ , независимости случайных величин  $S_1^*, \dots, S_r^*$  и сходимости их распределений к стандартному нормальному закону получаем, что случайная величина  $\sum_{i=1}^r \frac{S_i^*}{a_i \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}}$  имеет в пределе стандартный нормальный закон распределения. Значит, из формул (12), (13) и симметричности плотности распределения стандартного нормального закона следует утверждение теоремы. ■

**Замечание 4.** Условия теоремы 3 выполнены, если, например, случайные величины в наборах  $X^{(1)}, \dots, X^{(r)}$  независимы в совокупности,  $n_i \rightarrow +\infty$  при всех  $i = 1, \dots, r$ , а вероятности  $p_i$  остаются постоянными.

Теперь обратимся к случаю, когда число регистров  $r$  при переходе к пределу стремится к бесконечности.

**Теорема 4.** Пусть случайные величины в наборах  $X^{(1)}, \dots, X^{(r)}$  независимы в совокупности и имеют распределения (1),  $p_i = p_i(n_i)$ ,  $i = 1, \dots, r$ . Пусть при  $r \rightarrow +\infty$  величины  $n_1, \dots, n_r$  и  $p_1, \dots, p_r$  меняются так, что

$$\sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \left( \frac{a_1}{a_{j_1} \dots a_{j_i}} \right)^2 \rightarrow 0 \quad \text{и} \quad \frac{\sum_{i=1}^r |a_i|^{-3} (p_i(1-p_i))^{-3/4}}{\left( \sum_{i=1}^r \frac{1}{a_i^2} \right)^{3/2}} \rightarrow 0. \quad (14)$$

Тогда закон распределения случайной величины  $\frac{\tilde{\xi}_r - a_1 \dots a_r}{a_1 \dots a_r \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}}$  сходится к стандартному нормальному закону.

**Доказательство.** Воспользуемся представлением (9). Из оценки (11) и первого из условий (14) следует соотношение (13). Значит, остаётся показать, что при  $r \rightarrow \infty$  случайная величина  $\nu = \sum_{i=1}^r \frac{S_i^*}{a_i \sqrt{\frac{1}{a_1^2} + \dots + \frac{1}{a_r^2}}}$  сходится по распределению к стандартному нормальному закону.

Для этого воспользуемся неравенством Берри — Эссеена [8, с. 356], согласно которому при любом  $x \in \mathbb{R}$

$$|F_\nu(x) - \Phi(x)| \leq C \frac{\sum_{i=1}^r \mathbf{E} \left| \frac{a_1 S_i^*}{a_i} \right|^3}{\left( 1 + \left( \frac{a_1}{a_2} \right)^2 + \dots + \left( \frac{a_1}{a_r} \right)^2 \right)^{3/2}} = C \frac{\sum_{i=1}^r \mathbf{E} \left| \frac{S_i^*}{a_i} \right|^3}{\left( \frac{1}{a_1^2} + \dots + \frac{1}{a_r^2} \right)^{3/2}}. \quad (15)$$

Оценим отдельно каждое слагаемое в числителе правой части последней оценки. В силу неравенства Ляпунова [9, с. 48] имеем

$$\mathbf{E} \left| \frac{S_i^*}{a_i} \right|^3 = \frac{1}{|a_i|^3} \mathbf{E} |S_i^*|^3 \leq \frac{1}{|a_i|^3} (\mathbf{E} (S_i^*)^4)^{3/4}.$$

Для вычисления  $\mathbf{E} (S_i^*)^4$  воспользуемся производящей функцией моментов для биномиальной случайной величины  $S_i$ . Обозначим через  $g_X(t) = \mathbf{E} e^{tX}$  производящую функцию моментов случайной величины  $X$ . Имеем

$$g_{S_i - n_i p_i}(t) = \mathbf{E} e^{t(S_i - n_i p_i)} = e^{-tn_i p_i} \mathbf{E} e^{tS_i} = e^{-tn_i p_i} g_{S_i}(t) = e^{-tn_i p_i} (1 - p_i + p_i e^t)^{n_i}.$$

Тогда

$$\begin{aligned} \mathbf{E} (S_i^*)^4 &= \frac{1}{(n_i p_i (1 - p_i))^2} \frac{d^4}{dt^4} g_{S_i - n_i p_i}(t) \Big|_{t=0} = \\ &= \frac{1}{(n_i p_i (1 - p_i))^2} \frac{n_i p_i (1 - p_i)}{24} (1 + 3(n_i - 2)p_i(1 - p_i)) = \\ &= \frac{1}{24n_i p_i (1 - p_i)} (1 + 3(n_i - 2)p_i(1 - p_i)) \leq \\ &\leq \frac{1}{24n_i p_i (1 - p_i)} \left( 1 + \frac{3}{4}(n_i - 2) \right) \leq \frac{1}{24n_i p_i (1 - p_i)} \frac{3}{4} n_i = \frac{1}{32p_i(1 - p_i)}. \end{aligned}$$

Поэтому в правой части неравенства (15) получим

$$|F_\nu(x) - \Phi(x)| \leq \frac{C}{(32)^{3/4}} \frac{\sum_{i=1}^r |a_i|^{-3} (p_i(1 - p_i))^{-3/4}}{\left( \frac{1}{a_1^2} + \dots + \frac{1}{a_r^2} \right)^{3/2}}.$$

В условиях теоремы правая часть последней оценки стремится к нулю при  $r \rightarrow \infty$ . ■

**Замечание 5.** Условия теоремы 4 выполнены, если, например, случайные величины в наборах  $X^{(1)}, \dots, X^{(r)}$  независимы в совокупности,  $r \rightarrow +\infty$ ,  $n_i \rightarrow +\infty$ , а

вероятности  $p_i$  остаются постоянными,  $\sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \frac{n_1}{n_{j_1} \dots n_{j_i}} \rightarrow 0$  и  $\frac{\sum_{i=1}^r n_i^{-3/2}}{\left( \sum_{i=1}^r \frac{1}{n_i} \right)^{3/2}} \rightarrow 0$ .

**Замечание 6.** Вместо условий (14) теоремы 4 можно написать более простые, но несколько более грубые условия:

$$\frac{r}{a_2} \rightarrow 0, \quad \max \left\{ (p_i(1 - p_i))^{-3/4} \right\} \frac{a_r^3}{a_1^2 \sqrt{r}} \rightarrow 0.$$

Действительно,

$$\begin{aligned} \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \left( \frac{a_1}{a_{j_1} \dots a_{j_i}} \right)^2 &\leq \sum_{i=2}^r \sum_{1 \leq j_1 < \dots < j_i \leq r} \left( \frac{a_1}{a_1 a_{j_2} \dots a_{j_i}} \right)^2 < \\ &< \sum_{i=2}^r C_r^i a_2^{-2(i-1)} = a_2^2 \sum_{i=2}^r C_r^i a_2^{-2i} = \\ &= a_2^2 \left( (1 + a_2^{-2})^r - 1 - \frac{r}{a_2^2} \right) \leq a_2^2 \left( e^{r/a_2^2} - 1 - \frac{r}{a_2^2} \right) \leq a_2^2 \frac{r^2}{2a_2^4} e^{r/a_2^2} = \frac{r^2}{2a_2^2} e^{r/a_2^2}. \end{aligned}$$

Значит, если  $r/a_2 \rightarrow 0$ , то выполнено первое из условий (14).

Аналогично

$$\begin{aligned} \frac{\sum_{i=1}^r |a_i|^{-3} (p_i(1-p_i))^{-3/4}}{\left( \sum_{i=1}^r \frac{1}{a_i^2} \right)^{3/2}} &\leq \max \left\{ (p_i(1-p_i))^{-3/4} \right\} \frac{\sum_{i=1}^r |a_i|^{-3}}{\left( \sum_{i=1}^r \frac{1}{a_i^2} \right)^{3/2}} \leq \\ &\leq \max \left\{ (p_i(1-p_i))^{-3/4} \right\} \frac{r}{|a_1|^3 (r a_r^{-2})^{3/2}} = \max \left\{ (p_i(1-p_i))^{-3/4} \right\} \frac{|a_r|^3}{|a_1|^3 \sqrt{r}}. \end{aligned}$$

Значит, если правая часть последней формулы стремится к нулю, то выполнено второе условие в (14).

### Заключение

Проведено исследование устойчивости модели, описывающей генератор Пола. Для этого изучены вероятностные свойства числа единиц в выходной последовательности мультициклического генератора над полем  $\text{GF}(2)$  в случае, когда двоичные случайные знаки, заполняющие регистры, независимы, а вероятности появления единиц в регистрах отличны от  $1/2$  и могут меняться с ростом длин регистров. Для случая фиксированного числа регистров доказана предельная теорема о сходимости распределения нормированного числа единиц к распределению произведения независимых случайных величин, каждая из которых распределена по стандартному нормальному закону. Доказана также нормальная предельная теорема для нормированного числа единиц в случае, когда число регистров стремится к бесконечности. Результаты показывают, что нарушение свойства равновероятности распределения знаков в регистрах приводит к существенным изменениям свойств указанных предельных распределений по сравнению с равновероятным случаем.

Автор выражает признательность В. Г. Михайлову за ценные замечания и постоянное внимание к работе.

### ЛИТЕРАТУРА

1. Pohl P. The multicyclic vector method of generating pseudo-random numbers. I. Theoretical background, description of the method and algebraic analysis. Report TRITA-NA-7307. Stockholm, Sweden: Royal Inst. of Technology, 1973. 36 p.
2. Pohl P. Description of MCV, a pseudo-random number generator // Scand. Actuarial J. 1976. No. 1. P. 1–14.
3. Меженная Н. М., Михайлов В. Г. О распределении числа единиц в выходной последовательности генератора Пола над полем  $\text{GF}(2)$  // Математические вопросы криптографии. 2013. Т. 4. № 4. С. 95–107.



4. Меженная Н. М. Предельные теоремы для числа плотных серий с заданными параметрами в выходной последовательности генератора Пола // Инженерный журнал: наука и инновации. 2013. № 4(16). С. 1–8.
5. Mezhennaya N. M. Convergence rate estimators for the number of ones in outcome sequence of MCV generator with  $m$ -dependent registers items // Siber. Electr. Math. Rep. 2014. V. 11. P. 18–25.
6. Douglas W. M. A nonlinear random number generator with known, long cycle length // Cryptologia. 1993. V. 17(1). P. 55–62.
7. Deng L.-Y. and Xu H. A system of high-dimensional, efficient, long-cycle and portable uniform random number generators // ACM Trans. Modeling Comp. Simul. 2003. V. 13(4). P. 299–309.
8. Ширяев А. Н. Вероятность. М.: Наука, 1989. 581 с.
9. Севастьянов Б. А. Курс теории вероятностей и математической статистики. М.: Наука, 1982. 256 с.

#### REFERENCES

1. Pohl P. The multicyclic vector method of generating pseudo-random numbers. I. Theoretical background, description of the method and algebraic analysis. Report TRITA-NA-7307. The Royal Institute of Technology, Department of Information Processing and Computer Science, Stockholm, Sweden, 1973. 36 p.
2. Pohl P. Description of MCV, a pseudo-random number generator. Scand. Actuarial J., 1976, no. 1, pp. 1–14.
3. Mezhennaya N. M., Mihajlov V. G. O raspredelenii chisla edinic v vyhodnoj posledovatel'nosti generatora Pola nad polem GF(2). Matematicheskie Voprosy Kriptografii, 2013, vol. 4, no. 4, pp. 95–107. (in Russian)
4. Mezhennaya N. M. Predel'nye teoremy dlja chisla plotnyh serij s zadannymi parametrami v vyhodnoj posledovatel'nosti generatora Pola. Inzhenernyj Zhurnal: Nauka i Innovacii, 2013, no. 4(16), pp. 1–8. (in Russian)
5. Mezhennaya N. M. Convergence rate estimators for the number of ones in outcome sequence of MCV generator with  $m$ -dependent registers items. Siber. Electr. Math. Rep., 2014, vol. 11, pp. 18–25.
6. Douglas W. M. A nonlinear random number generator with known, long cycle length. Cryptologia, 1993, vol. 17(1), pp. 55–62.
7. Deng L.-Y. and Xu H. A system of high-dimensional, efficient, long-cycle and portable uniform random number generators. ACM Trans. Modeling Comp. Simul., 2003, vol. 13(4), pp. 299–309.
8. Shirjaev A. N. Veroyatnost'. Moscow, Nauka Publ., 1989. 581 p. (in Russian)
9. Sevast'janov B. A. Kurs teorii veroyatnostej i matematicheskoy statistiki. Moscow, Nauka Publ., 1982. 256 p. (in Russian)