ТЕОРИЯ ВЕРОЯТНОСТЕЙ И МАТЕМАТИЧЕСКАЯ СТАТИСТИКА

УДК 519.214
DOI: 10.18101/2304-5728-2018-2-3-12

О ЧИСЛЕ ЕДИНИЦ В ОДНОЙ МУЛЬТИЦИКЛИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ С ЗАВИСИМЫМИ ЗНАКАМИ

© Меженная Наталья Михайловна
кандидат физико-математических наук, доцент,
Московский государственный технический университет им. Н. Э. Баумана
Россия, 105005, г. Москва, ул. 2-я Бауманская, 5
E-mail: natalia.mezhennaya@gmail.com

В работе рассмотрено одно обобщение классического мультициклического генератора с r регистрами, выходная последовательность которого состоит из элементов, образованных произведениями двоичных знаков в регистрах при их циклическом сдвиге друг относительно друга. Знаки, заполняющие каждый регистр, циклически m-зависимы, а регистры независимы между собой. Для случайной величины, равной числу единиц в описанной мультициклической последовательности, найдены математическое ожидание и дисперсия при помощи формулы, связывающей ее значение с количествами единиц в каждом из регистров. Доказана центральная предельная теорема для числа единиц, когда длины регистров стремятся к бесконечности, а параметры распределений знаков, заполняющих регистры, и число регистров остаются фиксированными. Рассмотрено несколько частных случаев применения предельной теоремы к последовательностям случайных величин специального вида, заполняющих регистры. Для случая независимых и неравновероятных заполнений регистров приведены численные значения скорости сходимости к предельному распределению в равномерной метрике.

Ключевые слова: мультициклическая последовательность; генератор Пола; число единиц; центральная предельная теорема; m-зависимые случайные величины.

Введение

Мультициклический генератор из r регистров над кольцом вычетов по модулю 2 был предложен в работе [1] и определен следующим образом. Пусть $(x_0^{(j)},\dots,x_{m_j-1}^{(j)})$, $j=1,\dots,r$ — векторы заполнений ячеек регистров взаимно простых длин $m_1,\dots,m_r$, $x_k^{(j)}\in\{0,1\}$, $k=0,\dots,m_j-1$. Знаки мультициклической последовательности образуются по правилу:

$$z_t = x_{t(m_1)}^{(1)} \oplus \dots \oplus x_{t(m_r)}^{(r)},$$

где $t(M)=t \bmod M$, $\oplus$ — операция сложения по модулю 2. Выходная последовательность такого генератора является чисто периодической с (возможно не минимальной) длиной периода $T=m_1\dots m_r$. Поэтому при исследовании ее свойств достаточно рассматривать отрезок длины T.

В работе [2] число единиц на цикле выходной последовательности ге-

нератора выражено через числа единиц в его регистрах. В работах [3–5] получены аналогичные формулы для частот знаков в выходной последовательности комбинирующего и фильтрующего генераторов [6]. С помощью этого подхода в [2] получен широкий спектр предельных теорем нормального типа для числа единиц в мультициклической последовательности, когда регистры заполнены независимыми в совокупности двоичными случайными величинами с равномерными распределениями. В [7] результаты работы [2] были обобщены на случай циклически m-зависимых [8, с. 468] заполнений внутри регистров. В [2] и [7] также получены оценки скорости сходимости в предельных теоремах в равномерной метрике [9, с. 475]. Случай неравновероятных независимых заполнений регистров рассмотрен в [10].

1. Постановка задачи

Пусть $Y_0^{(j)},\dots,Y_{m_j-1}^{(j)}$, $j=1,\dots,r$ — независимые одинаково распределенные двоичные случайные величины. Построим по ним последовательности циклически m-зависимых случайных величин [8, с. 468–469]: $X_k^{(j)} = f_j(Y_k^{(j)},\dots,Y_{(k+m-1)(m_j)}^{(j)})$, $k=0,\dots,m_j-1$, $j=1,\dots,r$. (1)

Здесь $f_1,\dots,f_r$ — булевы функции, существенно зависящие хотя бы от одной и не более чем от m переменных, $m<m_j$, $j=1,\dots,r$. Случай $m=1$ и $f_1,\dots,f_r \neq const$ соответствует последовательности независимых случайных величин.

Случайные величины $X_0^{(j)},\dots,X_{m_j-1}^{(j)}$ имеют одинаковые одномерные распределения в силу независимости и одинаковой распределенности случайных величин $Y_0^{(j)},\dots,Y_{m_j-1}^{(j)}$. Пусть

$$p_j = \mathbf{P}\{f_j(Y_k^{(j)},\dots,Y_{(k+m-1)(m_j)}^{(j)})=1\}. \quad (2)$$

Рассмотрим обобщение классического мультициклического генератора [1]. Построим мультициклический генератор с r регистрами, заполненными наборами $X_k^{(j)}$, $k=0,\dots,m_j-1$, $j=1,\dots,r$, который вырабатывает выходную последовательность по правилу:

$$Z_t = X_{t(m_1)}^{(1)}\dots X_{t(m_r)}^{(r)}. \quad (3)$$

В настоящей работе мы изучим вопрос об асимптотическом распределении числа единиц на цикле длины $T=m_1\dots m_r$ выходной последовательности генератора (3).

2. Число единиц на цикле выходной последовательности мультициклического генератора

Обозначим через $S_j = \sum_{k=0}^{m_j-1} X_k^{(j)}$ — число единиц в j-м регистре, $j = 1,\dots,r$, $\xi = \sum_{k=0}^{T-1} Z_k$ — число единиц в цикле последовательности (3).

Лемма 1. Пусть $m_1,\dots,m_r \geq 1$. Тогда имеет место равенство:

$$\xi = S_1 \dots S_r. \tag{4}$$

Доказательство леммы 1. Докажем формулу (4) по индукции. Пусть сначала $r = 2$. Заметим, что $\{Z_k = 1\} = \{X_{k(m_1)}^{(1)} = 1, X_{k(m_2)}^{(2)} = 1\}$. Всего можно получить $S_1 S_2$ пар единиц при циклическом сдвиге первого и второго регистров друг относительно друга. Таким образом, при $r = 2$ формула (4) доказана. Остается заметить, что мультициклический генератор с r регистрами может быть представлен как мультициклический генератор с двумя регистрами, первый из которых заполнен выходной последовательностью генератора из первых $r-1$ регистров исходного генератора, а второй регистр совпадает с r-м регистром исходного генератора. *Лемма 1 доказана.*

Лемма 2. Пусть закон распределения случайных величин $X_k^{(j)}$, $k = 0,\dots,m_j - 1$, $j = 1,\dots,r$, задается формулами (1) и (2), $m \geq 1$, $m_1,\dots,m_r \geq 2m-1$. Тогда математическое ожидание и дисперсия числа единиц ξ равны

$$\mathbf{E}\xi = Tp_1 \dots p_r,$$

$$\mathbf{D}\xi = T\prod_{j=1}^{r}\left(p_j + 2\sum_{1\leq l\leq m-1} \mathbf{P}\{X_0^{(j)} X_l^{(j)} = 1\} + (m_j - 2m + 1)p_j^2 \right) - (Tp_1 \dots p_r)^2. \tag{5}$$

Доказательство леммы 2. Начнем с вычисления $\mathbf{E}\xi$. Согласно определению случайной величины S_j:

$$\mathbf{E}S_j = \sum_{k=0}^{m_j-1} \mathbf{P}\{X_k^{(j)} = 1\} = \sum_{k=0}^{m_j-1} \mathbf{P}\{f_j(Y_k^{(j)},\dots,Y_{(k+m-1)(m_j)}^{(j)}) = 1\} =$$

$$= m_j \mathbf{P}\{f_j(Y_0^{(j)},\dots,Y_{m-1}^{(j)}) = 1\} = m_j p_j. \tag{6}$$

Случайные величины $S_1,\dots,S_r$ независимы в совокупности, поэтому

$$\mathbf{E}\xi = \mathbf{E}S_1 \dots \mathbf{E}S_r = m_1 p_1 \dots m_r p_r = Tp_1 \dots p_r$$

(мы воспользовались определением длины цикла T и формулой (6)).

Теперь вычислим $\mathbf{D}\xi$. Заметим, что

$$\mathbf{D}\xi = \mathbf{E}(S_1 \dots S_r)^2 - (\mathbf{E}S_1 \dots S_r)^2 = \mathbf{E}S_1^2 \dots \mathbf{E}S_r^2 - (Tp_1 \dots p_r)^2. \tag{7}$$

Снова воспользуемся определением случайной величины S_j:

$$\mathbf{E}S_j^2 = \mathbf{E}\left(\sum_{k=0}^{m_j-1} I\{X_k^{(j)}=1\}\right)^2 = \mathbf{E}\sum_{k=0}^{m_j-1} I\{X_k^{(j)}=1\} + \mathbf{E}\sum_{0\le k,l\le m_j-1;k\ne l} I\{X_k^{(j)}X_l^{(j)}=1\} =$$

$$= m_j p_j + \sum_{0\le k,l\le m_j-1;k\ne l} \mathbf{P}\{X_k^{(j)}X_l^{(j)}=1\} = m_j p_j + m_j \sum_{1\le l\le m_j-1} \mathbf{P}\{X_0^{(j)}X_l^{(j)}=1\}.$$

Так как случайная величина $X_0^{(j)}$ зависима со случайными величинами $X_1^{(j)},\ldots,X_{m-1}^{(j)}$ и $X_{m_j-m+1}^{(j)},\ldots,X_{m_j-1}^{(j)}$, то

$$\mathbf{E}S_j^2 = m_j p_j + 2m_j \sum_{1\le l\le m-1} \mathbf{P}\{X_0^{(j)}X_l^{(j)}=1\} + m_j \sum_{m\le l\le m_j-m} \mathbf{P}\{X_0^{(j)}=1\}\mathbf{P}\{X_l^{(j)}=1\} =$$

$$= m_j\left(p_j + 2\sum_{1\le l\le m-1} \mathbf{P}\{X_0^{(j)}X_l^{(j)}=1\} + (m_j-2m+1)p_j^2\right). \qquad (8)$$

Подставив (8) в (7), получим (5). *Лемма 2 доказана*.

Замечание 1. Из формулы (8) нетрудно получить, что

$$\mathbf{D}S_j^2 = m_j\left(p_j + 2\sum_{1\le l\le m-1} \mathbf{P}\{X_0^{(j)}X_l^{(j)}=1\} - (2m-1)p_j^2\right). \qquad (9)$$

Замечание 2. При $m=1$ и $p_j = 1/2$ (для независимых равномерно распределенных случайных величин) получим, что

$$\mathbf{E}\xi = 2^{-r}T,\ \mathbf{D}\xi = T\prod_{j=1}^{r}\left(\frac{1}{2}+(m_j-1)\frac{1}{4}\right) - (2^{-r}T)^2 = 4^{-r}T\prod_{j=1}^{r}\left(m_j+1\right) - 4^{-r}T^2 =$$

$$= 4^{-r}T\left(1+\sum_{k=1}^{r-1}\sum_{1\le j_1\le\ldots\le j_k<r} m_{j_1}\ldots m_{j_k}\right).$$

Обозначим

$$\sigma_j^2 = \frac{\mathbf{D}S_j}{m_j} = p_j + 2\sum_{1\le l\le m-1} \mathbf{P}\{X_0^{(j)}X_l^{(j)}=1\} - (2m-1)p_j^2,\ \ j=1,\ldots,r.$$

Теорема 1. Пусть закон распределения случайных величин $X_k^{(j)}$, $k=0,\ldots,m_j-1,\ \ j=1,\ldots,r$ задается формулами (1) и (2), длины регистров $m_1,\ldots,m_r\to\infty$, а $m\ge 1$ и $p_1,\ldots,p_r\in(0,1)$ остаются фиксированными, $\sum_{j=1}^{r}\sigma_j^2 > 0$. Тогда закон распределения случайной величины

$$\left(\sum_{j=1}^{r}\frac{\sigma_j^2}{m_j p_j^2}\right)^{-1/2}\left(\frac{\xi}{Tp_1\ldots p_r}-1\right) \qquad (10)$$

сходится к стандартному нормальному закону распределения.

Доказательство теоремы 1. Обозначим $S_j^* = \dfrac{S_j - m_j p_j}{\sigma_j\sqrt{m_j}}$ — центрированное и нормированное число единиц в j-м регистре,

ванное и нормированное число единиц в j-м регистре, $j=1,\dots,r$. Тогда (4) можно записать в виде:

$$\xi=\prod_{j=1}^{r}\left(m_j p_j+S_j^*\sigma_j\sqrt{m_j}\right)=Tp_1\dots p_r\prod_{j=1}^{r}\left(1+S_j^*\frac{\sigma_j}{p_j\sqrt{m_j}}\right).$$

Отсюда получим, что

$$\frac{\xi}{Tp_1\dots p_r}=\prod_{j=1}^{r}\left(1+S_j^*\frac{\sigma_j}{p_j\sqrt{m_j}}\right)=$$

$$=1+\sum_{j=1}^{r}S_j^*\frac{\sigma_j}{p_j\sqrt{m_j}}+\sum_{k=2}^{r}\sum_{1\le j_1<\dots<j_k\le r}\prod_{l=1}^{k}S_{j_l}^*\frac{\sigma_{j_l}}{p_{j_l}\sqrt{m_{j_l}}}.$$

Пусть $m_*=\min\{m_1,\dots,m_r\}$. Так как случайные величины $S_j^*/\sqrt{m_j}$ стремятся по вероятности к нулю при $m_1,\dots,m_r\to\infty$, то

$$\sqrt{m_*}\left(\frac{\xi}{Tp_1\dots p_r}-1\right)=\sqrt{m_*}\sum_{j=1}^{r}S_j^*\frac{\sigma_j}{p_j\sqrt{m_j}}+O(m_*^{-1/2}) \qquad (11)$$

(запись $\zeta=O(t)$ означает, что случайная величина ζt^{-1} ограничена по вероятности при $t\to\infty$). Значит, из (11) предельные при $m_1,\dots,m_r\to\infty$ законы распределения для $\sqrt{m_*}\left(\frac{\xi}{Tp_1\dots p_r}-1\right)$ и $\psi=\sqrt{m_*}\sum_{j=1}^{r}S_j^*\frac{\sigma_j}{p_j\sqrt{m_j}}$ совпадают. Остается заметить, что для каждой из независимых в совокупности случайных величин $S_1^*,\dots,S_r^*$ выполнена центральная предельная теорема (см. теорему 19.2.1 кн. [8, с. 469]). Поэтому предельный закон распределения случайной величины ψ является нормальным с нулевым средним и положительной дисперсией $m_*\sum_{j=1}^{r}\frac{\sigma_j^2}{m_j p_j^2}$. Значит, случайная величина (10) также имеет в пределе при $m_1,\dots,m_r\to\infty$ стандартное нормальное распределение. *Теорема 1 доказана.*

3. Частные случаи теоремы 1

Рассмотрим несколько частных случаев.

Пусть $m=1$, $X_k^{(j)}$, $k=0,\dots,m_j-1$, $j=1,\dots,r$, — независимые в совокупности двоичные случайные величины с одинаковым законом распределения: $\mathbf{P}\{X_k^{(j)}=1\}=1-\mathbf{P}\{X_k^{(j)}=0\}=p_j$. Тогда $\mathbf{D}S_j=m_j p_j(1-p_j)$ и $\sigma_j^2=p_j(1-p_j)$.

Следствие 1. Пусть $X_k^{(j)}$, $k=0,\dots,m_j-1$, $j=1,\dots,r$, — независимые в совокупности двоичные случайные величины с законом распределения:

$\mathbf{P}\{X_k^{(j)}=1\}=1-\mathbf{P}\{X_k^{(j)}=0\}=p_j$. Пусть $m_1,\ldots,m_r\to\infty$, $p_1,\ldots,p_r\in(0,1)$ остаются фиксированными. Тогда закон распределения случайной величины $\eta=\left(\sum_{j=1}^{r}\frac{1-p_j}{m_j p_j}\right)^{-1/2}\left(\frac{\xi}{Tp_1\ldots p_r}-1\right)$ сходится к стандартному нормальному закону.

В таблице 1 приведены значения расстояния в равномерной метрике d между функцией распределения случайной величины η и функцией распределения стандартного нормального закона Φ для мультициклической последовательности, образованной двумя регистрами.

Таблица 1

Значения $d(F_\eta,\Phi)$ для мультициклической последовательности с двумя регистрами

	$m_1=10;$ $m_2=11$	$m_1=30;$ $m_2=31$	$m_1=50;$ $m_2=51$	$m_1=100;$ $m_2=101$
$p_1=0.2; p_2=0.2$	0.186	0.106	0.076	0.055
$p_1=0.2; p_2=0.4$	0.134	0.071	0.053	0.037
$p_1=0.2; p_2=0.5$	0.111	0.061	0.046	0.032
$p_1=0.2; p_2=0.6$	0.095	0.054	0.040	0.027
$p_1=0.2; p_2=0.8$	0.103	0.041	0.032	0.022
$p_1=0.4; p_2=0.4$	0.109	0.069	0.052	0.036
$p_1=0.4; p_2=0.5$	0.093	0.056	0.039	0.026
$p_1=0.4; p_2=0.6$	0.085	0.048	0.031	0.021
$p_1=0.4; p_2=0.8$	0.069	0.040	0.031	0.022
$p_1=0.5; p_2=0.5$	0.097	0.058	0.044	0.031
$p_1=0.5; p_2=0.6$	0.084	0.046	0.033	0.021
$p_1=0.5; p_2=0.8$	0.068	0.030	0.021	0.013
$p_1=0.6; p_2=0.6$	0.091	0.051	0.041	0.029
$p_1=0.6; p_2=0.8$	0.060	0.027	0.019	0.011
$p_1=0.8; p_2=0.8$	0.088	0.052	0.040	0.028

Замечание 3. Утверждение следствия 1 для равновероятных распределений случайных величин $X_k^{(j)}$ ($p_j=1/2$, $j=1,\ldots,r$) получено в [11].

Пусть теперь $m=2$, $Y_0^{(j)},\ldots,Y_{m_j-1}^{(j)}$, $j=1,\ldots,r$ — независимые одинаково распределенные двоичные случайные величины:

$$\mathbf{P}\{Y_k^{(j)}=1\}=1-\mathbf{P}\{Y_k^{(j)}=0\}=p, \tag{12}$$

$$X_k^{(j)} = Y_k^{(j)} \oplus Y_{(k+1)(m_j)}^{(j)},\ \ k = 0,\ldots,m_j - 1,\ \ j = 1,\ldots,r. \qquad (13)$$

В этом случае

$$\mathbf{P}\{X_k^{(j)} = 1\} = \mathbf{P}\{X_0^{(j)} = 1\} = \mathbf{P}\{Y_0^{(j)} \oplus Y_1^{(j)} = 1\} = 2p(1-p),$$

$$\mathbf{P}\{X_k^{(j)} = X_{k+1}^{(j)} = 1\} = \mathbf{P}\{X_0^{(j)} = X_1^{(j)} = 1\} = \mathbf{P}\{Y_0^{(j)} \oplus Y_1^{(j)} = Y_1^{(j)} \oplus Y_2^{(j)} = 1\} =$$

$$= (1-p)^2 p + p^2(1-p) = p(1-p),$$

при этом элементы последовательности $X_k^{(j)},\ \ k = 0,\ldots,m_j - 1,$ не являющиеся соседними, независимы между собой (считаем элементы $X_0^{(j)}$ и $X_{m_j-1}^{(j)}$ соседними). Тогда формула (9) перепишется в виде:

$$\mathbf{D}S_j^2 = m_j\left(p_j + 2\mathbf{P}\{X_0^{(j)}X_1^{(j)} = 1\} - (4-1)p_j^2\right) =$$

$$= m_j\left(2p(1-p) + 2p(1-p) - 3(2p(1-p))^2\right) = 4p(1-p)m_j\left(1 - 3p(1-p)\right).$$

Значит, $\sigma_j^2 = 4p(1-p)\left(1-3p(1-p)\right)$ и имеет место следующее утверждение.

Следствие 2. Пусть случайные величины $X_k^{(j)},\ \ k = 0,\ldots,m_j - 1,$ $j = 1,\ldots,r$ определены равенствами (12) и (13). Пусть $m_1,\ldots,m_r \to \infty$, $p \in (0,1)$ фиксировано. Тогда закон распределения случайной величины:

$$\left(\frac{1-3p(1-p)}{p(1-p)}\sum_{j=1}^{r}\frac{1}{m_j}\right)^{-1/2}\left(\frac{\xi}{T2^r p^r (1-p)^r} - 1\right)$$

сходится к стандартному нормальному закону.

Замечание 4. При $p = 1/2$ случайные величины $X_k^{(j)},\ \ k = 0,\ldots,m_j - 1,$ $j = 1,\ldots,r,$ определенные равенствами (12) и (13), независимы в совокупности. В этом случае утверждения следствий 1 и 2 совпадают.

Рассмотрим еще один частный случай, когда распределения случайных величин вместо (13) задаются равенством:

$$X_k^{(j)} = Y_k^{(j)}Y_{(k+1)(m_j)}^{(j)},\ \ k = 0,\ldots,m_j - 1,\ \ j = 1,\ldots,r, \qquad (14)$$

а $Y_0^{(j)},\ldots,Y_{m_j-1}^{(j)},\ \ j = 1,\ldots,r$ — независимые одинаково распределенные двоичные случайные величины, удовлетворяющие (12). Тогда

$$\mathbf{P}\{X_k^{(j)} = 1\} = \mathbf{P}\{X_0^{(j)} = 1\} = \mathbf{P}\{Y_0^{(j)}Y_1^{(j)} = 1\} = p^2,$$

$$\mathbf{P}\{X_k^{(j)} = X_{k+1}^{(j)} = 1\} = \mathbf{P}\{X_0^{(j)} = X_1^{(j)} = 1\} = \mathbf{P}\{Y_0^{(j)}Y_1^{(j)} = Y_1^{(j)}Y_2^{(j)} = 1\} = p^3.$$

Аналогично следствию 2 имеет место следующее утверждение.

Следствие 3. Пусть случайные величины $X_k^{(j)},\ \ k = 0,\ldots,m_j - 1,$ $j = 1,\ldots,r$ определены равенствами (12) и (14). Пусть $m_1,\ldots,m_r \to \infty$, $p \in (0,1)$ фиксировано. Тогда закон распределения случайной величины

$$\left(\frac{1+2p-3p^2}{p^2}\sum_{j=1}^{r}\frac{1}{m_j}\right)^{-1/2}\left(\frac{\xi}{Tp^{2r}}-1\right)$$

сходится к стандартному нормальному закону.

Заключение

В работе рассмотрено обобщение классического мультициклического генератора с r регистрами над кольцом вычетов по модулю 2. Знаки внутри каждого регистра циклически m-зависимы, а регистры независимы между собой. Доказана центральная предельная теорема для числа единиц в цикле мультициклической последовательности, когда длины регистров стремятся к бесконечности, а параметры распределений знаков, заполняющих регистры, и их число остаются фиксированными. Рассмотрено несколько частных случаев применения предельной теоремы к последовательностям случайных величин специального вида. Получены численные значения скорости сходимости к нормальному распределению в равномерной метрике для независимых и неравновероятных заполнений регистров.

Литература

1. Pohl P. Description of MCV, a pseudo-random number generator // Scand. Actuar. J. 1976. Vol. 1. P. 1–14. DOI: 10.1080/03461238.1976.10405931.

2. 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. DOI: 10.4213/mvk101.

3. Биляк И. Б., Камловский О. В. Частотные характеристики циклов выходных последовательностей комбинирующих генераторов над полем из двух элементов // Прикладная дискретная математика. 2015. Т. 3, № 29(3). С. 17–31. DOI: 10.17223/20710410/29/2.

4. Камловский О. В. Количество появлений векторов на циклах выходных последовательностей двоичных комбинирующих генераторов // Проблемы передачи информации. 2017. Т. 53, № 1. С. 84–91. DOI: 10.1134/S0032946017010070.

5. Камловский О. В. Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. Т. 3, № 21. С. 11–25.

6. Агибалов Г. П. Конечные автоматы в криптографии // Прикладная дискретная математика. Приложение. 2009. Т. 2. С. 43–73.

7. Mezhennaya N. M. Convergence rate estimators for the number of ones in outcome sequence of MCV generator with m-dependent registers items // Sib. Electron. Math. Reports. 2014. Vol. 11. P. 18–25.

8. Ибрагимов И. А., Линник Ю. В. Независимые и стационарно связанные величины. М.: Наука, 1965. 524 с.

9. Ширяев А. Н. Вероятность-1. 4–е изд. М.: Изд-во МЦНМО, 2011. 552 с.

10. Меженная Н. М. О распределении числа единиц в двоичной мультициклической последовательности // Прикладная дискретная математика. 2015. Т. 1(27). С. 69–77.

11. Mezhennaya N. M., Mikhailov V. G. Limit theorem for number of ones in the extended Pohl generator outcome sequence // OP&PM Surveys on Applied and Industrial Mathematics. 2018. Vol. 25, № 1. P. 48–50.

ON THE NUMBER OF ONES IN A MULTI-CYCLIC SEQUENCE WITH DEPENDENT SIGNS

Natalya M. Mezhennaya
Cand. Sci. (Phys. and Math.), A/Prof.,
Bauman Moscow State Technical University
5 2nd Bauman St., Moscow 105005, Russia
E-mail: natalia.mezhennaya@gmail.com

The article considers one extension of a classical multi-cyclic generator with r registers, which output sequence consists of elements formed by the products of binits in the registers under their cyclic shift relative to each other. The signs that fill each register are cyclically m-dependent, and the registers are independent of each other. We have found the mathematical expectation and variance for a random variable equal to the number of ones in the presented multi-cyclic sequence using the formula connecting its value with the number of ones for each registers. The central limit theorem for the number of ones is proved under the conditions when the lengths of registers tend to infinity, and the parameters of signs distributions filling the registers and the number of registers are fixed. We consider several particular cases of the limit theorem application to the sequences of random variables of a special type filling the registers. The numerical values of the convergence rate to the limiting distribution in the uniform metric for the case of independent and non-uniform fillings of registers are given.
Keywords: multi-cyclic sequence; Pohl generator; number of ones; central limit theorem; m-dependent random variables.

References

1. Pohl P. Description of MCV, a Pseudo-Random Number Generator. *Scand. Actuar. J.* 1976. V. 1. Pp. 1–14. DOI: 10.1080/03461238.1976.10405931.

2. Mezhennaya N. M., Mikhailov V. G. O raspredelenii chisla edinits v vykhodnoi posledovatel'nosti generatora Pola nad polem GF (2) [On the Distribution of the Number of Ones in the Output Sequence of MCV-Generator over GF(2)]. *Matematicheskie voprosy kriptografii — Mathematical Aspects of Cryptography.* 2013. V. 4. No. 4. Pp. 95–107. DOI: 10.4213/mvk101.

3. Bilyak I. B., Kamlovskii O. V. Chastotnye kharakteristiki tsiklov vykhodnykh posledovatel'nostei kombiniruyushchikh generatorov nad polem iz dvukh elementov [Frequency Characteristics of Cycles in Output Sequences Generated by Combining Generators over a Field of Two Elements]. *Prikladnaya diskretnaya matematika — Applied Discrete Mathematics.* 2015. V. 3, No. 29 (3). Pp. 17–31. DOI: 10.17223/20710410/29/2.

4. Kamlovskii O. V. Kamlovskii O. V. Kolichestvo poyavlenii vektorov na tsiklakh vykhodnykh posledovatel'nostei dvoichnykh kombiniruyushchikh generatorov [Occurrence Numbers for Vectors in Cycles of Output Sequences of Binary Combining Generators]. *Problemy peredachi informatsii — Problems of Information Transmission.* 2017. V. 53, No. 1. Pp. 84–91. DOI: 10.1134/S0032946017010070.

5. Kamlovskii O. V. Kolichestvo poyavlenii elementov v vyhodnyh posledovatel'nostyah fil'truyuschih generatorov [Distribution Properties of Sequences Produced by Filtering Generators]. *Prikladnaya diskretnaya matematika — Applied Discrete Mathematics.* 2013. V. 3, No. 21. Pp. 11–25.

6. Agibalov G. P. Konechnye avtomaty v kriptografii [Finite Automata in Cryptography]. *Prikladnaya diskretnaya matematika. Prilozhenie — Applied Discrete Mathematics. Supplement.* 2009. V. 2. Pp. 43–73.

7. Mezhennaya N. M. Convergence Rate Estimators for the Number of Ones in Outcome Sequence of MCV-generator with *m*-dependent Registers Items. *Sib. Electron. Math. Reports.* 2014. V. 11. Pp. 18–25.

8. Ibragimov I. A., Linnik Yu. V. *Nezavisimye i statsionarno svyazannye velichiny* [Independent and Stationary Related Variables]. Moscow: Nauka Publ., 1965, 524 p.

9. Shiryaev A. N. *Veroyatnost'-1* [Probability-1]. 4th ed. Moscow: MTsNMO, 2011. 552 p.

10. Mezhennaya N. M. O raspredelenii chisla edinits v dvoichnoi mul'titsiklicheskoi posledovatel'nosti [On Distribution of Number of Ones in Binary Multicycle Sequence]. *Prikladnaya diskretnaya matematika — Applied Discrete Mathematics.* 2015. V. 1(27). Pp. 69–77.

11. Mezhennaya N. M., Mikhailov V. G. Limit Theorem for Number of Ones in the Extended Pohl Generator Outcome Sequence. *OP&PM Surveys on Applied and Industrial Mathematics.* 2018. V. 25. No. 1. Pp. 48–50.