Дискретная математика

том 29 выпуск 3 * 2017

УДК 519.212.2+519.214 DOI https://doi.org/10.4213/dm1457

О свойствах выходной последовательности мультициклического генератора над прямой суммой групп вычетов по модулю 2

© 2017 г. Н. М. Меженная*, В. Г. Михайлов**

Выведена формула для частот знаков в выходной последовательности мультициклического генератора над прямой суммой групп вычетов по модулю 2. В случае, когда заполнения регистров генератора случайны и равновероятны, а длины регистров стремятся к бесконечности, найдено предельное совместное распределение для этих случайных величин.

Ключевые слова: мультициклический генератор, прямая сумма групп вычетов по модулю 2, случайная мультициклическая последовательность, частоты знаков

1. Введение

Пусть G — конечная абелева группа с операцией сложения $\circ$, а $n_1, \ldots, n_r \geqslant 2$ — взаимно простые натуральные числа. Мультициклический генератор псевдослучайных элементов группы G содержит r циклических регистров длин $n_1, \ldots, n_r$, ячейки которых заполнены элементами $X_0^{(j)}, \ldots, X_{n_j-1}^{(j)} \in G$, $j = 1, \ldots, r$, соответственно. Он вырабатывает последовательность $\{Z_t\}_{t \geqslant 0}$ (называемую мультициклической последовательностью) по правилу

$$Z_t = X_{t(n_1)}^{(1)} \circ \ldots \circ X_{t(n_r)}^{(r)}, \quad t = 0, 1, \ldots, \tag{1}$$

где $t(n_j) = t - [t/n_j]n_j$. Здесь и далее через $[x]$ обозначена целая часть числа x.

Первые исследования, относящиеся к рассматриваемым далее свойствам мультициклического генератора, были проведены в работах [1], [2], где в качестве G рассматривалась группа $\mathbb{Z}_2$ (группа вычетов по модулю 2).

Если величины в регистрах случайны и имеют равномерное распределение на G, то последовательность Z_t представляет собой теоретико-вероятностную модель выходной последовательности мультициклического генератора, и ее можно использовать при изучении статистических свойств последней.

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

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

Отрезок $Z = (Z_0, Z_1, \ldots, Z_{n_1 \ldots n_r - 1})$ принято называть *циклом* мультициклической последовательности $\{Z_t\}$. Пусть

$$\varkappa(h) = \sum_{i=0}^{n_1 \ldots n_r - 1} I\{Z_i = h\}, \quad h \in G.$$

Далее эти величины называем *частотами* элементов $h \in G$ в мультициклической последовательности.

В [3], [4], [5] было изучено асимптотическое поведение при $n_1, \ldots, n_r \to \infty$ распределения величины $\varkappa(1)$ в случае, когда $G = \mathbb{Z}_2$, а в [6], [7] — асимптотическое поведение совместного распределения величин $\varkappa(h)$ в случае $G = \mathbb{Z}_4$.

Целью настоящей работы является изучение свойств величин $\varkappa(h)$, в частности, асимптотического поведения при $n_1, \ldots, n_r \to \infty$ их совместного распределения в случае, когда G — прямая сумма $m \geqslant 2$ групп $\mathbb{Z}_2$ с операцией сложения по модулю 2. Обозначим

$$\mathbb{G}_m = \bigoplus_{l=1}^{m} \mathbb{Z}_2^{(l)}, \quad \text{где} \quad \mathbb{Z}_2^{(1)}, \ldots, \mathbb{Z}_2^{(m)} \quad \text{— копии группы} \quad \mathbb{Z}_2.$$

Известно (см., например, [8]), что в случае, когда абелева группа G порядка $|G| = q_1 \ldots q_s$ является прямой суммой s циклических групп порядков $q_1, \ldots, q_s$, элемент $h \in G$ может рассматриваться как вектор $\mathbf{h} = (h_1, \ldots, h_s)$, где h_j — элемент поля вычетов по модулю q_j, $j = 1, \ldots, s$. Поэтому элемент $h \in \mathbb{G}_m$ будем рассматривать как вектор $\mathbf{h} = (h_1, \ldots, h_m)$, где $h_1, \ldots, h_m \in \mathbb{Z}_2$.

Пусть

$$X^{(j)} = (X_0^{(j)}, \ldots, X_{n_j - 1}^{(j)}), \quad j = 1, \ldots, r,$$

$$X_{k_j}^{(j)} = (X_{k_j}^{1,(j)}, \ldots, X_{k_j}^{m,(j)}), \quad k_j = 0, \ldots, n_j - 1, \ j = 1, \ldots, r,$$

где $X_{k_j}^{u,(j)} \in \mathbb{Z}_2$.

В этом случае $Z_t = (Z_t^1, \ldots, Z_t^m)$, где $Z_t^1, \ldots, Z_t^m$ — элементы группы $\mathbb{Z}_2$, а равенство (1) записывается в виде m равенств

$$Z_t{}^u = X_{t(n_1)}^{u,(1)} + \ldots + X_{t(n_r)}^{u,(r)} \bmod 2, \quad t = 0, 1, \ldots, \quad u = 1, \ldots, m. \tag{2}$$

Для каждого набора $\mathbf{g} = (g_1, \ldots, g_m) \in \mathbb{G}_m \backslash \{\mathbf{0}\}$, где $\mathbf{0} = (0, \ldots, 0)$ — нулевой элемент группы $\mathbb{G}_m$, введем величины

$$X_{k_j}^{(g_1, \ldots, g_m)(j)} = g_1 X_{k_j}^{1,(j)} + \ldots + g_m X_{k_j}^{m,(j)} \bmod 2, \tag{3}$$

где $k_j = 0, \ldots, n_j - 1$, $j = 1, \ldots, r$, и последовательности

$$Z_t^{(g_1, \ldots, g_m)} = g_1 Z_t^1 + \ldots + g_m Z_t^m \bmod 2,$$

получаемые по формуле (1) как выходные последовательности двоичного генератора Пола с этими заполнениями.

Пусть $\varkappa^{(g_1,\ldots,g_m)}(h)$ — число появлений знака $h \in \mathbb{Z}_2$ в наборе

$$Z_0^{(g_1,\ldots,g_m)}, \ldots, Z_{n_1\ldots n_r-1}^{(g_1,\ldots,g_m)},$$

а $\varkappa(\mathbf{h})$ — число появлений знака $\mathbf{h} = (h_1, \ldots, h_m) \in \mathbb{G}_m$ в цикле выходной последовательности рассматриваемого генератора над $\mathbb{G}_m$, т. е. в наборе $Z_0, \ldots, Z_{n_1\ldots n_r-1}$.

Теорема 1. *При всех* $\mathbf{h} = (h_1, \ldots, h_m) \in \mathbb{G}_m$

$$\varkappa(\mathbf{h}) = \frac{1}{2^{m-1}} \sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\setminus\{\mathbf{0}\}} \varkappa^{(g_1,\ldots,g_m)}(g_1h_1 + \ldots + g_mh_m) - -\frac{(2^{m-1}-1)}{2^{m-1}} n_1 \ldots n_r. \tag{4}$$

При $m = 2$ утверждение теоремы 1 имеет более простой вид.

Следствие 1. *При всех* $h_1, h_2 \in \mathbb{Z}_2$

$$\varkappa(h_1, h_2) = \frac{1}{2}\big(\varkappa^{(1,0)}(h_1) + \varkappa^{(0,1)}(h_2) + \varkappa^{(1,1)}(h_1 + h_2) - n_1 \ldots n_r\big).$$

Пусть теперь наборы $X^{(j)} = (X_0^{(j)}, \ldots, X_{n_j-1}^{(j)})$, $j = 1, \ldots, r$, образованы независимыми в совокупности случайными величинами, имеющими равномерное распределение на множестве элементов группы $\mathbb{G}_m$. Тогда

$$X_{k_j}^{(j)} = (X_{k_j}^{1,(j)}, \ldots, X_{k_j}^{m,(j)}), \quad k_j = 0, \ldots, n_j - 1,\ j = 1, \ldots, r,$$

где величины $X_{k_j}^{u,(j)}$ независимы в совокупности и имеют равномерное распределение на $\mathbb{Z}_2$.

В этом случае набор $\left(Z_t^1, \ldots, Z_t^m\right)$ состоит из независимых в совокупности случайных последовательностей элементов группы $\mathbb{Z}_2$ (нулей и единиц).

При $\mathbf{h} = (h_1, \ldots, h_m) \in \mathbb{G}_m$ введем обозначение

$$\tilde{\varkappa}(\mathbf{h}) = \frac{2^m\varkappa(\mathbf{h}) - n_1 \ldots n_r}{\sqrt{n_1 \ldots n_r}}.$$

Через Φ_r обозначим распределение произведения r независимых случайных величин, имеющих стандартное гауссовское распределение.

Теорема 2. *Пусть случайные величины* $X_t^{(j)}$ *независимы в совокупности и имеют равномерное распределение на* $\mathbb{G}_m$. *Тогда при* $n_1, \ldots, n_r \to \infty$ *распределение вектора* $(\tilde{\varkappa}(\mathbf{h}), \mathbf{h} \in \mathbb{G}_m)$ *сходится к распределению вектора* $(\alpha(\mathbf{h}), \mathbf{h} \in \mathbb{G}_m)$, *где*

$$\alpha(\mathbf{h}) = \sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\setminus\{\mathbf{0}\}} (-1)^{g_1h_1+\ldots+g_mh_m} \xi_{g_1,\ldots,g_m},$$

а случайные величины $\xi_{g_1,\ldots,g_m}, (g_1, \ldots, g_m) \in \mathbb{G}_m\setminus\{\mathbf{0}\}$, *независимы в совокупности и имеют одно и то же распределение* Φ_r.

Следствие 2. *Пусть выполнены условия теоремы* 2. *Тогда для каждого* $\mathbf{h} \in \mathbb{G}_m$ *при* $n_1, \ldots, n_r \to \infty$ *распределение случайной величины* $\tilde{\varkappa}(\mathbf{h})$ *сходится к свертке* $2^m - 1$ *распределений* Φ_r.

Замечание 1. При $m = 1$ аналогичная следствию 2 предельная теорема была доказана в [3]. Там же была получена оценка скорости сходимости в этой предельной теореме.

2. Вспомогательные результаты

Пусть G — конечная абелева группа с операцией сложения $\circ$. Для генератора Пола над группой G существует формула, выражающая частоты знаков в цикле выходной последовательности генератора через частоты знаков в его регистрах (см. Основную лемму ниже).

Введем обозначение $\nu^{(j)}(g)$ для числа появлений элемента $g \in G$ в последовательности $X^{(j)} = (X_0^{(j)}, \ldots, X_{n_j-1}^{(j)})$, $j = 1, \ldots, r$, и обозначение $\varkappa(g)$ для числа появлений элемента $g \in G$ на цикле последовательности Z. Нам также понадобятся обозначения

$$\nu^{(j)} = (\nu^{(j)}(g), g \in G), \quad j = 1, \ldots, r, \quad \varkappa = (\varkappa(g), g \in G). \tag{5}$$

Выразим вектор $\varkappa$ через векторы $\nu^{(j)}$, $j = 1, \ldots, r$. Для этого воспользуемся известными свойствами вероятностных распределений на конечных группах.

Введем вероятностные распределения на G

$$P^{(j)} = \left(\frac{\nu^{(j)}(g)}{n_j}, g \in G \right), \ j = 1, \ldots, r, \quad P = \left(\frac{\varkappa(g)}{n_1 \ldots n_r}, \ g \in G \right). \tag{6}$$

Из формулы (1) и взаимной простоты $n_1, \ldots, n_r$ (см. введение) следует, что

$$P = P^{(1)} \star \ldots \star P^{(r)}, \tag{7}$$

где $\star$ обозначает операцию свертки распределений на группе G.

Рассмотрим случайные элементы $\eta^{(1)}, \ldots, \eta^{(r)}$, выбранные независимо из G в соответствии с распределениями $P^{(1)}, \ldots, P^{(r)}$. Равенство (7) означает, что P является распределением суммы $\eta = \eta^{(1)} \circ \ldots \circ \eta^{(r)}$.

Пусть $\chi_g(h)$, $g, h \in G$, — характеры группы G, а $\bar{z}$ — комплексное число, сопряженное с z, а $\mathcal{O}$ — нулевой элемент группы G. Напомним, что характеры $\chi_g(h)$ обладают следующими свойствами (см., например, [8]):

$$\chi_g(h' \circ h'') = \chi_g(h')\chi_g(h''),$$

$$\chi_g(\mathcal{O}) = 1, \quad \chi_g(h) = \chi_h(g),$$

$$\sum_{g \in G} \chi_g(\mathcal{O}) = |G|, \qquad \sum_{g \in G} \chi_g(h) = 0, \quad h \neq \mathcal{O}.$$

Основная лемма. *При* $r \geqslant 2$

$$\varkappa(h) = \frac{1}{|G|} \sum_{g \in G} \chi_g(h) \prod_{j=1}^{r} D_g^{(j)}, \quad h \in G, \tag{8}$$

где

$$D_g^{(j)} = \sum_{h\in G} \nu^{(j)}(h)\bar{\chi}_g(h), \quad g \in G. \tag{9}$$

Доказательство. Распределение произвольной случайной величины η со значениями в конечной абелевой группе G, следуя [9], запишем 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, $\Delta_{\mathcal{O}} = 1$.

Пусть случайные величины η' и η'' со значениями в G независимы, $\eta = \eta' \circ \eta''$, а характеристики Δ_g, ${\Delta'}_g$, ${\Delta''}_g$ отвечают случайным величинам η, η', η'' соответственно. Тогда при всех $g \in G$ выполнено равенство $\Delta_g = {\Delta_g}'{\Delta_g}''$.

Поэтому в нашем случае

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

где

$$\Delta_g^{(j)} = \sum_{h'\in G} \mathbf{P}\{\eta^{(j)} = h'\}\bar{\chi}_g(h') = \frac{D_g^{(j)}}{n_j}. \tag{10}$$

Согласно (6)

$$\mathbf{P}\{\eta^{(j)} = h\} = \frac{\nu^{(j)}(h)}{n_j}, \ j = 1, \ldots, r, \quad \mathbf{P}\{\eta = h\} = \frac{\varkappa(h)}{n_1 \ldots n_r}, \quad h \in G.$$

Поэтому

$$\frac{\varkappa(h)}{n_1 \ldots n_r} = \frac{1}{|G|}\sum_{g\in G} \chi_g(h) \prod_{j=1}^{r} \Delta_g^{(j)}, \quad h \in G,$$

где

$$\Delta_g^{(j)} = \sum_{h\in G} \frac{\nu^{(j)}(h)}{n_j}\bar{\chi}_g(h), \quad g \in G,$$

что согласно (10) равносильно (8). Лемма доказана.

Перейдем к исследованию свойств абелевой группы $\mathbb{G}_m$. Как уже отмечалось выше, элемент $h \in \mathbb{G}_m$ может рассматриваться как вектор $\mathbf{h} = (h_1, \ldots, h_m)$, где $h_1, \ldots, h_m$ — элементы поля вычетов по модулю 2, $j = 1, \ldots, s$. Для него выполнена формула (см. [8])

$$\chi_{\mathbf{g}}(\mathbf{h}) = \chi_{g_1,\ldots,g_m}(h_1, \ldots, h_m) = (-1)^{g_1h_1+\ldots+g_mh_m}. \tag{11}$$

Согласно (9) при всех $j = 1, \ldots, r$

$$D_{g_1,\ldots,g_m}^{(j)} = \sum_{(h_1,\ldots,h_m)\in\mathbb{G}_m} \nu^{(j)}(h_1, \ldots, h_m)(-1)^{g_1h_1+\ldots+g_mh_m}.$$

Здесь $\nu^{(j)}(h_1,\ldots,h_m)$ — число появлений знака $(h_1,\ldots,h_m)$ в заполнении j-го регистра генератора. Ясно, что $D^{(j)}_{0,\ldots,0}=n_j$.

Подставив эти выражения в (8), получим, что при $\mathbf{h}=(h_1,\ldots,h_m)\in\mathbb{G}_m$

$$\varkappa(\mathbf{h})=\varkappa(h_1,\ldots,h_m)=\frac{1}{2^m}\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m}(-1)^{g_1h_1+\ldots+g_mh_m}D_{g_1,\ldots,g_m}=$$

$$=\frac{1}{2^m}\left(n_1\ldots n_r+\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\setminus\{\mathbf{0}\}}(-1)^{g_1h_1+\ldots+g_mh_m}D_{g_1,\ldots,g_m}\right), \tag{12}$$

где

$$D_{g_1,\ldots,g_m}=\prod_{j=1}^{r}D^{(j)}_{g_1,\ldots,g_m}. \tag{13}$$

При $m=1$ эта система равенств приводится к виду

$$(-1)^h\big(2\varkappa(h)-n_1\ldots n_r\big)=D^{(1)}_1\ldots D^{(r)}_1,\quad h\in\mathbb{Z}_2. \tag{14}$$

Замечание 2. Аналогичная (12) система равенств выполнена и для величин $\nu^{(j)}(h_1,\ldots,h_m)$, $j=1,\ldots,r$:

$$\nu^{(j)}(h_1,\ldots,h_m)=\frac{1}{2^m}\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m}(-1)^{g_1h_1+\ldots+g_mh_m}D^{(j)}_{g_1,\ldots,g_m}=$$

$$=\frac{1}{2^m}\left(n_j+\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\setminus\{\mathbf{0}\}}(-1)^{g_1h_1+\ldots+g_mh_m}D^{(j)}_{g_1,\ldots,g_m}\right). \tag{15}$$

В частности,

$$\nu^{(j)}(0,\ldots,0)=\frac{1}{2^m}\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m}D^{(j)}_{g_1,\ldots,g_m},\quad j=1,\ldots r.$$

3. Доказательство теоремы 1

Напомним, что при $k_j=0,\ldots,n_j-1,\ j=1,\ldots,r$

$$X^{(g_1,\ldots,g_m)(j)}_{k_j}=g_1X^{1,(j)}_{k_j}+\ldots+g_mX^{m,(j)}_{k_j}\bmod 2.$$

Пусть $\nu^{(g_1,\ldots,g_m)(j)}(h)$ — число появлений знака $h\in\mathbb{Z}_2$ в наборе

$$X^{(g_1,\ldots,g_m)(j)}_0,\ldots,X^{(g_1,\ldots,g_m)(j)}_{n_j-1}.$$

Лемма 1. *При всех $j=1,\ldots,r$ и всех $g_1,\ldots,g_m\in\mathbb{Z}_2$*

$$D^{(j)}_{g_1,\ldots,g_m}=\nu^{(g_1,\ldots,g_m)(j)}(0)-\nu^{(g_1,\ldots,g_m)(j)}(1)=2\nu^{(g_1,\ldots,g_m)(j)}(0)-n_j. \tag{16}$$

В частности, $D^{(j)}_{0,\ldots,0}=n_j$.

Доказательство (леммы 1). Согласно определению

$$D^{(j)}_{g_1,\ldots,g_m} = \sum_{(h_1,\ldots,h_m)\in\mathbb{G}_m} \nu^{(j)}(h_1,\ldots,h_m)(-1)^{h_1g_1+\ldots+h_mg_m} =$$

$$= \sum_{(h_1,\ldots,h_m)\in\mathbb{G}_m} \sum_{t=0}^{n_j-1} I\{X_t^{(j)} = (h_1,\ldots,h_m)\}(-1)^{g_1h_1+\ldots+g_mh_m} =$$

$$= \sum_{t=0}^{n_j-1} (-1)^{g_1X_t^{1,(j)}+\ldots+g_mX_t^{m,(j)}}. \tag{17}$$

В последней сумме слагаемое равно 1, если

$$X_t^{1,(j)}g_1 + \ldots + X_t^{m,(j)}g_m = 0 \mod 2,$$

и равно -1 в противном случае. Значит,

$$D^{(j)}_{g_1,\ldots,g_m} = \sum_{t=0}^{n_j-1} I\{X_t^{1,(j)}g_1 + \ldots + X_t^{m,(j)}g_m = 0 \mod 2\} -$$

$$- \sum_{t=0}^{n_j-1} I\{X_t^{1,(j)}g_1 + \ldots + X_t^{m,(j)}g_m = 1 \mod 2\},$$

откуда следует, что

$$D^{(j)}_{g_1,\ldots,g_m} = \nu^{(g_1,\ldots,g_m),(j)}(0) - \nu^{(g_1,\ldots,g_m),(j)}(1) = 2\nu^{(g_1,\ldots,g_m)(j)}(0) - n_j.$$

Осталось заметить, что $\nu^{(0,\ldots,0)(j)}(0) = n_j$, $j = 1,\ldots,r$. Лемма 1 доказана.

Перейдем к доказательству теоремы 1. Из (14) и (16) вытекает, что при $(g_1,\ldots,g_m) \in \mathbb{G}_m\backslash\{\mathbf{0}\}$ и любом $h \in \mathbb{Z}_2$

$$D_{g_1,\ldots,g_m} = \prod_{j=1}^{r} D^{(j)}_{g_1,\ldots,g_m} = (-1)^h\Big(2\varkappa^{(g_1,\ldots,g_m),(j)}(h) - n_1\ldots n_r\Big). \tag{18}$$

Положив $h = g_1h_1+\ldots+g_mh_m$ и подставив выражение (18) с таким h в (12), получим:

$$2^m\varkappa(h_1,\ldots,h_m) = n_1\ldots n_r +$$

$$+ \sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\backslash\{\mathbf{0}\}} 1\cdot\Big(2\varkappa^{(g_1,\ldots,g_m)}(g_1h_1+\ldots+g_mh_m) - n_1\ldots n_r\Big) =$$

$$= n_1\ldots n_r + 2\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\backslash\{\mathbf{0}\}} \varkappa^{(g_1,\ldots,g_m)}(g_1h_1+\ldots+g_mh_m) -$$

$$-(2^m-1)n_1\ldots n_r =$$

$$= 2\sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\backslash\{\mathbf{0}\}} \varkappa^{(g_1,\ldots,g_m)}(h_1,\ldots,h_m) - (2^m-2)n_1\ldots n_r.$$

Из последней формулы получаем (4). Теорема 1 доказана.

4. Доказательство теоремы 2

Нам понадобится следующее утверждение.

Лемма 2. *При $n_j \to \infty$ вектор*

$$n_j^{-1/2}\left(D^{(j)}_{g_1,\ldots,g_m}, (g_1,\ldots,g_m) \in \mathbb{G}_m\backslash\{\mathbf{0}\}\right)$$

имеет в пределе (2^m-1)-мерное нормальное распределение с нулевым вектором средних и единичной ковариационной матрицей.

Доказательство (леммы 2). Согласно формуле (17)

$$D^{(j)}_{g_1,\ldots,g_m} = \sum_{t=0}^{n_j-1} (-1)^{g_1 X_t^{1,(j)}+\ldots+g_m X_t^{m,(j)}}.$$

В силу независимости и равномерности распределений на $\mathbb{Z}_2$ величин $X_t^{1,(j)},\ldots,X_t^{m,(j)}$ выполнено равенство

$$\mathbf{E}(-1)^{g_1 X_t^{1,(j)}+\ldots+g_m X_t^{m,(j)}} = 0, \quad (g_1,\ldots,g_m) \neq 0.$$

Кроме того, ясно, что $\mathbf{D}(-1)^{g_1 X_t^{1,(j)}+\ldots+g_m X_t^{m,(j)}} = 1$.

Теперь покажем, что

$$\operatorname{cov}\left((-1)^{g_1 X_t^{1,(j)}+\ldots+g_m X_t^{m,(j)}}, (-1)^{h_1 X_t^{1,(j)}+\ldots+h_m X_t^{m,(j)}}\right) = 0$$

при $(g_1,\ldots,g_m) \neq (h_1,\ldots,h_m)$. Для этого достаточно убедиться, что случайные величины $g_1 X_t^{1,(j)}+\ldots+g_m X_t^{m,(j)} \bmod 2$ и $h_1 X_t^{1,(j)}+\ldots+h_m X_t^{m,(j)} \bmod 2$ независимы.

Воспользуемся тем свойством равномерного распределения на $\mathbb{Z}_2$, что случайные величины $g_1 X_t^{1,(j)} + \ldots + g_m X_t^{m,(j)} \bmod 2$ и $h_1 X_t^{1,(j)} + \ldots + h_m X_t^{m,(j)} \bmod 2$ имеют равномерное распределение и независимы, если $(g_1,\ldots,g_m) \neq (h_1,\ldots,h_m)$, $(g_1,\ldots,g_m),(h_1,\ldots,h_m) \neq 0$. Поэтому случайный вектор

$$\left((-1)^{g_1 X_t^{1,(j)}+\ldots+g_m X_t^{m,(j)}},\ (g_1,\ldots,g_m) \in \mathbb{G}_m\backslash\{\mathbf{0}\}\right)$$

имеет нулевой вектор средних и единичную ковариационную матрицу.

При $t = 0,\ldots,n_j-1$ эти векторы независимы в совокупности, и по многомерной центральной предельной теореме (см., например, [10], с. 420) распределение их нормированной множителем $n_j^{-1/2}$ суммы сходится при $n_j \to \infty$ к (2^m-1)-мерному нормальному распределению с нулевым вектором средних и единичной ковариационной матрицей. Лемма 2 доказана.

Из независимости заполнений регистров, формулы (13) и леммы 2 вытекает, что при $n_1,\ldots,n_r \to \infty$ случайные величины

$$\frac{D_{g_1,\ldots,g_m}}{\sqrt{n_1\ldots n_r}}, \quad (g_1,\ldots,g_m) \in \mathbb{G}_m\backslash\{\mathbf{0}\},$$

асимптотически независимы и каждая из них имеет в пределе распределение Φ_r. Осталось воспользоваться формулой

$$\tilde{\varkappa}(h_1, \ldots, h_m) = \sum_{(g_1,\ldots,g_m)\in\mathbb{G}_m\setminus\{\mathbf{0}\}} (-1)^{g_1h_1+\ldots+g_mh_m} \frac{D_{g_1,\ldots,g_m}}{\sqrt{n_1\ldots n_r}},$$

вытекающей из (12). Теорема 2 доказана.

Авторы благодарны А. М. Зубкову за полезные замечания.

Список литературы

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, 1973, 36 pp.
2. Pohl P., “Description of MCV, a pseudo–random number generator”, *Scand. Actuarial J.*, **1** (1976), 1–14.
3. Меженная Н. М., Михайлов В. Г., “О распределении числа единиц в выходной последовательности генератора Пола над полем $GF(2)$”, *Математические вопросы криптографии*, **4**:4 (2013), 95—107.
4. Mezhennaya N. M., “Convergence rate estimators for the number of ones in outcome sequence of MCV generator with m-dependent registers items”, *Siberian Electronic Mathematical Reports*, **11** (2014), 18–25.
5. Меженная Н. М., “О распределении числа единиц в двоичной мультициклической последовательности”, *Прикл. дискр. матем.*, 2015, №1(27), 69–77.
6. Меженная Н. М., Михайлов В. Г., “О числе появлений знаков в мультициклической случайной последовательности по модулю 4”, *Дискретная математика*, **26**:4 (2014), 51–58; англ. пер.: Mezhennaya N. M., Mikhailov V. G., “On frequencies of elements in multicyclic random sequence modulo 4”, *Discrete Math. Appl.*, **25**:6 (2015), 359–365.
7. Меженная Н. М., Михайлов В. Г., “Об асимптотической нормальности чисел появлений знаков в неравновероятной мультициклической случайной последовательности по модулю 4”, *Математические вопросы криптографии*, **7**:4 (2016), 81-94.
8. Хассе Г., *Лекции по теории чисел*, М.: Наука, 1953, 533 с.; пер. с нем.: Hasse H., *Vorlesungen über Zahlentheorie*, Berlin, 1950.
9. Севастьянов Б. А.“Условное распределение выхода автоматов без памяти при заданных характеристиках входа”, *Дискретная математика*, **6**: 1 (1994), 34—39; англ. пер.: Sevastyanov B. A., “The conditional distribution of the output of an automaton without memory for given characteristics of the input”, *Discrete Math. Appl.*, **4**:1 (1994), 1–6.
10. Ширяев А. Н., *Вероятность – I*, 3-е изд., МЦНМО, М., 2004, 520 с.; англ. пер.: Shiryaev A. N., *Probability*-1, Springer-Verlag, New York, 2016, 486 pp.

Статья поступила 16.05.2017.
Переработанный вариант поступил 04.07.2017.