S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 16, стр. 229–235 (2019) УДК 519.213, 519.214
DOI 10.33048/semi.2019.16.014 MSC 60F05, 94B12, 14G50

О ЧИСЛЕ ЕДИНИЦ В ЦИКЛЕ МУЛЬТИЦИКЛИЧЕСКОЙ ПОСЛЕДОВАТЕЛЬНОСТИ, ОПРЕДЕЛЯЕМОЙ БУЛЕВОЙ ФУНКЦИЕЙ

Н.М. МЕЖЕННАЯ, В.Г. МИХАЙЛОВ

Abstract. The paper presents formulas that denote the relationship between the number of ones in the cycle of a multicyclic sequence modulo 2, defined by the Boolean function, and the number of ones in the registers of the generator through the spectral characteristics of this function. Using these formulas, we prove normal-type limit theorems for the number of ones in the cycle of the multicyclic sequence if the registers are filled with independent binary random variables with the same distributions within each register, the lengths of the registers tend to infinity and their number remains fixed. We prove that the limit distribution can be both the usual normal distribution and the distribution of the product of independent standard normal random variables.

Keywords: number of ones, multicyclic sequence, Boolean function, central limit theorem.

1. Введение

Пусть имеется r циклических регистров сдвига взаимно простых длин $m_1, \dots, m_r$ над кольцом вычетов по модулю 2. Обозначим через $(x_0^{(j)}, \dots, x_{m_j-1}^{(j)})$, $j = 1, \dots, r$, векторы заполнений ячеек регистров, $t(m) = t \bmod m$. Мультициклический генератор, определяемый булевой функцией $f(y_1, \dots, y_r)$, строит выходную последовательность по правилу

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

Mezhennaya, N.M., Mikhailov, V.G., On the number of ones in the cycle of multicyclic sequence determined by Boolean function.

Поступила 4 июля 2018 г., опубликована 21 февраля 2019 г.

где $f(y_1,\dots,y_r)$ существенным образом зависит от всех своих аргументов $y_1,\dots,y_r$. При $f(y_1,\dots,y_r)=y_1\oplus\ldots\oplus y_r$ (здесь и далее $\oplus$ — операция сложения по модулю 2) обобщенный генератор Пола совпадает с обычным генератором Пола (см. [1]). Использование свойств таких последовательностей в криптографических задачах хорошо известно [2].

Выходная последовательность (1) является чисто периодической и имеет период (возможно, не минимальный) длины $L=m_1m_2\dots m_r$. В настоящей работе изучим свойства случайной величины ξ — числа единиц в отрезке $(z_0,\dots,z_{L-1})$, называемом *циклом* выходной последовательности.

Для двоичного генератора Пола был получен широкий спектр предельных теорем для числа единиц в цикле выходной последовательности при разных предположениях о распределении знаков в регистрах, когда $m_1,\dots,m_r\to\infty$, а число регистров r остается фиксированным или также стремится к бесконечности. Для доказательства была использована полученная в [3] формула, связывающая число единиц на цикле выходной последовательности с числами единиц в заполнениях регистров генератора (см. теорему 1 ниже). В [3] и [4] были рассмотрены мультициклические генераторы с регистрами, заполненными знаками независимых в совокупности равновероятных и неравновероятных бернуллиевских последовательностей соответственно. Аналогичная формула для обобщенного мультициклического генератора была приведена в [5]. В настоящей работе с помощью этой формулы будут получены аналогичные результаты для числа единиц в цикле последовательности (1).

2. Формулы для числа единиц

Будем использовать обозначения:

1) $|A|$ для числа элементов множества A;

2) $W_f(z)$ для коэффициента Уолша–Адамара функции f (см. [6, с. 77]):

$$W_f(z)=\sum_{u\in\{0,1\}^r}(-1)^{f(u)+z_1u_1+\ldots+z_ru_r}; \tag{2}$$

3) $\mathbf{1}_{(j_1,\dots,j_k)}\in\{0,1\}^r$ для двоичного вектора, в котором единицы стоят на местах с номерами $\{j_1,\dots,j_k\}$, $1\le k\le r$, а остальные знаки — нули;

4) $\mathrm{wt}(f)$ для веса функции f (см. [6, с. 75]);

5) $U(f)=\bigl\{u=(u_1,\dots,u_r)\in\{0,1\}^r:\ f(u_1,\dots,u_r)=1\bigr\}$.

Ясно, что $\mathrm{wt}(f)=|U(f)|$.

Пусть s_j — количество единиц в заполнении j-го регистра $(x_0^{(j)},\dots,x_{m_j-1}^{(j)})$, $j=1,\dots,r$.

Следующее утверждение связывает число единиц ξ в выходной последовательности мультициклического генератора (1) с числами единиц $s_1,\dots,s_r$ в его регистрах.

Лемма 1. *Пусть мультициклический генератор вида* (1) *с регистрами длин* $m_1,\dots,m_r$ *задается булевой функцией* $f(y_1,\dots,y_r)$. *Тогда*

$$\frac{2^r\xi}{m_1\dots m_r}=\mathrm{wt}(f)-\frac12\sum_{k=1}^{r}\sum_{1\le j_1<\ldots<j_k\le r}W_f(\mathbf{1}_{(j_1,\dots,j_k)})\prod_{l=1}^{k}\left(\frac{m_{j_l}-2s_{j_l}}{m_{j_l}}\right). \tag{3}$$

Доказательство. Любая булева функция $f(y_1,\dots,y_r)$ может быть записана в виде суммы

$$f(y_1,\dots,y_r)=\sum_{u\in U(f)}\prod_{j=1}^{r}y_j^{u_j}\left(1-y_j\right)^{1-u_j}, \tag{4}$$

в которой только одно слагаемое равно единице при каждом значении набора переменных $(y_1,\dots,y_r)$.

Пусть $u=(u_1,\dots,u_r)\in U(f)$. Тогда

$$\{z_t=1\}=\bigcup_{u\in U(f)}\{x_{t(m_1)}=u_1,\dots,x_{t(m_r)}=u_r\}.$$

Следовательно, число единиц ξ в цикле последовательности (1) равно

$$\xi=\sum_{t=0}^{L-1}z_t=\sum_{u\in U(f)}\prod_{j=1}^{r}\left(s_j^{u_j}(m_j-s_j)^{1-u_j}\right).$$

Выделяя в каждой скобке в правой части последней формулы выражение m_j-2s_j, получаем

$$\xi=\sum_{u\in U(f)}\prod_{j=1}^{r}\left(m_j+(-1)^{u_j}(m_j-2s_j)\right)$$

$$=\frac{m_1\dots m_r}{2^r}\sum_{u\in U(f)}\prod_{j=1}^{r}\left(1+(-1)^{u_j}\frac{m_j-2s_j}{m_j}\right). \tag{5}$$

Согласно (5) для любой булевой функции f

$$\frac{2^r\xi}{m_1\dots m_r}=\sum_{u=(u_1,\dots,u_r)\in U(f)}\prod_{j=1}^{r}\left(1+(-1)^{u_j}\frac{m_j-2s_j}{m_j}\right)$$

$$=|U(f)|+\sum_{k=1}^{r}\sum_{1\le j_1<\dots<j_k\le r}W(j_1,\dots,j_k)\prod_{l=1}^{k}\left(\frac{m_{j_l}-2s_{j_l}}{m_{j_l}}\right), \tag{6}$$

где

$$W(j_1,\dots,j_k)=\sum_{u\in U(f)}(-1)^{u_{j_1}+\dots+u_{j_k}},\quad k=1,\dots,r.$$

Так как для индикатора события $\{f(u)=1\}$ выполнена формула

$$I\{f(u)=1\}=\frac{1-(-1)^{f(u)}}{2},\quad \text{а}\quad \sum_{u\in\{0,1\}^r}(-1)^{u_{j_1}+\dots+u_{j_k}}=0,\quad k=1,\dots,r,$$

то

$$W(j_1,\dots,j_k)=-\frac{1}{2}\sum_{u\in\{0,1\}^r}(-1)^{f(u)+u_{j_1}+\dots+u_{j_k}}=-\frac{1}{2}W_f(\mathbf{1}_{(j_1,\dots,j_k)}). \tag{7}$$

Подставив (7) в (6), получим (3). □

Замечание. Формула для частот знаков в выходной последовательности комбинирующего генератора (см. [7]), аналогичная (5), получена в [8] (см. также [9]).

3. Предельные теоремы

Обозначим

$$b_j = \sqrt{p_j(1-p_j)}\Big(W_f(\mathbf{1}_{(j)}) + \sum_{k=1}^{r-1} \sum_{\substack{1\le j_1<\ldots<j_k\le r,\\ j_1,\ldots,j_k\ne j}} W_f(\mathbf{1}_{(j,j_1,\ldots,j_k)}) \prod_{l=1}^{k}(1-2p_{j_l})\Big),$$

$$C^2 = \sum_{j=1}^{r} \frac{b_j^2}{m_j},$$

$$A = \mathrm{wt}(f) - \frac{1}{2}\sum_{k=1}^{r} \sum_{1\le j_1<\ldots<j_k\le r} W_f(\mathbf{1}_{(j_1,\ldots,j_k)}) \prod_{l=1}^{k}(1-2p_{j_l}). \tag{8}$$

Теорема 1. *Пусть мультициклический генератор вида* (1) *с* $r \ge 2$ *регистрами длин* $m_1 < \ldots < m_r$ *задается булевой функцией* $f(y_1,\ldots,y_r)$, *заполнения* $x_k^{(j)}$ *ячеек регистров случайны, независимы в совокупности и*

$$\mathbf{P}\{x_k^{(j)} = 1\} = 1 - \mathbf{P}\{x_k^{(j)} = 0\} = p_j \in (0;1),$$

при $k = 0,\ldots,m_j-1$, $j = 1,\ldots,r$, *и* $b_1^2 > 0$. *Если* $m_1,\ldots,m_r \to \infty$ *и все остальные параметры схемы остаются фиксированными, то закон распределения случайной величины*

$$\frac{1}{C}\left(\frac{2^r\xi}{m_1\ldots m_r} - A\right)$$

сходится к стандартному нормальному закону.

Доказательство. В условиях теоремы величины s_j, $j = 1,\ldots,r$, случайны, независимы в совокупности и имеют биномиальные распределения с параметрами (m_j, p_j) соответственно. Поэтому случайные величины

$$\tilde{s}_j = \frac{m_j p_j - s_j}{\sqrt{m_j p_j(1-p_j)}}, \quad j = 1,\ldots,r, \tag{9}$$

имеют нулевые средние и единичные дисперсии. Эти величины независимы в совокупности и при $m_1,\ldots,m_r \to \infty$ имеют в качестве предельного стандартный нормальный закон. Представим выражение $\frac{m_j-2s_j}{m_j}$ в виде

$$\frac{m_j - 2s_j}{m_j} = (1-2p_j) + 2\tilde{s}_j\frac{\sqrt{p_j(1-p_j)}}{\sqrt{m_j}}.$$

Тогда из (3) вытекает

$$\frac{2^r\xi}{m_1\ldots m_r} - \mathrm{wt}(f) = -\frac{1}{2}\sum_{k=1}^{r} \sum_{1\le j_1<\ldots<j_k\le r} W_f(\mathbf{1}_{(j_1,\ldots,j_k)}) \times \prod_{l=1}^{k}\left((1-2p_{j_l}) + 2\tilde{s}_{j_l}\frac{\sqrt{p_{j_l}(1-p_{j_l})}}{\sqrt{m_{j_l}}}\right). \tag{10}$$

Преобразуем правую часть (10), раскрыв скобки в произведении. Также перегруппируем слагаемые, чтобы выделить свободный член и коэффициенты при произведениях $\prod_{l=1}^{k} \tilde{s}_{j_l}$. В результате получим следующее равенство:

$$\frac{2^r\xi}{m_1\dots m_r} - \operatorname{wt}(f) + \frac{1}{2}\sum_{k=1}^{r}\sum_{1\le j_1<\dots<j_k\le r} W_f(\mathbf{1}_{(j_1,\dots,j_k)})\prod_{l=1}^{k}(1-2p_{j_l})$$
$$= -\sum_{j=1}^{r}\tilde{s}_j\frac{\sqrt{p_j(1-p_j)}}{\sqrt{m_j}}\Big(W_f(\mathbf{1}_{(j)})$$

$$+\sum_{k=1}^{r-1}\sum_{\substack{1\le j_1<\dots<j_k\le r,\\ j_1,\dots,j_k\ne j}} W_f(\mathbf{1}_{(j,j_1,\dots,j_k)})\prod_{l=1}^{k}(1-2p_{j_l})\Big) + O(m_1^{-1}) \tag{11}$$

(здесь и далее записи вида $\zeta_1 = o(t)$ и $\zeta_2 = O(t)$ означают, что при $t\to\infty$ величина $\zeta_1 t^{-1}$ стремится по вероятности к нулю, а величина $\zeta_2 t^{-1}$ ограничена по вероятности). В наших обозначениях равенство (11) перепишется в виде

$$\frac{2^r\xi}{m_1\dots m_r} - A = -\sum_{j=1}^{r}\frac{b_j}{\sqrt{m_j}}\tilde{s}_j + O(m_1^{-1}).$$

Их условия $b_1^2 > 0$ следует, что $C^{-1} = O(m_1^{1/2})$. Поэтому предельные законы распределения случайных величин

$$\frac{1}{C}\left(\frac{2^r\xi}{m_1\dots m_r} - A\right) \quad \text{и} \quad \frac{1}{C}\sum_{j=1}^{r}\frac{b_j}{\sqrt{m_j}}\tilde{s}_j,$$

если они существуют, совпадают. Минус перед вторым выражением опущен, так как предельные распределения случайных величин $\tilde{s}_j$ и $-\tilde{s}_j$ одинаковы.

Из того, что законы распределения независимых случайных величин $\tilde{s}_j$ сходятся к стандартному нормальному, вытекает, что совпадают предельные законы распределения случайных величин

$$\frac{1}{C}\sum_{j=1}^{r}\frac{b_j}{\sqrt{m_j}}\tilde{s}_j \quad \text{и} \quad \frac{1}{C}\sum_{j=1}^{r}\frac{b_j}{\sqrt{m_j}}\eta_j,$$

где $\eta_1,\dots,\eta_r$ — независимые случайные величины со стандартным нормальным распределением. Используя определение C^2 и формулу для дисперсии суммы независимых случайных слагаемых, получаем, что

$$\mathbf{D}\left(\frac{1}{C}\sum_{j=1}^{r}\frac{b_j}{\sqrt{m_j}}\tilde{s}_j\right) = 1.$$

□

Замечание. Аналогичный результат для случая $p_j = 1/2$, $j = 1,\dots,r$, был получен в работе [10].

Теорему 1 можно обобщить. Обозначим

$$b_{j_1,\dots,j_k} = \left(\prod_{j=1}^{k}\sqrt{p_j(1-p_j)}\right)\Big(W_f(\mathbf{1}_{(j_1,\dots,j_k)}) + \sum_{u=1}^{r-k}\sum_{\substack{1\le i_1<\dots<i_u\le r,\\ |\{i_1,\dots,i_u,j_1,\dots,j_k\}|=k+u}} W_f(\mathbf{1}_{(j_1,\dots,j_k,i_1,\dots,i_u)})\prod_{l=1}^{u}(1-2p_{i_l})\Big),$$

$$B_k^2 = \sum_{1\le j_1<\dots<j_k\le r} b_{j_1,\dots,j_k}^2.$$

Теорема 2. *Пусть обобщенный генератор Пола с $r \ge 2$ регистрами длин $m_1 < \dots < m_r$ задается булевой функцией $f(y_1,\dots,y_r)$, заполнения $x_k^{(j)}$ ячеек регистров случайны, независимы в совокупности и*

$$\mathbf{P}\{x_k^{(j)} = 1\} = 1 - \mathbf{P}\{x_k^{(j)} = 0\} = p_j \in (0,1),$$

при $k = 0,\dots,m_j-1$, $j = 1,\dots,r$, и существует число $1 \le v \le r$, для которого $B_k^2 = 0$ при $k < v$ и $B_v^2 > 0$. Если $m_1,\dots,m_r \to \infty$, так что $m_1/m_j \to \rho_j^2 \in (0;1]$, а все остальные параметры схемы остаются фиксированными, то закон распределения случайной величины

$$\sqrt{m_1\dots m_v}\left(\frac{2^r\xi}{m_1\dots m_r} - A\right),$$

где параметр A определен формулой (8), сходится к закону распределения невырожденной формы

$$\sum_{1\le j_1<\dots<j_v\le r}\frac{\rho_{j_1}\dots\rho_{j_v}}{\rho_1\dots\rho_l}b_{j_1,\dots,j_v}\eta_{j_1}\dots\eta_{j_v}$$

от произведения независимых в совокупности стандартных нормальных случайных величин $\eta_1,\dots,\eta_r$.

Доказательство. Доказательство теоремы 2 аналогично доказательству теоремы 1. В условиях теоремы 2 в формуле (10) слагаемые, соответствующие коэффициентам $b_{j_1,\dots,j_k}$ при $k < v$ равны нулю, поэтому

$$\frac{2^r\xi}{m_1\dots m_r} - A = -\sum_{k=v}^{r}\sum_{1\le j_1<\dots<j_k\le r}\frac{b_{j_1,\dots,j_k}}{\sqrt{m_{j_1}\dots m_{j_k}}}\tilde{s}_{j_1}\dots\tilde{s}_{j_k}.$$

Выделим главный член выражения в правой части последнего равенства. Получаем

$$\frac{2^r\xi}{m_1\dots m_r} - A = -\sum_{1\le j_1<\dots<j_v\le r}\frac{b_{j_1,\dots,j_v}}{\sqrt{m_{j_1}\dots m_{j_v}}}\tilde{s}_{j_1}\dots\tilde{s}_{j_v} + O(m_1^{-(v+1)/2}). \tag{12}$$

Тогда функция распределения случайной величины

$$\sqrt{m_1\dots m_v}\left(\frac{2^r\xi}{m_1\dots m_r} - A\right)$$

имеет тот же предел, что и функция распределения суммы

$$\sqrt{m_1\dots m_v}\sum_{1\le j_1<\dots<j_v\le r}\frac{b_{j_1,\dots,j_v}}{\sqrt{m_{j_1}\dots m_{j_v}}}\tilde{s}_{j_1}\dots\tilde{s}_{j_v}$$

$$= \sum_{1\le j_1<\ldots<j_v\le r} b_{j_1,\ldots,j_v} \prod_{l=1}^{v} \left(\sqrt{\frac{m_{j_l}}{m_l}}\, \tilde{s}_{j_l} \right).$$

Здесь минус перед суммой снова не ставим в силу симметричности распределения каждого отдельного слагаемого в ней.

Так как при любых $1 \le j_1 < \ldots < j_v \le r$ закон распределения произведения $\tilde{s}_{j_1} \ldots \tilde{s}_{j_v}$ сходится при $m_1, \ldots, m_r \to \infty$ к закону распределения произведения $\eta_{j_1} \ldots \eta_{j_v}$ и

$$\sqrt{\frac{m_{j_l}}{m_l}} \to \frac{\rho_{j_l}}{\rho_l}, \quad m_1, \ldots, m_r \to \infty,$$

то из формулы (12) и перечисленных свойств получаем утверждение теоремы 2. □

Авторы благодарны рецензентам за полезные замечания и внимание к работе.

References

[1] P. Pohl, *Description of MCV, a pseudo-random number generator*, Scand. Actuar. J., **1** (1976), 1–14. MR0474695

[2] G.P. Agibalov, *Finite automata in cryptography*, Prikl. Diskr. Mat. Suppl., **2** (2009), 43–73. (in Russian).

[3] N.M. Mezhennaya, V.G. Mikhailov, *On the distribution of the number of ones in the output sequence of the MCV-generator over $GF(2)$*, Mat. Vopr. Kriptogr., **4**:4 (2013), 95–107. (in Russian).

[4] N.M. Mezhennaya, *On distribution of number of ones in binary multicycle sequence*, Prikl. Diskr. Mat., **1(27)** (2015), 69–77. (in Russian).

[5] N.M. Mezhennaya, V.G. Mikhailov, *On the number of ones in the output sequence of a multicyclic generator determined by Boolean function*, in: Proc. of the X International Conference "Discrete Models in Control Systems Theory", Moscow and Moscow region (2018), 195–198. (in Russian).

[6] O.A. Logachev, A.A. Sal'nikov, S.V. Smyshlyaev, V.V. Yashchenko, *Boolean functions in coding theory and cryptology*, MCCME, Moscow, 2012. (in Russian).

[7] *Glossary of cryptographic terms*, B.A. Pogorelov, V.N. Sachkov (eds.), MCCME, Moscow, 2006. (in Russian).

[8] I.B. Bilyak, O.V. Kamlovskii, *Frequency characteristics of cycles in output sequences generated by combining generators over the field of two elements*, Prikl. Diskr. Mat., **3(29)** (2015), 17–31. (in Russian).

[9] O.V. Kamlovskii, *Occurrence numbers for vectors in cycles of output sequences of binary combining generators*, Probl. Inf. Trans., **53**:1 (2017), 84–91. MR3661762

[10] N.M. Mezhennaya, V.G. Mikhailov, *On the number of ones in outcome sequence of extended Pohl generator* Discrete Math. Appl., **31** (2019). (in Russian).

Natalia Mikhailovna Mezhennaya
Bauman Moscow State Technical University,
5, 2-aya Baumanskaya st.,
Moscow, 105005, Russia
E-mail address: natalia.mezhennaya@gmail.com

Vladimir Gavrilovich Mikhailov
Steklov Mathematical Institute of Russian Academy of Sciences,
8, Gubkina st.,
Moscow, 119991, Russia
E-mail address: mikh_vg@mail.ru