International Journal of Applied Mathematics

Volume 32 No. 5 2019, 835-845
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v32i5.10

ON THE NUMBER OF 1'S PER CYCLE OF A BINARY RANDOM MULTICYCLIC SEQUENCE

Natalia M. Mezhennaya[1] [§], Vladimir G. Mikhailov[2]

[1] Applied Mathematics Department
Bauman Moscow State Technical University
ul. Baumanskaya 2-ya, 5/1
Moscow - 105005, RUSSIA

[2] Discrete Mathematics Department
Steklov Mathematical Institute
of Russian Academy of Sciences
ul. Gubkina, 8
Moscow - 119991, RUSSIA

Abstract: A binary random multicyclic sequence is determined by a Boolean function of r variables and r independent binary random cyclic sequences with period lengths $m_1, \dots, m_r$. We obtain the limit distribution of the number of 1's per cycle of a multicyclic sequence in the case when the numbers $m_1, \dots, m_r \to \infty$ and the number of 1's for each sequence has its own limit distribution.

AMS Subject Classification: 60F05, 94B12, 14G50
Key Words: number of 1's, multicyclic sequence, Boolean function, limit theorem

1. Introduction

Let there be r binary vectors $\mathbf{x}_j = (x_0^{(j)}, \dots, x_{m_j-1}^{(j)})$, $j = 1, \dots, r$, of mutually prime lengths $m_1, \dots, m_r$. Each vector $\mathbf{x}_j$ represents a cyclic sequence of values used as arguments of the Boolean function $f(y_1, \dots, y_r)$, $j = 1, \dots, r$. The multicyclic sequence determined by the Boolean function f is constructed by

Received: September 19, 2019

[§] Correspondence author

the rule

$$z_t = f\bigl(x^{(1)}_{t(m_1)}, \ldots, x^{(r)}_{t(m_r)}\bigr), \qquad (1)$$

where $t(m) = t \bmod m$. We assume that the function $f(y_1, \ldots, y_r)$ essentially depends on all its arguments $y_1, \ldots, y_r$.

If the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are output sequences of some random generators (see, e.g., [1, 2, 3]) and we consider them to be the content of shift registers, then the multicyclic sequence of the form (1) describes the output sequence of a combining generator [1, 2]. A simple example of such a generator is the Pohl generator for which $f(y_1, \ldots, y_r) = y_1 \oplus \ldots \oplus y_r$ (hereinafter, $\oplus$ denotes the addition operation modulo 2) (see [4]).

The multicyclic sequence (1) is purely periodical with a period (possibly, not minimal) of length $L = m_1 m_2 \ldots m_r$.

The number of 1's per cycle (any segment of length L of the sequence (1)) is equal to

$$\xi = \sum_{t=0}^{m_1 \ldots m_r - 1} z_t.$$

This variable is uniquely determined by the number of 1's in the cells of generator registers. Such a formula for Pohl generator ($f(y_1, \ldots, y_r) = y_1 \oplus \ldots \oplus y_r$) was derived by Mezhennaya and Mikhailov [5]. In the general case (for arbitrary f), the corresponding formula was obtained by Mezhennaya and Mikhailov [6, 7]. Bilyak and Kamlovskii [1, 2] got a similar result for the output sequence of the combining generator.

Some results on periodicity properties of the output sequence of the combining generator are contained in [3]. The properties of the letter frequencies in the sequences produced by filtering generators which have relatively similar properties and applications in coding theory are studied by Kamlovskii [8], Dai, Feng, Liu, and Wan [9, 10], and Niederreiter [11].

Well-known results describe (see, for example, [12]) the linear complexity of linear recurrent sequences, which can be assumed as register content. The properties of binary-exponent alternating sums [13] are required to study the probabilistic characteristics of sequence (1). The problem of the frequency characteristics of linear recurrent sequences, random number generators, and, in particular, sequences constructed according to rule (1), turned out to be less studied.

Mezhennaya and Mikhailov in [5] obtained a wide spectra of limit theorems for the number ξ of 1's per cycle of the output sequence of the Pohl generator, when $m_1, \ldots, m_r \to \infty$ and the number of registers r remains fixed or tends to infinity, and the registers contain mutually independent equiprobably distributed random variables. The Pohl generators with registers containing mutually independent segments of non-equiprobable Bernoulli sequences were considered in [14].

The distribution of the number of 1's in a random multicyclic sequence determined by a Boolean function (of arbitrary form) with mutually independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ with uniformly distributed on $\{0, 1\}$ and possibly dependent letters was considered by Mezhennaya and Mikhailov in [6]. The paper [7] was devoted to a similar problem for the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ with independent components that have an arbitrary distribution on $\{0, 1\}$.

The present research completes and summarizes a series of research papers by the authors. We obtain a generalization of the results for the number ξ of 1's in the cycle of the sequence (1) based on only the assumption that the numbers of 1's in each of the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ (with proper normalization) have their own limit distributions, and the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are mutually independent. Previously, assumptions about the asymptotic normality of the number of 1's in the generator registers [5, 7, 14] or, moreover, assumptions on the independence and identical distribution of letters in the cells of generator registers [5, 14] were used.

In the future, it is also interesting to obtain limit distributions for the numbers of tuples and runs with a given structure in a sequence of the form (1) (see, e.g., [15, 16, 17, 18, 19]).

2. Limit theorem

We denote the numbers of 1's in the vectors $\mathbf{x}_j = (x_0^{(j)}, \ldots, x_{m_j-1}^{(j)})$ by s_j, $j = 1, \ldots, r$, and suppose that the joint distribution of the binary vectors $\mathbf{x}_j$, $j = 1, \ldots, r$, and the Boolean function f satisfy the following conditions.

Condition 1. Let the binary vectors $\mathbf{x}_j = (x_0^{(j)}, \ldots, x_{m_j-1}^{(j)})$, $j = 1, \ldots, r$, be random and mutually independent, and let there be the numbers $a_1, \ldots, a_r$ and $b_1, \ldots, b_r > 0$ such that the random variable $\tilde{s}_j = b_j^{-1}(a_j - 2s_j)$ converges in distribution for $m_j \to \infty$ to some proper random variable η_j, $j = 1, \ldots, r$.

Condition 2. Let for $m_1, \ldots, m_r \to \infty$ the numbers $a_1, \ldots, a_r, b_1, \ldots, b_r$ vary so that

$$\frac{m_j - a_j}{m_j} \to \alpha_j \in [-1; 1], \quad \frac{b_j}{m_j} \to 0, \quad \frac{m_1 b_j}{m_j b_1} \to \rho_j \in (0; 1]. \qquad (2)$$

Let

$$\beta_{j_1,\dots,j_k} = -\frac{1}{2}\frac{\rho_{j_1}\dots\rho_{j_k}}{\rho_1\dots\rho_k}\Bigg(W_f(\mathbf{1}_{(j_1,\dots,j_k)})$$

$$+\sum_{u=1}^{r-k}\sum_{\substack{1\le i_1<\dots<i_u\le r,\\ |\{j_1,\dots,j_k,i_1,\dots,i_u\}|=k+u}} W_f(\mathbf{1}_{(j_1,\dots,j_k,i_1,\dots,i_u)})\prod_{l=1}^{u}\alpha_{i_l}\Bigg), \tag{3}$$

$$B_k^2 = \sum_{1\le j_1<\dots<j_k\le r}\beta^2_{j_1,\dots,j_k}, \tag{4}$$

$$A = \frac{1}{2}\sum_{k=1}^{r}\sum_{1\le j_1<\dots<j_k\le r} W_f(\mathbf{1}_{(j_1,\dots,j_k)})\prod_{l=1}^{k}\left(\frac{m_{j_l}-a_{j_l}}{m_{j_l}}\right) - \mathrm{wt}(f), \tag{5}$$

where $W_f(z)$ is a Walsh–Hadamard coefficient of the function f (see [21, p. 59]):

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

$\mathbf{1}_{(j_1,\dots,j_k)}\in\{0,1\}^r$ is a binary vector in which the components with the numbers $\{j_1,\dots,j_k\}$, $1\le k\le r$, are 1's, and the remaining components are 0's, $\mathrm{wt}(f)$ is the weight of the function f (see [21, p. 59]), and $|A|$ is the cardinality of the set A. We assume that the sum over the empty set is 0.

Condition 3. A number $q: 1\le q\le r$ exists such that

$$B_k^2 = 0,\quad k=1,\dots,q-1,\quad B_q^2>0.$$

Theorem 1. *Under Conditions* $1-3$ *the random variable*

$$\tilde{\xi} = \frac{m_1\dots m_q}{b_1\dots b_q}\left(\frac{2^r\xi}{m_1\dots m_r}+A\right)$$

converges in distribution to the random variable

$$V_q = \sum_{1\le j_1<\dots<j_q\le r}\beta_{j_1,\dots,j_q}\eta_{j_1}\dots\eta_{j_q}.$$

Remark 1. Theorems 2 and 3 of [6] and Theorem 1 of [7] are special cases of Theorem 1.

3. Proof of Theorem 1

We cite the formula from the paper [7, Lemma 1, formula (3)] which establishes a linkage between the number ξ of 1's per cycle of the sequence (1) and the numbers $s_1, \dots, s_r$ of 1's in the vectors $\mathbf{x}_1, \dots, \mathbf{x}_r$:

$$\frac{2^r \xi}{m_1 \dots m_r} = \mathrm{wt}(f)$$
$$-\frac{1}{2} \sum_{k=1}^{r} \sum_{1 \le j_1 < \dots < j_k \le r} W_f(\mathbf{1}_{(j_1, \dots, j_k)}) \prod_{l=1}^{k} \left(\frac{m_{j_l} - 2s_{j_l}}{m_{j_l}} \right). \tag{6}$$

Since

$$\frac{m_j - 2s_j}{m_j} = \frac{m_j - a_j}{m_j} + \frac{\tilde{s}_j b_j}{m_j},$$

then it follows from (6) that

$$\frac{2^r \xi}{m_1 \dots m_r} - \mathrm{wt}(f) = -\frac{1}{2} \sum_{k=1}^{r} \sum_{1 \le j_1 < \dots < j_k \le r} W_f(\mathbf{1}_{(j_1, \dots, j_k)})$$
$$\times \prod_{l=1}^{k} \left(\frac{m_{j_l} - a_{j_l}}{m_{j_l}} + \frac{\tilde{s}_{j_l} b_{j_l}}{m_{j_l}} \right). \tag{7}$$

We expand the brackets and rearrange the terms in the right-hand side of (7) to select the free term and the coefficients for $\tilde{s}_{j_1} \dots \tilde{s}_{j_k}$. We start with the free term. Obviously, it is equal to the following:

$$-\frac{1}{2} \sum_{k=1}^{r} \sum_{1 \le j_1 < \dots < j_k \le r} W_f(\mathbf{1}_{(j_1, \dots, j_k)}) \prod_{l=1}^{k} \left(\frac{m_{j_l} - a_{j_l}}{m_{j_l}} \right). \tag{8}$$

Now we separate the coefficient for $\tilde{s}_j$. Each such coefficient is formed only by the terms in which there is an index j in the products on the right-hand side of (7). As a result, we obtain the following coefficient:

$$\frac{b_j}{m_j} \prod_{l=1}^{r-1} \left(\frac{m_{i_l} - a_{i_l}}{m_{i_l}} \right), \quad 1 \le i_1 < \dots < i_{r-1}, \quad i_l \ne j. \tag{9}$$

(We assume that the product over an empty set is 1). Similarly, the coefficient for the product of $\tilde{s}_{j_1} \dots \tilde{s}_{j_k}$ is equal to

$$\prod_{p=1}^{k} \left(\frac{b_{j_p}}{m_{j_p}} \right) \prod_{l=1}^{u} \left(\frac{m_{i_l} - a_{i_l}}{m_{i_l}} \right), \quad 0 \le u \le r - k. \tag{10}$$

Next, we perform the transformations similar to those that led to the expressions (8) and (10). Thus, from (7) we obtain the following equality:

$$\frac{2^r\xi}{m_1\dots m_r}-\mathrm{wt}(f)$$
$$=-\frac{1}{2}\sum_{k=1}^{r}\sum_{1\le j_1<\ldots<j_k\le r}W_f(\mathbf{1}_{(j_1,\ldots,j_k)})\prod_{l=1}^{k}\left(\frac{m_{j_l}-a_{j_l}}{m_{j_l}}\right)$$
$$-\frac{1}{2}\sum_{k=1}^{r}\sum_{1\le j_1<\ldots<j_k\le r}\tilde{s}_{j_1}\dots\tilde{s}_{j_k}\frac{b_{j_1}}{m_{j_1}}\dots\frac{b_{j_k}}{m_{j_k}}c_{j_1,\ldots,j_k}, \qquad (11)$$

where

$$c_{j_1,\ldots,j_k}=W_f(\mathbf{1}_{(j_1,\ldots,j_k)})$$
$$+\sum_{u=1}^{r-k}\sum_{\substack{1\le i_1<\ldots<i_u\le r,\\ |\{j_1,\ldots,j_k,i_1,\ldots,i_u\}|=k+u}}W_f(\mathbf{1}_{(j_1,\ldots,j_k,i_1,\ldots,i_u)})\prod_{l=1}^{u}\left(\frac{m_{i_l}-a_{i_l}}{m_{i_l}}\right). \qquad (12)$$

Considering the notation (4), (5), and (12), the formula (11) can be rewritten as

$$\frac{2^r\xi}{m_1\dots m_r}+A$$
$$=-\frac{1}{2}\sum_{k=1}^{r}\sum_{1\le j_1<\ldots<j_k\le r}\tilde{s}_{j_1}\dots\tilde{s}_{j_k}\frac{b_{j_1}}{m_{j_1}}\dots\frac{b_{j_k}}{m_{j_k}}c_{j_1,\ldots,j_k}. \qquad (13)$$

According to Condition 1 the terms of the exterior sum for $k\le q-1$ on the right-hand side of (13) are of the order $o(1)$. Hereinafter, the entries of the form $\zeta_1=o(t)$ and $\zeta_2=O(t)$ mean that, for $t\to\infty$, the value of $\zeta_1 t^{-1}$ tends in probability to zero, and the value of $\zeta_2 t^{-1}$ is bounded in probability.

Then, from the conditions (2) we get the following dominant term of the right-hand side of (13):

$$\frac{2^r\xi}{m_1\dots m_r}+A$$
$$=-\frac{1}{2}\sum_{1\le j_1<\ldots<j_q\le r}\tilde{s}_{j_1}\dots\tilde{s}_{j_q}\frac{b_{j_1}}{m_{j_1}}\dots\frac{b_{j_q}}{m_{j_q}}c_{j_1,\ldots,j_q}+R(f), \qquad (14)$$

where, according to Condition 1, the remainder $R(f)$ can be estimated as

$$R(f)=O\left(\sum_{1\le j_1<\ldots<j_{q+1}\le r}\frac{b_{j_1}}{m_{j_1}}\dots\frac{b_{j_{q+1}}}{m_{j_{q+1}}}\right),\quad m_1,\ldots,m_r\to\infty. \qquad (15)$$

Consequently, if $m_1, \dots, m_r \to \infty$ the formula (15) results in the following:

$$\frac{m_1 \dots m_q}{b_1 \dots b_q} R(f) = O\left(\sum_{1 \le j_1 < \dots < j_{q+1} \le r} \frac{m_1 \dots m_q}{b_1 \dots b_q} \frac{b_{j_1}}{m_{j_1}} \dots \frac{b_{j_{q+1}}}{m_{j_{q+1}}} \right).$$

From Condition 2, we find that, for $m_1, \dots, m_r \to \infty$, there is a limit relation of the form

$$\frac{m_1 \dots m_q}{b_1 \dots b_q} \frac{b_{j_1}}{m_{j_1}} \dots \frac{b_{j_q}}{m_{j_q}} \to \frac{\rho_{j_1} \dots \rho_{j_q}}{\rho_1 \dots \rho_q} \in (0; 1].$$

Therefore, it remains bounded, and $b_{j_{q+1}}/m_{j_{q+1}} = o(1)$. Thus, $R(f) = o(1)$, and from (14) and Condition2 for $m_1, \dots, m_r \to \infty$, we derive

$$\tilde{\xi} = -\frac{m_1 \dots m_q}{2b_1 \dots b_q} \sum_{1 \le j_1 < \dots < j_q \le r} \tilde{s}_{j_1} \dots \tilde{s}_{j_q} \frac{b_{j_1}}{m_{j_1}} \dots \frac{b_{j_q}}{m_{j_q}} c_{j_1, \dots, j_q} + o(1). \qquad (16)$$

Under the conditions of Theorem 1 for $m_1, \dots, m_r \to \infty$

$$-\frac{m_1 \dots m_q}{2b_1 \dots b_q} \frac{b_{j_1}}{m_{j_1}} \dots \frac{b_{j_q}}{m_{j_q}} c_{j_1, \dots, j_k} \to \beta_{j_1, \dots, j_k}, \quad k = 1, \dots, r,$$

thus, it follows from (2) that the random variable on the right-hand side of (16) has the same limit distribution as the random variable V_q. The proof of Theorem 1 is complete.

4. Some examples

We assume that the registers contain mutually independent binary random letters, but their distributions may not be equiprobable for one or several registers.

Let $\eta_1, \dots, \eta_r$ be mutually independent random variables, each of which is distributed by the standard normal law.

Example 1. We consider the function f_1 of $r = 2$ variables of the form $f_1(u_1, u_2) = u_1 \oplus u_2$. For it, we have $W_{f_1}(\mathbf{1}_{(1,2)}) = 4$ and $W_{f_1}(z_1, z_2) = 0$ as $(z_1, z_2) \neq \mathbf{1}_{(1,2)}$. According to the formula (3)

$$\beta_j = -2\alpha_i \frac{\rho_j}{\rho_1}, \quad i \neq j, \quad i, j \in \{1, 2\}, \quad \beta_{1,2} = -4 \cdot \frac{1}{2} = -2.$$

If registers contain equiprobably distributed random letters, then $\alpha_i = 0$ and $\beta_j = 0$, $i, j = 1, 2$. Thus, in (4) $B_1^2 = 0$, $B_2^2 > 0$ and Condition 3 is satisfied for $q = 2$. Therefore, ξ converges in distribution to $V_2 = 2\eta_1\eta_2$ as in [5].

If $i \in \{1, 2\} : \alpha_i \neq 0$ exists then Condition 3 is satisfied for $q = 1$, and the limit distribution is a normal distribution corresponding to the random variable $V_1 = 2\left(\alpha_2\eta_1 + \alpha_1\frac{\rho_2}{\rho_1}\eta_2\right)$.

A similar result holds for the linear function of r variables of the form $f_1(u_1, \dots, u_r) = u_1 \oplus \dots \oplus u_r$. For this function, we have $W_{f_1}(\mathbf{1}_{(1,2,\dots,r)}) = 2^r$ and $W_{f_1}(z_1, \dots, z_r) = 0$ as $(z_1, \dots, z_r) \neq \mathbf{1}_{(1,\dots,r)}$. Thus, if registers contain equiprobably distributed random letters, then $\beta_{1,\dots,r} = -\frac{1}{2} \cdot 2^r = 2^{r-1}$ and all $\beta_{j_1,\dots,j_k} = 0$ for $1 \leq k \leq r - 1$. Thus, $q = r$ in Condition 3 and ξ converges in distribution to $V_r = -2^{r-1}\eta_1 \dots \eta_r$.

Example 2. We consider the function f_2 of $r = 2$ variables of the form $f_2(u_1, u_2) = u_1u_2$. For this function, we have $W_{f_2}(\mathbf{1}_{(1,2)}) = -2$ and $W_{f_2}(\mathbf{1}_{(j)}) = 2$, $j = 1, 2$. According to the formula (3)

$$\beta_j = -\frac{\rho_j}{\rho_1}(1 - \alpha_i), \quad i \neq j, \quad i, j \in \{1, 2\}, \quad \beta_{1,2} = -2 \cdot \frac{1}{2} = -1.$$

If $\alpha_i \neq 1$, $i = 1, 2$, then $B_1^2 > 0$ in (4), and Condition 3 is satisfied for $q = 1$. Consequently, ξ converges in distribution to $V_1 = (1-\alpha_2)\eta_1+(1-\alpha_1)\eta_2\frac{\rho_2}{\rho_1}$, which has a normal distribution with zero mean and variance $(1 - \alpha_2)^2 + (1 - \alpha_1)^2\frac{\rho_2^2}{\rho_1^2}$.

Particularly, if registers contain equiprobable random letters ($\alpha_i = 0$, $i = 1, 2$), then the distribution of ξ converges to the normal distribution with zero mean and variance $1 + \rho_2^2/\rho_1^2$.

Example 3. As in Example 1, we consider a balanced Boolean function of three variables $f_3(u_1, u_2, u_3) = u_1u_2 \oplus u_3$. For this function, we have

$$W_{f_3}(\mathbf{1}_{(3)}) = W_{f_3}(\mathbf{1}_{(1,3)}) = W_{f_3}(\mathbf{1}_{(2,3)}) = 4, \quad W_{f_3}(\mathbf{1}_{(1,2,3)}) = -4,$$
$$W_{f_3}(\mathbf{1}_{(1)}) = W_{f_3}(\mathbf{1}_{(2)}) = W_{f_3}(\mathbf{1}_{(1,2)}) = 0.$$

According to (3)

$$\beta_1 = -2\alpha_3(1 - \alpha_2), \quad \beta_2 = -2\frac{\rho_2}{\rho_1}\alpha_3(1 - \alpha_1),$$
$$\beta_3 = -2\frac{\rho_3}{\rho_1}(1 + \alpha_1 + \alpha_2 - \alpha_1\alpha_2), \quad \beta_{1,2} = -2\alpha_3,$$
$$\beta_{1,3} = -2\frac{\rho_3}{\rho_2}(1 - \alpha_1), \quad \beta_{2,3} = -2\frac{\rho_3}{\rho_1}(1 - \alpha_2), \quad \beta_{1,2,3} = 2.$$

The sum $B_1^2 = \sum_{j=1}^3 \beta_j^2 > 0$, if $\alpha_3 \neq 0$ or $(1 - \alpha_1)(1 - \alpha_2) \neq 2$. Hence, $q = 1$ in Condition 3. In that case the limit distribution of ξ is the normal distribution corresponding to the random variable

$$V_1 = -2\left(\alpha_3\left((1-\alpha_2)\eta_1 + \frac{\rho_2}{\rho_1}(1-\alpha_1)\eta_2\right) + \right.$$
$$\left. + \frac{\rho_3}{\rho_1}(1+\alpha_1+\alpha_2-\alpha_1\alpha_2)\eta_3\right).$$

For example, in the equiprobable case, we have $V_1 = -2\frac{\rho_3}{\rho_1}\eta_3$.

The sum $B_1^2 = \sum_{j=1}^3 \beta_j^2 = 0$, if $\alpha_3 = 0$ and $(1-\alpha_1)(1-\alpha_2) = 2$. It is not difficult to see that in this case $B_2^2 > 0$ ($q = 2$ in Condition 3), and the number ξ of 1's converges in distribution to the random variable

$$V_2 = -2\eta_3\left(\frac{\rho_3}{\rho_2}(1-\alpha_1)\eta_1 + \frac{\rho_3}{\rho_1}\frac{2}{1-\alpha_1}\eta_2\right).$$

In this case, the distribution of V_2 is formed by the product of two independent centered normal random variables with different variances.

Condition 3 for $q = 3$ cannot be satisfied for the function f_3 and any distribution of the random letters in the registers.

5. Conclusion

The present research completes and summarizes a series of research papers by the authors.The generalization of the results of Mezhennaya and Mikhailov [6, 7] for the limit distribution the number ξ of 1's per cycle of the random binary multicyclic sequence determined by Boolean function is obtained. The conditions of the limit theorem contain only the assumption that the numbers of 1's in each of the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ (with proper normalization) have their own limit distributions when their lengths tend to infinity, and the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_r$ are mutually independent. Previously, assumptions about the asymptotic normality of the number of 1's in the generator registers or assumptions on the independence and identical distribution of letters in the cells of generator registers [5, 14] were used.

References

[1] 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**, No 29 (2015), 17–31 (in Russian).

[2] O.V. Kamlovskii, Occurrence numbers for vectors in cycles of output sequences of binary combining generators, *Probl. Inf. Trans.*, **53**, No 1 (2017), 84–91.

[3] V.M. Fomichev, On periods of complicated sequences, *Mat. Vopr. Kibern.*, **13** (2004), 37–40 (in Russian).

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

[5] 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**, No 4 (2013), 95–107 (in Russian).

[6] N.M. Mezhennaya, V.G. Mikhailov, On the number of ones in outcome sequence of extended Pohl generator, *Discrete Math. Appl.*, **31**, No 1 (2019), 111–124 (in Russian).

[7] N.M. Mezhennaya, V.G. Mikhailov, On the number of ones in the cycle of multicyclic sequence determined by Boolean function, *Sib. Electr. Math. Reports*, **16** (2019), 229–235.

[8] O.V. Kamlovskii, Distribution properties of sequences produced by filtering generators, *Prikl. Diskr. Mat.*, **3(21)** (2013), 11-25 (in Russian).

[9] Z.D. Dai, X.N. Feng, M.L. Liu, Z.X. Wan, Some statistical properties of feedforward sequences (I), *Science in China* (*Ser. A*), **37**, No 1 (1994), 34–41.

[10] Z.D. Dai, X.N. Feng, M.L. Liu, Z.X. Wan, Some statistical properties of feedforward sequences (II). *Science in China* (*Ser. A*), **37**, No 2 (1994), 129–136.

[11] H. Niederreiter, Distribution properties of feedback shift register sequences, *Probl. Control and Inform. Theory*, **15**, No 1 (1986), 19–34.

[12] R.A. Rueppel, *Analysis and Design of Stream Ciphers.* Springer Verlag, Berlin-Heidelberg (1986).

[13] P. Pohl, On binary-exponent alternating sums, *BIT Numerical Mathematics*, **16**, No 3 (1976), 308–312.

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

[15] J.C. Fu, W.Y.W. Lou, Z.-D. Bai, G. Li, The exact and limiting distributions for the number of successes in success runs within a sequence of Markov-dependent two-state trials, *Ann. Inst. Statist. Math.*, **54**, No 4 (2002), 719–730.

[16] K. Inoue, S. Aki, Joint distributions of numbers of runs of specified length in a sequence of Markov dependent multistate trials, *Ann. Inst. Statist. Math.*, **59**, No 3 (2007), 577–595.

[17] N.M. Mezhennaya, On the number of event appearances in a Markov chain, *Int. J. Appl. Math.*, **32**, No 3 (2019), 537–547; DOI: 10.12732/ijam.v32i3.13.

[18] V.G. Mikhailov, Estimates of accuracy of the Poisson approximation for the distribution of number of runs of long string repetitions in a Markov chain, *Discrete Math. Appl.*, **26**, No 2 (2016), 105–113.

[19] V.G. Mikhailov, A.M. Shoitov, On repetitions of long tuples in a Markov chain, *Discrete Math. Appl.*, **25**, No 5 (2015), 295–303.

[20] T. Ritter, *Ritter's Crypto Glossary and Dictionary of Technical Cryptography*, 2007; Available at: http://ciphersbyritter.com/GLOSSARY.HTM.

[21] B. Preneel, O.A. Logachev, *Boolean Functions in Cryptology and Information Security*, IOS Press, Amsterdam (2008).