

## РАДИОФИЗИКА

---

УДК 519.7

DOI: 10.34680/2076-8052.2023.5(134).700-707

ГРНТИ 27.47

Специальность ВАК 1.3.4

*Научная статья*

### СИММЕТРИЧНАЯ 2-АДИЧЕСКАЯ СЛОЖНОСТЬ ОБОБЩЕННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ХОЛЛА

Едемский В. А., Гаврушко В. В., Петров В. М.

*Новгородский государственный университет имени Ярослава Мудрого  
(Великий Новгород, Россия)*

**Аннотация** Исследуется симметричная 2-адическая сложность обобщенных циклотомических последовательностей Холла, период которых равен степени простого числа. Для определения последовательностей применяются обобщенные циклотомические классы. Показано, что рассмотренные последовательности обладают высокой симметричной 2-адической сложностью. Метод исследования основан на применении обобщенных гауссовых периодов.

**Ключевые слова:** симметричная 2-адическая сложность, обобщенные бинарные циклотомические последовательности, гауссовы периоды

**Для цитирования:** Едемский В. А., Гаврушко В. В., Петров В. М. Симметричная 2-адическая сложность обобщенных последовательностей Холла // Вестник НовГУ. 2023. 5(134). 700-707. DOI: 10.34680/2076-8052.2023.5(134).700-707

*Research Article*

### SYMMETRIC 2-ADIC COMPLEXITY OF HALL GENERALIZED CYCLOTOMIC SEQUENCES

Edemskiy V. A., Gavrushko V. V., Petrov V. M.

*Yaroslav-the-Wise Novgorod State University (Veliky Novgorod, Russia)*

**Abstract** We study the symmetric 2-adic complexity of Hall generalized cyclotomic sequences whose period is equal to the power of a prime. Sequences are defined based on generalized cyclotomic classes. It is shown that the considered sequences have high symmetric 2-adic complexity. The research method uses generalized Gaussian periods.

**Keywords:** symmetric 2-adic complexity, generalized binary cyclotomic sequences, Gaussian periods

**For citation:** Edemskiy V. A., Gavrushko V. V., Petrov V. M. Symmetric 2-adic complexity of Hall generalized cyclotomic sequences // Vestnik NovSU. 2023. 5(134). 700-707. DOI: 10.34680/2076-8052.2023.5(134).700-707

### Введение

Псевдослучайные последовательности имеют множество характеристик, таких как автокрелляция, сбалансированность, сложность и другие. Сложность последовательности определяет её непредсказуемость, что важно для некоторых приложений. Бинарные последовательности относятся к наиболее часто изучаемым и применяемым. В [1] показано, что важной характеристикой непредсказуемости

бинарной последовательности является её 2-адическая сложность, которая определяется как наименьшая длина регистра сдвига с обратной связью с переносом. Согласно [1], 2-адическую сложность последовательности  $s^\infty = (s_0, s_1, s_2, \dots)$  можно найти по следующей формуле:

$$\Phi(s^\infty) = \left\lfloor \log_2 \left( \frac{2^N - 1}{\text{НОД}(S(2), 2^N - 1)} + 1 \right) \right\rfloor, \quad (1)$$

где  $S(x) = \sum_{i=0}^{N-1} s_i x^i \in \mathbb{Z}[x]$  – образующий многочлен последовательности, а  $[x]$  – целая часть числа  $x$ . Таким образом, задача исследования 2-адической сложности сводится к анализу  $\text{НОД}(S(2), 2^N - 1)$ . В общем случае это достаточно сложная задача. В [2] предложен метод вычисления данного НОД с применением циклического определителя, составленного из значений дискретного преобразования Фурье последовательности. Далее, метод анализа 2-адической сложности с использованием периодической автокорреляционной функции представлен в [3], также в [3] показано, что 2-адическая сложность бинарных последовательностей с идеальной периодической автокорреляцией достигает максимально возможного значения. Совсем недавно, в [4] предложен метод анализа 2-адической сложности на основе обобщенных гауссовых периодов. В этой работе будем использовать модификацию этого метода. Покажем, что обобщенные циклотомические последовательности Холла с периодом  $p^n$  при  $p = A^2 + 3B^2$ ,  $A \equiv 1 \pmod{3}$ ,  $B \equiv 0 \pmod{3}$  и нечетном значении  $(p-1)/6$  обладают большой 2-адической сложностью. В частном случае, для  $B = 3$  это показано в [3]. Метод, применяемый здесь, отличается от подхода, используемого в [3].

Далее, в [5] было показано, что для оценки непредсказуемости бинарных последовательностей предпочтительнее использовать симметричную 2-адическую сложность  $\bar{\Phi}(s^\infty)$ , которая определяется как  $\bar{\Phi}(s^\infty) = \min(\Phi(s^\infty), \Phi(\tilde{s}^\infty))$ , где  $\tilde{s}^\infty = (s_{N-1}, s_{N-2}, \dots, s_0)$  – последовательность, обратная к  $s^\infty$ . Поэтому в этой статье исследуем также симметричную 2-адическую сложность обобщенной последовательности Холла. Ранее, 2-адическая сложность и симметричная 2-адическая сложность циклотомических последовательностей простого периода и кратного ему изучались в [6-9]; сложность обобщенных бинарных циклотомических последовательностей с периодом  $p^n, n > 1$ , сформированных на классах второго порядка, исследовалась в [10], шестого в [11], при другом определении последовательностей.

### Определение последовательностей

Пусть  $p$  – простое число, такое что  $p \equiv 7 \pmod{12}$ , и  $n \geq 1$  – целое число. Обозначим через  $g$  примитивный корень по модулю  $p^n$ . Хорошо известно, что он всегда существует и его порядок по модулю  $p^n$  равен значению функции Эйлера, то есть порядок  $g$  равен  $p^{n-1}(p-1)$ .

Для каждой степени простого числа  $p^k$ ,  $k = 1, 2, \dots, n$  определим Динга-Хеллесета обобщенные циклотомические классы шестого порядка по этому модулю:

$$D_j^{(p^k)} = \{g^{j+6t} \pmod{p^k} \mid 0 \leq t < p^{k-1}(p-1)/6\}, \quad j = 0, 1, \dots, 5.$$

Обозначим через  $\mathbb{Z}_{p^k}$  кольцо классов вычетов по модулю  $p^k$ , а через  $\mathbb{Z}_{p^k}^*$  группу его обратимых элементов. Тогда справедливы разбиения:

$$\mathbb{Z}_{p^k}^* = \bigcup_{j=0}^5 D_j^{(p^k)} \text{ и } \mathbb{Z}_{p^n} = \bigcup_{k=1}^n \bigcup_{j=0}^5 p^{n-k} D_j^{(p^k)} \cup \{0\}.$$

Пусть  $C_0 = \bigcup_{k=1}^n p^{n-k} (D_0^{(p^k)} \cup D_1^{(p^k)} \cup D_3^{(p^k)})$  and  $C_1 = \bigcup_{k=1}^n p^{n-k} (D_2^{(p^k)} \cup D_4^{(p^k)} \cup D_5^{(p^k)}) \cup \{0\}$ .

Обобщенная последовательность Холла  $s^\infty = (s_0, s_1, s_2, \dots)$  с периодом  $p^n$  определяется следующим образом:

$$s_i = \begin{cases} 0, & \text{if } i \pmod{p^n} \in C_0, \\ 1, & \text{if } i \pmod{p^n} \in C_1. \end{cases} \quad (2)$$

Когда  $n = 1$ , последовательность  $s^\infty$  является последовательностью шестеричных вычетов Холла. Её линейная сложность исследована в [12]. Хорошо известно, что, если период последовательности Холла равен  $p = A^2 + 27$ ,  $A \equiv 1 \pmod{3}$ , то она обладает идеальной автокорреляцией. Следовательно, как отмечено во введении, её 2-адическая сложность достигает максимально возможного значения и равна периоду последовательности. Здесь исследуем её 2-адическую сложность для  $B \equiv 0 \pmod{3}$ , в том числе, для  $n > 1$ . С этой целью в следующем разделе рассмотрим свойства обобщенных гауссовых периодов.

### Обобщенные гауссовы периоды

Обозначим через  $H_i$  циклотомические классы третьего порядка по модулю  $p$ , тогда  $H_i = D_i^{(p)} \cup D_{i+3}^{(p)}$ ,  $i = 0, 1, 2$ .

Пусть  $\eta_j(a) = \sum_{i \in H_j} a^i$ ,  $j = 0, 1, 2$  и  $\zeta_j(a) = \sum_{i \in D_j^{(p)}} a^i$ ,  $j = 0, 1, \dots, 5$ . Когда  $a$  – комплексный или алгебраический корень  $p$ -ой степени из единицы, то эти суммы называются гауссовыми периодами третьего и шестого порядков, соответственно. Суммы по циклотомическим классам четвертого порядка с  $a = 2$  использовались в [4] для исследования 2-адической сложности последовательностей Динга-Хеллесета-Мартинсена. Авторы называли их обобщенными гауссовыми периодами. Здесь для изучения свойств обобщенных гауссовых периодов потребуются циклотомические числа  $(k, f)_3$  третьего порядка и  $(u, j)_6$  шестого порядка. По определению,  $(k, f)_3 = |(H_k + 1) \cap H_f|$  и  $(u, j)_3 = |(D_u^{(p)} + 1) \cap D_j^{(p)}|$ ,  $k, f, u, j \in \mathbb{Z}$ .

Следующие свойства обобщенных гауссовых периодов обсуждались в ряде статей, в частности, в [11]. Имеют место следующее утверждения.

**Лемма 1.** Пусть  $a = 2^{p^m}$ . Тогда:

1.  $\eta_l(a) \cdot \eta_{l+k}(a) \equiv \sum_{f=0}^3 (k, f)_3 \eta_{f+l}(a) + \delta_1 \pmod{a^p - 1}$ , где  $k, l = 0, 1, 2$  и

$$\delta_1 = \begin{cases} (p-1)/3, & \text{если } k = 0, \\ 0, & \text{иначе.} \end{cases}$$

2.  $\zeta_u(a) \cdot \zeta_{u+v}(a) \equiv \sum_{j=0}^6 (u, j)_6 \zeta_{j+u}(a) + \delta_2 \pmod{a^p - 1}$ , где  $u, v = 0, 1, \dots, 5$  и

$$\delta_2 = \begin{cases} \frac{p-1}{6}, & \text{если } p \equiv 1 \pmod{12}, k = 0 \text{ или } p \equiv 7 \pmod{12}, k = 3, \\ 0, & \text{иначе.} \end{cases}$$

Воспользовавшись леммой 1 и соотношением  $\eta_l(a) = \zeta_l(a) + \zeta_{l+3}(a)$ ,  $l = 0, 1, 2$ , получаем, что

$$\zeta_1(a) \cdot \zeta_4(a) \equiv (2, 0)_6 \eta_0(a) + (0, 0)_6 \eta_1(a) + (1, 0)_6 \eta_2(a) + \frac{p-1}{6} \pmod{a^p - 1}. \quad (3)$$

Известны следующие формулы для циклотомических чисел третьего порядка [13]:

$$(0, 0)_3 = (p - 8 + L)/9, (0, 1)_3 = (2, 2)_3 = (2p - 4 - L - 9M)/18,$$

$$(0, 2)_3 = (1, 1)_3 = (2p - 4 - L + 9M)/18, (1, 2)_3 = (p + 1 + L)/9,$$

где  $M, L : 4p = L^2 + 27M^2$ ,  $L \equiv 1 \pmod{3}$ , знак определяется  $M$  выбором  $g$ .

**Лемма 2.** Пусть  $a = 2^{p^m}$ . Тогда разности обобщенных гауссовых периодов  $\eta_0(a) - \eta_1(a)$ ,  $\eta_1(a) - \eta_2(a)$  и  $\eta_2(a) - \eta_0(a)$  удовлетворяют сравнению:

$$X^3 - pX - pM \equiv 0 \pmod{(a^p - 1)/(a - 1)}.$$

Для доказательства леммы 2 воспользуемся теоремой Виета. Ясно, что сумма  $\eta_0(a) - \eta_1(a)$ ,  $\eta_1(a) - \eta_2(a)$  и  $\eta_2(a) - \eta_0(a)$  равна нулю. Далее, пусть  $E = (\eta_0(a) - \eta_1(a))(\eta_1(a) - \eta_2(a)) + (\eta_2(a) - \eta_0(a))(\eta_0(a) - \eta_1(a)) + (\eta_1(a) - \eta_2(a))(\eta_2(a) - \eta_0(a)) = \eta_0(a)\eta_1(a) + \eta_1(a)\eta_2(a) + \eta_0(a)\eta_2(a) - \eta_0^2(a) - \eta_1^2(a) - \eta_2^2(a)$ . Согласно [9],  $\eta_0(a)\eta_1(a) + \eta_1(a)\eta_2(a) + \eta_0(a)\eta_2(a) \equiv -(p-1)/3 \pmod{(a^p - 1)/(a - 1)}$ , значит  $\eta_0^2(a) + \eta_1^2(a) + \eta_2^2(a) = (2p+1)/3 \pmod{(a^p - 1)/(a - 1)}$ . Тогда  $E = -p$ .

Наконец, если  $F = (\eta_0(a) - \eta_1(a))(\eta_1(a) - \eta_2(a))(\eta_2(a) - \eta_0(a))$ , то, применяя лемму 1 и упомянутые выше формулы для циклотомических чисел третьего порядка, получаем, что

$F = ((0, 1)_3 - (0, 2)_3)(\eta_0(a)\eta_1(a) + \eta_1(a)\eta_2(a) + \eta_0(a)\eta_2(a) - \eta_0^2(a) - \eta_1^2(a) - \eta_2^2(a)) = Mp$ , что завершает доказательство леммы 2.

**Лемма 3.** Пусть  $U(a) = \zeta_0(a) + \zeta_1(a) + \zeta_3(a)$  и  $\tilde{U}(a) = \zeta_0(a) + \zeta_4(a) + \zeta_3(a)$ . Тогда

$$U(a)\tilde{U}(a) \equiv (B - 3)(\eta_2(a) - \eta_0(a))/6 + (p + 1)/4 \pmod{(a^p - 1)/(a - 1)}. \quad (4)$$

**Доказательство.** Так как  $\zeta_0(a) + \zeta_3(a) = \eta_0(a)$ , то  $U(a)\tilde{U}(a) = \eta_0^2(a) + \eta_0(a)\eta_1(a) + \zeta_1(a)\zeta_4(a)$ . Далее, для  $p \equiv 1 \pmod{6}$  справедливо разложение  $p = A^2 +$

$3B^2$ ,  $A \equiv 1 \pmod{3}$ , которое определяет формулы для вычисления циклотомических чисел шестого порядка [13]. В частности, для  $p \equiv 7 \pmod{12}$  и  $B \equiv 0 \pmod{3}$  имеем, что  $(0,0)_6 = (p - 11 - 8A)/36$ ,  $(1,0)_6 = (p - 5 + 4A + 6B)/36$ ,  $(2,0)_6 = (p - 5 + 4A - 6B)/36$ . Кроме этого, известно, что  $L = -2A$ ,  $-3M = 2B$  [13]. Применяя лемму 1 и данные формулы, получаем, что  $U(a)\tilde{U}(a) \equiv (B - 3)(\eta_2(a) - \eta_0(a))/6 + (p + 1)/4 \pmod{(a^p - 1)/(a - 1)}$ , что и доказывает лемму 3.

### Симметричная 2-адическая сложность последовательностей

В этом разделе завершим исследование 2-адической сложности последовательности. Прежде всего, рассмотрим порождающий многочлен  $\tilde{S}(x)$ , последовательности, обратной к  $s^\infty$ . Согласно определению этой последовательности, имеем:  $\tilde{S}(x) = \sum_{i=0}^{p^n-1} s_{p^{n-1}-i} x^i$  и  $2\tilde{S}(2) = \sum_{i=1}^{p^n} s_{p^n-i} 2^i$ . Тогда  $2\tilde{S}(2) = \sum_{i=0}^{p^n-1} s_{-i} 2^i - s_0 + s_0 2^{p^n}$  и  $2\tilde{S}(2) \equiv \sum_{i=0}^{p^n-1} s_{-i} 2^i \pmod{2^{p^n} - 1}$ . По условию,  $p \equiv 7 \pmod{12}$ , значит  $-1 \in D_3^{(p^n)}$ , следовательно,  $-i \in p^m D_{(j+3) \bmod 2}^{(p^n)}$ , когда  $i \in p^m D_j^{(p^n)}$ . Таким образом,

$$2\tilde{S}(2) = \sum_{k=0}^{n-1} \sum_{i \in p^{n-k}(D_0^{(p^k)} \cup D_4^{(p^k)} \cup D_3^{(p^k)})} 2^i.$$

Следующая лемма может быть доказана тем же самым способом, что и лемма 5 из [11].

**Лемма 4.** Пусть последовательность  $s^\infty$  определена по (2) и  $S(x) = \sum_{i=0}^{p^n-1} s_i x^i$  её многочлен. Тогда

1.  $S(2) \equiv p^{n-m-1} U(2^{p^m}) + (p^{n-m-1} - 1)/2 \left( \bmod \frac{2^{p^{m+1}} - 1}{2^{p^m} - 1} \right)$ ,
2.  $2\tilde{S}(2) \equiv p^{n-m-1} \tilde{U}(2^{p^m}) + (p^{n-m-1} - 1)/2 \left( \bmod \frac{2^{p^{m+1}} - 1}{2^{p^m} - 1} \right)$ .

для  $m = 0, 1, \dots, n - 1$ .

**Теорема 1.** Если последовательность  $s^\infty$  определена по формуле (2) при  $p \equiv 7 \pmod{12}$ ,  $B \equiv 0 \pmod{3}$ , то  $\bar{\Phi}(s^\infty) \geq p^n - p^{n-1} - 3 \log_2 p$ .

**Доказательство.** Согласно лемме 4 видим, что  $S(2) \equiv U(2^{p^{n-1}}) \left( \bmod \frac{2^{p^n} - 1}{2^{p^{n-1}} - 1} \right)$  и  $2\tilde{S}(2) \equiv \tilde{U}(2^{p^{n-1}}) \left( \bmod \frac{2^{p^n} - 1}{2^{p^{n-1}} - 1} \right)$ . Пусть  $a = 2^{p^{n-1}}$ . В силу соотношения (4) получаем, что

$$S(2)\tilde{S}(2) \equiv (B - 3)(\eta_2(a) - \eta_0(a))/6 + (p + 1)/4 \pmod{(a^p - 1)/(a - 1)}. \quad (5)$$

Рассмотрим два случая.

1) Пусть  $B = 3$ . Тогда, согласно сравнению (5), имеем, что  $S(2)\tilde{S}(2) \equiv ((p + 1)/4 \pmod{(a^p - 1)/(a - 1)})$ . Следовательно, любое натуральное число  $d \neq 1$ , что делит  $\text{НОД}(S(2), (a^p - 1)/(a - 1))$  или  $\text{НОД}(\tilde{S}(2), (a^p - 1)/(a - 1))$  должно делить также  $(p + 1)/4$ , что невозможно, так как по малой теореме Ферма  $d - 1$  делится на

$p^n$ . Таким образом,  $\text{НОД}(S(2), (a^p - 1)/(a - 1)) = \text{НОД}(\tilde{S}(2), (a^p - 1)/(a - 1)) = 1$ . Это означает, что  $\text{НОД}(S(2), 2^{p^n} - 1) \leq 2^{p^{n-1}} - 1$  и  $\text{НОД}(\tilde{S}(2), 2^{p^n} - 1) \leq 2^{p^{n-1}} - 1$ , тогда, воспользовавшись формулой (1), получаем следующие неравенства:  $\Phi(s^\infty) \geq p^n - p^{n-1}$ ,  $\Phi(\tilde{s}^\infty) \geq p^n - p^{n-1}$ , таким образом  $\bar{\Phi}(s^\infty) \geq p^n - p^{n-1}$ . Утверждение теоремы 1 доказано в первом случае.

2) Пусть  $B \neq 3$  и  $d = \text{НОД}(S(2), (a^p - 1)/(a - 1))$ . Тогда, воспользовавшись леммой 3, получаем следующее сравнение:  $(B - 3)(\eta_2(a) - \eta_0(a))/3 \equiv -(p + 1)/2 \pmod{d}$ . Согласно лемме 2,  $(B - 3)(\eta_2(a) - \eta_0(a))/3$  удовлетворяет сравнению  $Z^3 - 36p(B - 3)^2Z - 216p(B - 3)^2M \equiv 0 \pmod{d}$ . Следовательно,  $-(p + 1)^3/8 + 9p(B - 3)^2(p + 1) - 36p(B - 3)^2M \equiv 0 \pmod{d}$ . Так как  $-(p + 1)^3/8 + 9p(B - 3)^2(p + 1) - 36p(B - 3)^2M \neq 0$ , то  $d < |-(p + 1)^3/8 + 9p(B - 3)^2(p + 1) - 36p(B - 3)^2M|$ . Следовательно,  $d < p^3$  и  $\text{НОД}(S(2), 2^N - 1) < p^3(2^{p^{n-1}} - 1)$ . Таким образом,  $\Phi(s^\infty) \geq p^n - p^{n-1} - 3 \log_2 p$ .

Как уже отмечалось,  $2\tilde{S}(2) \equiv \tilde{U}(2^{p^{n-1}}) \pmod{(a^p - 1)/(a - 1)}$ . Следовательно, снова применяя сравнение (4), можем показать таким же самым способом, что  $\text{НОД}(\tilde{S}(2), (a^p - 1)/(a - 1)) < p^3$  и  $\Phi(\tilde{s}^\infty) \geq p^n - p^{n-1} - 3 \log_2 p$ , что завершает доказательство теоремы.

Теорема 1 показывает, что симметричная 2-адическая сложность рассмотренных последовательностей больше половины периода, то есть они обладают высокой сложностью.

### Заключение

В работе изучена симметричная 2-адическая сложность обобщенных циклотомических последовательностей Холла. Показано, что рассмотренные последовательности обладают высокой 2-адической сложностью. Результаты обобщают полученные ранее в [5, 11]. Применяя метод, разработанный в [11], полученную оценку можно улучшить при увеличении  $n$ .

### Благодарности

Работа выполнена при поддержке Российского научного фонда, проект № 22–21–00516.

### Список литературы

1. Goresky M., Klapper A. Algebraic Shift Register Sequences. Cambridge University Press, 2012. 498 p.
2. Xiong H., Qu L., Li C. A new method to compute the 2-adic complexity of binary sequences // IEEE Transactions on Information Theory. 2014. 60(4). 2399-2406. DOI: 10.1109/TIT.2014.2304451
3. Hu H. Comments on "A new method to compute the 2-adic complexity of binary sequences" // IEEE Transactions on Information Theory. 2014. 60(9). 5803-5804. DOI: 10.1109/TIT.2014.2336843

4. Zhang L., Zhang J., Yang M., Feng K. On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences // IEEE Transactions on Information Theory. 2020. 66(7). 4613-4620. DOI: 10.1109/TIT.2020.2964171
5. Hu H., Feng D. On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences // IEEE Transactions on Information Theory. 2008. 54(2). 874-883. DOI: 10.1109/TIT.2007.913238
6. Xiao Z., Zeng X., Ke M. On the symmetric 2-adic complexity of periodic binary sequences // Advances in Mathematics of Communications. 2022. DOI: 10.3934/amc.2022088
7. Sun Y., Yan T., Chen Z., Wang L. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude // Cryptography and Communications. 2020. 12(3). 675-683. DOI: 10.1007/s12095-019-00411-4
8. Sun F., Yue Q., Li X. On the 2-adic complexity of cyclotomic binary sequences of order four // Applicable Algebra in Engineering Communication and Computing (AAECC). 2023. DOI: 10.1007/s00200-023-00598-3
9. Sun F., Yue Q., Li X. On the 2-adic complexity of cyclotomic binary sequences of order three // Advances in Mathematics of Communications. 2022. 16(4). 985-999. DOI: 10.3934/amc.2022049
10. Xiao Z., Zeng X., Sun Z. 2-Adic complexity of two classes of generalized cyclotomic binary sequences // International Journal of Foundations of Computer Science. 2016. 27(7). 879-893. DOI: 10.1142/s0129054116500350
11. Edemskiy V. A., Koltsova S. A. Symmetric 2-adic complexity of generalized cyclotomic sequences of order six with period  $p^n$  // Journal of Physics: Conference Series. 2021. 2052. 012009. DOI: 10.1088/1742-6596/2052/1/012009
12. Kim J.-H., Song H.-Y. On the linear complexity of Hall's sextic residue sequences // IEEE Transactions on Information Theory. 2001. 47(5). 2094-2096. DOI: 10.1109/18.930950
13. Холл М. Комбинаторика / перевод с английского С. А. Широковой. Москва: Мир, 1970. 424 с.
14. Cusick T., Ding C., Renvall A. Stream Ciphers and Number Theory. North-Holland mathematical library. Elsevier, 2004. 474 p.

## References

1. Goresky M., Klapper A. Algebraic Shift Register Sequences. Cambridge University Press, 2012. 498 p.
2. Xiong H., Qu L., Li C. A new method to compute the 2-adic complexity of binary sequences // IEEE Transactions on Information Theory. 2014. 60(4). 2399-2406. DOI: 10.1109/TIT.2014.2304451
3. Hu H. Comments on "A new method to compute the 2-adic complexity of binary sequences" // IEEE Transactions on Information Theory. 2014. 60(9). 5803-5804. DOI: 10.1109/TIT.2014.2336843
4. Zhang L., Zhang J., Yang M., Feng K. On the 2-adic complexity of the Ding-Helleseth-Martinsen binary sequences // IEEE Transactions on Information Theory. 2020. 66(7). 4613-4620. DOI: 10.1109/TIT.2020.2964171
5. Hu H., Feng D. On the 2-adic complexity and the k-error 2-adic complexity of periodic binary sequences // IEEE Transactions on Information Theory. 2008. 54(2). 874-883. DOI: 10.1109/TIT.2007.913238
6. Xiao Z., Zeng X., Ke M. On the symmetric 2-adic complexity of periodic binary sequences // Advances in Mathematics of Communications. 2022. DOI: 10.3934/amc.2022088

7. Sun Y., Yan T., Chen Z., Wang L. The 2-adic complexity of a class of binary sequences with optimal autocorrelation magnitude // *Cryptography and Communications*. 2020. 12(3). 675-683. DOI: 10.1007/s12095-019-00411-4
8. Sun F., Yue Q., Li X. On the 2-adic complexity of cyclotomic binary sequences of order four // *Applicable Algebra in Engineering Communication and Computing (AAECC)*. 2023. DOI: 10.1007/s00200-023-00598-3
9. Sun F., Yue Q., Li X. On the 2-adic complexity of cyclotomic binary sequences of order three // *Advances in Mathematics of Communications*. 2022. 16(4). 985-999. DOI: 10.3934/amc.2022049
10. Xiao Z., Zeng X., Sun Z. 2-Adic complexity of two classes of generalized cyclotomic binary sequences // *International Journal of Foundations of Computer Science*. 2016. 27(7). 879-893. DOI: 10.1142/s0129054116500350
11. Edemskiy V. A., Koltsova S. A. Symmetric 2-adic complexity of generalized cyclotomic sequences of order six with period  $pn$  // *Journal of Physics: Conference Series*. 2021. 2052. 012009. DOI: 10.1088/1742-6596/2052/1/012009
12. Kim J.-H., Song H.-Y. On the linear complexity of Hall's sextic residue sequences // *IEEE Transactions on Information Theory*. 2001. 47(5). 2094-2096. DOI: 10.1109/18.930950
13. Hall M. *Combinatorial Theory*. Blaisdell, Waltham, MA, 1967. 310 p. (Russ. ed.: Khol M. *Kombinatorika*. Moscow, Mir Publ., 1970. 424 p.)
14. Cusick T., Ding C., Renvall A. *Stream Ciphers and Number Theory*. North-Holland mathematical library. Elsevier, 2004. 474 p.

#### **Информация об авторах**

*Едемский Владимир Анатольевич* – доктор физико-математических наук, доцент, заведующий кафедрой, Новгородский государственный университет имени Ярослава Мудрого (Великий Новгород, Россия), ORCID: 0000-0003-1368-3827, Vladimir.Edemsky@novsu.ru

*Гаверушко Валерий Владимирович* – доктор технических наук, профессор, профессор, Новгородский государственный университет имени Ярослава Мудрого (Великий Новгород, Россия), ORCID: 0000-0002-8704-6751, Valery.Gavrushko@novsu.ru

*Петров Владимир Михайлович* – доктор технических наук, профессор, профессор, главный научный сотрудник, Новгородский государственный университет имени Ярослава Мудрого (Великий Новгород, Россия), ORCID: 0000-0002-7733-1030, Vladimir.Petrov@novsu.ru