

РАДИОТЕХНИКА И СВЯЗЬ

УДК 519.7:517.521.1

DOI: 10.34680/2076-8052.2024.3(137).489-497

Поступила в редакцию / Received 04.07.2024

ГРНТИ 27.47.17

Специальность ВАК 2.2.13; 1.3.4

Принята к публикации / Accepted 19.09.2024

Научная статья

О СИММЕТРИЧНОЙ 2-АДИЧЕСКОЙ СЛОЖНОСТИ ЧЕРЕДУЮЩИХСЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЛЕЖАНДРА

Едемский В. А., Дроганова Д. С.

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

Аннотация 2-адическая сложность, наряду с линейной сложностью, являются важными характеристиками псевдослучайных последовательностей, значимыми для их практических приложений. Для оценки непредсказуемости бинарных последовательностей предпочтительнее симметричная 2-адическая сложность, которая определяется как наименьшая из 2-адической сложности последовательности и 2-адической сложности последовательности, записанной в обратном порядке. В статье исследуется симметричная 2-адическая сложность чередующихся бинарных последовательностей, обладающих высокой линейной сложностью и хорошими автокорреляционными свойствами. Для определения рассматриваемых последовательностей используются циклические сдвиги последовательностей Лежандра и их дополнения. Показано, что для этих последовательностей симметричная 2-адическая сложность близка к максимально возможной и достаточна для отражения атак посредством алгоритма рациональной аппроксимации. Метод исследования основан на анализе соотношения между периодической автокорреляционной функцией последовательности, значения которой известны, и порождающего многочлена последовательности, инверсной к искомой.

Ключевые слова: бинарные последовательности, симметричная 2-адическая сложность, чередование последовательностей Лежандра

Для цитирования: Едемский В. А., Дроганова Д. С. О симметричной 2-адической сложности чередующихся последовательностей на основе последовательностей Лежандра // Вестник НовГУ. 2024. 3 (137). 489-497. DOI: 10.34680/2076-8052.2024.3(137).489-497

Research Article

ABOUT SYMMETRIC 2-ADIC COMPLEXITY OF INTERLEAVING SEQUENCES BASED ON LEGENDRE SEQUENCES

Edemskiy V. A., Droганova D. S.

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

Abstract 2-adic complexity, along with linear complexity, are important characteristics of pseudorandom sequences that are significant for their practical applications. To assess the unpredictability of binary sequences, symmetric 2-adic complexity is preferred, which is defined as the lesser of the 2-adic complexity of the sequence and the 2-adic complexity of the sequence written in reverse order. The article studies the symmetric 2-adic complexity of alternating binary sequences with high linear complexity and good autocorrelation properties. To determine the sequences under consideration, cyclic shifts of Legendre sequences and their complements are used. It is shown that for these sequences the symmetric 2-adic complexity is close to the maximum possible and is sufficient to repel attacks using the rational approximation algorithm. The research method is based on the analysis of the relationship between the periodic autocorrelation function of a sequence, the values of which are known, and the generating polynomial of the sequence, inverse to the desired one.

Keywords: *binary sequences, symmetric 2-adic complexity, interleaving Legendre sequences*

For citation: Edemskiy V. A., Droганova D. S. About symmetric 2-adic complexity of interleaving sequences based on Legendre sequences // Vestnik NovSU. 2024. 3(137). 489-497. DOI: 10.34680/2076-8052.2024.3(137).489-497

Введение

Для оценки непредсказуемости бинарных псевдослучайные последовательности применяются различные виды сложностей, в частности 2-адическая и симметричная 2-адическая сложности [1, 2]. Понятие 2-адической сложности предложено Горески и Клаппер в [1] при исследовании свойств последовательностей, формируемых посредством нового регистра сдвига, который они назвали регистром сдвига с обратной связью с переносом.

Изучению 2-адической сложности и симметричной 2-адической сложности бинарных последовательностей, в частности циклотомических и полученных их чередованием, посвящено много работ [3-9]. В настоящей статье продолжим исследование 2-адической сложности, начатое в [8, 9] и изучим симметричную 2-адическую сложность бинарных последовательностей, которые получаются чередованием циклических сдвигов последовательностей Лежандра и их дополнений.

Определение последовательностей

Рассмотрим множество из M последовательностей $\{a_0, a_1, \dots, a_{M-1}\}$ с периодом N . Через $u = I(a_0, a_1, \dots, a_{M-1})$ будем обозначать чередующуюся последовательность, полученную из $a_0, a_1, \dots, a_{M-1}$. Здесь, I – оператор чередования. Как показано в [10-14], при соответствующем выборе $a_0, a_1, \dots, a_{M-1}$ последовательность u , имеющую высокую линейную сложность и хорошие автокорреляционные свойствами, в частности, если в качестве последовательностей $a_0, a_1, \dots, a_{M-1}$ использованы циклические сдвиги последовательностей Лежандра и их дополнения [10]. Здесь исследуем симметричную 2-адическую сложность двух семейств таких.

Пусть $p > 5$ – нечетное простое число. Множества квадратичных вычетов и невычетов по модулю p обозначим через QR и NR , соответственно. Эти множества образуют разбиение группы обратимых элементов: $\mathbb{Z}_N^* = QR \cup NR$.

Пусть $\left(\frac{m}{p}\right)$ – символ Лежандра, то есть

$$\left(\frac{m}{p}\right) = \begin{cases} 0, & \text{если } m = 0, \\ 1, & \text{если } m \in QR, \\ -1, & \text{если } m \in NR. \end{cases}$$

Двоичные последовательности Лежандра l и l' определяются по следующим формулам

$$(t) = \begin{cases} 1, & \text{если } t = 0, \\ 1, & \text{если } t \in \mathbb{QR}, \\ 0, & \text{если } t \in \mathbb{NR}. \end{cases} \quad \text{и} \quad l'(t) = \begin{cases} 0, & \text{если } t = 0, \\ 1, & \text{если } t \in \mathbb{QR}, \\ 0, & \text{если } t \in \mathbb{NR}. \end{cases}$$

2-адическая сложность двух семейств последовательностей, получающихся из последовательностей l и l' исследована в [13], но вопрос об их симметричной 2-адической сложности остался открытым.

Рассмотрим бинарную последовательность s с периодом $4p$, получаемую посредством формулы (1) из пары l и l' :

$$s = I(l, L^d(l) + b(1), L^{2d}(l) + b(2), L^{3d}(l') + b(3)), \quad (1)$$

где L - оператор циклического сдвига на единицу влево, $p \equiv 3 \pmod{4}$, $d = (p+1)/4$ и числа $b(1)$, $b(2)$, $b(3)$ равны нулю или единице. В [13] рассмотрено четыре варианта значений $(b(1), b(2), b(3))$, когда они равны соответственно $(0, 0, 1)$, $(0, 1, 0)$, $(1, 0, 0)$ или $(1, 1, 1)$. Для последовательности s в этих случаях будем применять обозначение s_k , $k = 1, 2, 3, 4$, как и в [13]. Многочлены этих последовательностей обозначим через $S_k(x)$, $k = 1, 2, 3, 4$, соответственно.

Пример 1. Пусть $p = 7$. Тогда $l = (1, 1, 1, 0, 1, 0, 0)$ и $l' = (0, 1, 1, 0, 1, 0, 0)$. Рассмотрим первый случай, когда $(b(1), b(2), b(3)) = (0, 0, 1)$. Здесь $d = 2$, следовательно: $L^d(l) = L^2(l) = (1, 0, 1, 0, 0, 1, 1)$; $L^{2d}(l) = L^4(l) = (1, 0, 0, 1, 1, 1, 0)$; $L^{3d}(l') = L^6(l') = (0, 0, 1, 1, 0, 1, 0)$ и $L^{3d}(l') + b(3) = (1, 1, 0, 0, 1, 0, 1)$ и окончательно получаем, что

$$s = 1, 1, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1.$$

Во втором случае, чередующаяся последовательность v также с периодом равным $4p$, определяется по формуле

$$v = I(l, L^d(l) + b(1), L^{2d}(l') + b(2), L^{3d}(l') + b(3)), \quad (2)$$

где $d = (p+1)/4$, если $p \equiv 3 \pmod{4}$ и $d = (3p+1)/4$, когда $p \equiv 1 \pmod{4}$. Здесь в [13] также рассмотрено четыре варианта последовательностей, в зависимости от значений $b(1)$, $b(2)$, $b(3)$.

Вспомогательные леммы

Пусть $S(x) = \sum_{t=0}^{4p-1} s(t)x^t$ - многочлен, соответствующий рассматриваемой последовательности. Для вычисления 2-адической сложности воспользуемся хорошо известной формулой

$$\Phi_2(s) = \log_2 \left(\frac{2^{4p}-1}{\text{НОД}(S(2), 2^{4p}-1)} \right),$$

где, как обычно, $\text{НОД}(m, n)$ – наибольший общий делитель двух чисел m, n [1].

Следовательно, если $S(x)$ – порождающий многочлен последовательности $\tilde{s} = (s(N-1), s(N-2), \dots, s(0))$, то её 2-адическая сложность вычисляется по следующей формуле:

$$\Phi_2(\tilde{s}) = \log_2 \left(\frac{2^{4p}-1}{\text{НОД}(S(2), 2^{4p}-1)} \right). \quad (3)$$

Так как, $\tilde{\Phi}_2(s) = \min(\Phi_2(s), \Phi_2(\tilde{s}))$, то для вычисления симметричной 2-адической сложности последовательности, 2-адическая сложность которой известна, достаточно найти $\text{НОД}(S(2), 2^{4p}-1)$.

Для этого напомним свойства многочлена чередующейся последовательности, которые доказаны в [14]. Требуемые для дальнейшего свойства приведены в следующей лемме.

Лемма 1. Пусть c, e, f, h – бинарные последовательности с периодом N . Тогда для их многочленов над конечным полем второго порядка справедливы следующие соотношения:

1. $S_e(x) \equiv x^{N-d} S_c(x) \pmod{x^N - 1}$, если $e = L^d(c)$;
2. $S_e(x) = S_c(x) + \frac{x^N - 1}{x - 1}$, если e – дополнение последовательности c ;
3. $S_u(x) = S_c(x^4) + x S_e(x^4) + x^2 S_f(x^4) + x^3 S_h(x^4)$, если $u = I(c, e, f, h)$.

Лемма 2. Пусть s – двоичная последовательность, определенная по формуле

$$(1). \text{ Тогда } \tilde{s} = I \left(L^{p-3d} \left(\tilde{l}' \right) + b(3), L^{p-2d} \left(\tilde{l} \right) + b(2), L^{p-d} \left(\tilde{l} \right) + b(1), \tilde{l} \right).$$

Утверждение этой леммы следует из определения обратной последовательности и леммы 1.

Пример 2. Пусть $p = 7, (b(1), b(2), b(3)) = (0, 0, 1)$, как u в примере 1. Тогда $\tilde{l} = (0, 0, 1, 0, 1, 1, 1)$, $\tilde{l}' = (0, 0, 1, 0, 1, 1, 0)$, следовательно, $L^{p-3d}(\tilde{l}') = L(\tilde{l}') = (0, 1, 0, 1, 1, 0, 0)$, $L^{p-3d}(\tilde{l}') + b(3) = (1, 0, 1, 0, 0, 1, 1)$, $L^{p-2d}(\tilde{l}) = L^3(\tilde{l}) = (0, 1, 1, 1, 0, 0, 1)$ и $L^{p-d}(\tilde{l}) = L^5(\tilde{l}) = (1, 1, 0, 0, 1, 0, 1)$. Таким образом,

$$\tilde{s} = 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1.$$

Лемма 3. Пусть $S_k(x)$ – многочлен последовательности $s_k, k = 1, 2, 3, 4$. Тогда

$$\text{НОД}(\tilde{S}_k(2), 15) = \begin{cases} 15, & \text{если } k = 1, \\ 5, & \text{если } k = 3. \\ 3, & \text{если } k = 2, 4 \end{cases}$$

Доказательство. Положим $c = L^{p-3d}(\tilde{l}') + b(3), e = L^{p-2d}(\tilde{l}) + b(2), f = L^{p-d}(\tilde{l}) + b(1), h = \tilde{l}$. Тогда, по леммам 1 и 2 получаем, что

$$\tilde{S}_k(2) = S_c(2^4) + 2S_e(2^4) + 2^2S_f(2^4) + 2^3S_h(2^4).$$

Следовательно, справедливо сравнение

$$\tilde{S}_k(2) \equiv S_c(1) + 2S_e(1) + 2^2S_f(1) + 2^3S_h(1) \pmod{15}. \quad (4)$$

Так как коэффициенты используемых многочленов равны 0 или 1, то значение $S_c(1)$ равно числу ненулевых членов в многочлене $S_c(x)$, то есть в соответствующей последовательности c . Этот же факт имеет место и для других многочленов, участвующих в сравнении (4).

По определению, последовательность l имеет $(p+1)/2$ ненулевых элементов, а последовательность l' соответственно $(p-1)/2$.

Пусть $k = 1$. Здесь, $b(3) = 1$ и $S_c(1) = p - (p-1)/2 = (p+1)/2$, $b(2) = 0$ и $S_e(1) = (p+1)/2$, $b(1) = 0$ и $S_f(1) = (p+1)/2$, а также $S_h(1) = (p+1)/2$. В итоге, применяя сравнение (4), получаем, что $\tilde{S}_1(2) \equiv 0 \pmod{15}$. Значит, 15 делит $\tilde{S}_1(2)$. Утверждение этой леммы для других трех оставшихся случаев может быть показано тем же самым образом.

Лемма 4. Пусть $G(x^{-1}) = \sum_{t=0}^{4p-1} (-1)^{s(t)} x^t$. Тогда

$$2^{4p}G(2^{-1}) \equiv -4\tilde{S}(2) \pmod{2^{4p}-1}.$$

Доказательство. По определению имеем $2^{4p}G(2^{-1}) = \sum_{t=0}^{4p-1} (-1)^{s(t)} 2^{4p-t}$. Ясно, что $(-1)^{s(t)} = 1 - 2s(t)$. Следовательно,

$$2^{4p}G(2^{-1}) = \sum_{t=0}^{4p-1} (1 - 2s(t)) 2^{4p-t} = 2^{4p} - 1 - 2 \sum_{t=0}^{4p-1} s(t) 2^{4p-t}.$$

Далее, $\tilde{S}(2) = s(4p-1) + s(4p-2)2 + \dots + s(0)2^{4p-1}$. Значит, $\tilde{S}(2) = \sum_{t=0}^{4p-1} s(t) 2^{4p-t}$. Из последнего равенства следует утверждение этой леммы.

Симметричная 2-адическая сложность чередующихся последовательностей

Основные результаты работы представлены в этом разделе.

Теорема 1. Пусть $p > 3$. Тогда

$$\bar{\Phi}_2(s) = \Phi_2(\tilde{s}) = \Phi_2(s) = \begin{cases} \log_2 \left(\frac{2^{4p} - 1}{15} \right), & \text{если } k = 1, \\ \log_2 \left(\frac{2^{4p} - 1}{5} \right), & \text{если } k = 3, \\ \log_2 \left(\frac{2^{4p} - 1}{15} \right), & \text{если } k = 2, 4. \end{cases}$$

Доказательство. Согласно [13] имеем, что

$$\Phi_2(s) = \begin{cases} \log_2 \left(\frac{2^{4p} - 1}{15} \right), & \text{если } k = 1, \\ \log_2 \left(\frac{2^{4p} - 1}{5} \right), & \text{если } k = 3, \\ \log_2 \left(\frac{2^{4p} - 1}{15} \right), & \text{если } k = 2, 4. \end{cases}$$

Следовательно, для доказательства теоремы 1 достаточно показать, что $\Phi_2(\tilde{s}) = \Phi_2(s)$. Как замечено выше, для вычисления симметричной 2-адической сложности последовательностей по формуле (3) достаточно определить $\text{НОД}(\tilde{S}_k(2), 2^{4p} - 1)$.

Следующее сравнение, устанавливающее связь между многочленом последовательности $S(x) = \sum_{t=0}^{4p-1} s(t)x^t$ и её периодической автокорреляционной функцией $R_s(t) = \sum_{i=0}^{4p-1} (-1)^{s(i+t)+s(i)}$, доказано в [13]:

$$-2S(x)G(x^{-1}) \equiv 4p + \sum_{t=0}^{4p-1} R_s(t)x^t - G(x^{-1}) \sum_{t=0}^{4p-1} x^t \pmod{x^{4p} - 1},$$

$$\text{где } G(x^{-1}) = \sum_{t=0}^{4p-1} (-1)^{s(t)} x^t.$$

В силу леммы 4 имеем, что $2^{4p} G_k(2^{-1}) \equiv -4\tilde{S}_k(2) \pmod{2^{4p} - 1}$. Воспользовавшись леммой 11 из [13], получаем следующие сравнения:

$$1. \quad -4\tilde{S}_k(2)S_k(2) \equiv 2 \left[\frac{2^{4p}-1}{15} - (1 + (-1)^{b(1)2^p})(2^{2p} + 1) - p \right] \pmod{2^{4p} - 1}, \quad (5)$$

если $k = 1, 3$;

$$2. \quad -4S_k(2) \tilde{S}_k(2) \equiv 2 \left[\frac{2^{4p}-1}{15} 16 + (-1)^{b(3)} 2^p (2^{2p} - 1) \sum_{\mathbb{Z}_p^*} \frac{i}{p} \right] 2^{4i} - p \text{right}(\text{mod } 2^{4p} - 1),$$

если $k = 2, 4$.

Так как справедливо разложение $2^{4p} - 1 = 15 \cdot \frac{2^{4p}-1}{15}$ и $\text{НОД}(15, (2^{4p} - 1)/15) = 1$ для $p > 5$, то дальше рассмотрим два наибольших общих делителя $\text{НОД}(\tilde{S}_k(2), (2^{4p} - 1)/15)$ и $\text{НОД}(\tilde{S}_k(2), 15)$ [13].

Пусть $k = 1$ и q - простое число, делящее $\text{НОД}(\tilde{S}_1(2), (2^{4p} - 1)/15)$. Значение $b(1) = 0$ для $k = 1$. Тогда в силу сравнения (5) число q делит $\frac{2^{4p}-1}{15} - (1 + 2^p)(2^{2p} + 1) - p$. Так как q делит также $(2^{4p} - 1)/15$, то отсюда имеем, что q делит $p(2^p - 1)$, а именно, $2^p - 1$. Тогда q делит $-4 - p$, что противоречит малой теореме Ферма, согласно которой p делит $q - 1$, так как q и p - простые числа. Следовательно, $\text{НОД}(\tilde{S}_1(2), (2^{4p} - 1)/15) = 1$. Это утверждение также можно получить, воспользовавшись леммами 12-15 из [13].

Таким образом, $\text{НОД}(\tilde{S}_1(2), 2^{4p} - 1) = \text{НОД}(\tilde{S}_1(2), 15)$. Далее, согласно лемме 3 имеем $\text{НОД}(\tilde{S}_1(2), 15) = 15$. Таким образом, утверждение теоремы 1 для $k = 1$ следует из последнего равенства.

Доказательство теоремы 1 для $k = 2, 3, 4$ может быть получено подобным же образом.

Рассмотрим теперь второе семейство последовательностей, когда для определения последовательности v , применяется формула (2). Здесь, как и ранее, также рассмотрим четыре варианта для значений $(b(1), b(2), b(3))$, обозначая соответствующие последовательности через $v_k, k = 1, 2, 3, 4$, а их многочлены через $V_k(x), k = 1, 2, 3, 4$.

Теорема 2. Пусть $p > 5$. Тогда симметричная 2-адическая сложность последовательности v_k равна $\Phi_2(v_k) = \Phi_2(\tilde{v}_k) = \Phi_2(v_k) = \log_2(2^{4p} - 1)$ для $k = 1, 2, 3, 4$.

Доказательство. Используя те же самые рассуждения, как и при доказательстве теоремы 1, получаем, что $\text{НОД}(\tilde{V}_k(2), 2^{4p} - 1) = \text{НОД}(\tilde{V}_k(2), 15)$. Далее, как и в леммах 2 и 3 получаем, что справедливо сравнение

$$\tilde{V}_k(2) \equiv S_c(1) + 2S_e(1) + 2^2S_f(1) + 2^3S_h(1) \pmod{15}, \quad (6)$$

где $c = L^{p-3d}(\tilde{l}') + b(3)$, $e = L^{p-2d}(\tilde{l}') + b(2)$, $f = L^{p-d}(\tilde{l}) + b(1)$, $h = \tilde{l}$.

Пусть $k = 1$. Здесь, $b(3) = 1$ и $S_c(1) = p - (p-1)/2 = (p+1)/2$, $b(2) = 0$ и $S_e(1) = (p-1)/2$, $b(1) = 0$ и $S_f(1) = (p-1)/2$, а также $S_h(1) = (p+1)/2$. В итоге, из сравнения (6), видим, что

$$\tilde{V}_1(2) \equiv (p+1)/2 + 2(p-1)/2 + 4(p+1)/2 + 8(p+1)/2 \pmod{15}$$

или $2\tilde{V}_1(2) \equiv 11 \pmod{15}$. Значит, $\text{НОД}(\tilde{V}_1(2), 15) = 1$.

Значение 2-адической сложности для $k = 2, 3, 4$ может быть вычислено тем же самым способом.

Таким образом, показано, что симметричная 2-адическая сложность рассмотренных последовательностей во втором случае достигает максимально возможного значения, а в первом случае близка к нему.

Заключение

В работе исследована симметричная 2-адическая сложность, которые получаются чередованием циклических сдвигов последовательностей Лежандра и их дополнений. Показано, что симметричная 2-адической сложности рассмотренных последовательностей близка к максимально возможной. Полученные результаты развивают и обобщают полученные ранее в [13].

Благодарности

Работа выполнена при поддержке Российского научного фонда, проект № 24–21–00442.

Список литературы / References

1. Klapper A., Goresky M. Feedback shift registers, 2-adic span, and combiners with memory // Journal of Cryptology. 1997. 10 (2). 111-147. DOI: 10.1007/s001459900024
2. Goresky M., Klapper A. Algebraic Shift Register Sequences. Cambridge: Cambridge University Press, 2012.
3. 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
4. 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

5. 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
6. Xiao Z., Zeng X., Sun Z. 2-Adic complexity of two classes of generalized cyclotomic binary sequences // *International Journal of Foundations Computer Science*. 2016. 27 (7), 879-893. DOI: 10.1142/S0129054116500350
7. 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
8. Xiao Z., Zeng X., Ke M. On the symmetric 2-adic complexity of periodic binary sequences // *Advances in Mathematics of Communications*. 2024. 18 (5). 1303-1314. DOI: 10.3934/amc.2022088
9. Edemskiy V. Symmetric 4-adic complexity of quaternary sequences with low autocorrelation and period pq // *Advances in Mathematics of Communications*. 2024. 18 (6). 1723-1732. DOI: 10.3934/amc.2023017
10. Tang X., Gong G. New constructions of binary sequences with optimal autocorrelation value/magnitude // *IEEE Transactions on Information Theory*. 2010. 56 (3). 1278-1286. DOI: 10.1109/TIT.2009.2039159
11. Li N., Tang X. On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude // *IEEE Transactions on Information Theory*. 2011. 57 (11). 7597-7604. DOI: 10.1109/TIT.2011.2159575
12. Xiong H., Qu L., Li C. 2-Adic complexity of binary sequences with interleaved structure // *Finite Fields and their Applications*. 2015. 33. 14-28. DOI: 10.1016/j.ffa.2014.09.009
13. Xiao Z., Zeng X. 2-Adic complexity of two constructions of binary sequences with period $4N$ and optimal autocorrelation magnitude // *Cryptography and Communications*. 2021. 13 (5). 865-885. DOI: 10.1007/s12095-021-00498-8
14. Wang Q., Du X. N. The linear complexity of binary sequences with optimal autocorrelation / *IEEE Transactions on Information Theory*. 2010. 56 (12). 6388-6397. DOI: 10.1109/TIT.2010.2079550

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

Дроганова Дарья Сергеевна – студент, Новгородский государственный университет имени Ярослава Мудрого (Великий Новгород, Россия), ORCID: 0009-0000-5010-026X, darya.droganova@gmail.com